How to Deliver Sustainable Configuration Management

Nelson Ruest & Danielle Ruest

Developed for Ecora Software

Abstract

This white paper provides an overview of IT documentation practices and procedures. Its intended audience is IT executives, system administrators and technicians who belong to organizations that want to implement a structured approach to system management, especially, through proper documentation practices. It also addresses organizations that need to comply with recent regulation implementations such as HIPAA or the Sarbanes-Oxley Act. This paper presents a comprehensive look at the reasoning behind documentation requirements and standards implementations. It then proceeds to describe how to address these issues, especially in time-constrained IT environments.

In addition, this paper outlines a selection of best practices for documentation. It also provides a list of selection criteria that can be used for the acquisition of automated tools that can help support standard processes.

About the Authors

Danielle Ruest and Nelson Ruest are IT professionals specializing in systems administration, migration and design. They are authors of multiple books, notably two books published by McGraw-Hill Osborne, “Windows Server 2003: Best Practices for Enterprise Deployments”, ISBN 0-07-222343-X and “Windows Server 2003 Pocket Administrator”, ISBN 0-07-222977-2 as well as “Preparing for .NET Enterprise Technologies”, published by Addison Wesley, ISBN 0-201-73487-7. They have extensive experience in standard operating procedure development and documentation strategies.

Table of Contents

1. The Case for Infrastructure Control

The bane of the technician is documentation. Don't you hate it when someone hounds you to get a document done? What's interesting is the technology itself and what it can do, not how you use it, right? Besides, you don't have time to document; you're too busy putting out fires. Did you know that each document you create automatically puts out its own fires? That's right. There *is* a reason why documentation is so important. Well, more than one actually.

Different Takes on Documentation

The CIO:
"I need documentation to be able to know what's going on."

The Administrator:
"I need documentation to ensure that we can fix things if you aren't there."

The Technician:
"We don't have time for documentation!"

Few people understand and control their infrastructure completely. When asked point blank: "How many servers do you have?", it's not unusual to receive a vague answer; something like "We have between eighty (80) and one hundred (100) servers." Well, which is it? Eighty or one hundred? There is a significant difference. How can you manage what you don't know? The answer is easy: you can't!

That's why IT personnel are so busy putting out fires. IT infrastructures aren't getting simpler, they're getting more complex. Users want to have all the functionalities—instant messaging, collaboration, integrated search engines, email, mobile Internet, Single Sign On and more—and they don't care how it's done. But one thing is sure, it better work all the time once they get it.

It's IT's responsibility to provide these services and to make sure they're always available. But as an IT professional, you're often faced with legacy systems you need to keep running while integrating and deploying new technologies. It's also quite common to find yourself in a situation where you inherit systems from other organizations through mergers or acquisitions. These systems, of course, will be running on completely different platforms or will be outdated, running older versions of operating systems and application software. This only serves to complicate matters.

Working with Heterogeneous Environments

Ecora Enterprise Auditor supports information reporting from environments that include technologies such as Microsoft Windows, Novell NetWare and Unix, among others.

Your job is to install and support the IT infrastructure. Given that, one of your major responsibilities is to know this infrastructure, ideally inside and out. The job is simpler if you only have a handful of servers and a few users, but when you get to very large infrastructures with multiple hundreds of servers and thousands of users, it gets much more complex.

This is one reason why more and more people are opting for new, standard approaches to IT management. One approach is to use the Information Technology Infrastructure Library (ITIL). That's because it helps provides the standards you need in technology management. But complexity is not the only reason to standardize. There are also a series of new compliance measures—Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and so on—whose requirements you have to meet; all this in addition to your everyday tasks.

So you see, documentation is important and it is becoming more so every day. It's not that you're not interested in good documentation; sometimes it's just trying to find out where to start that seems overwhelming. There are methods and approaches that can help, but no matter which approach you use, documenting an infrastructure involves work. The biggest problem is gathering the information. There are hundreds of configuration settings on each server; there are hundreds of software products in your network; and, there are dozens of other component types that are just as complex to document. But once you do know what you have, you'll soon realize that you'll be able to do a so much more with you infrastructure.

Know Your Infrastructure

If you can automate the process of gathering your information, you should aim for the automation of at least 80 percent of the contents of your systems. This greatly reduces manual preparation of information.

For example, an infrastructure you know is a lot more secure by default. There are no rogue accounts left without passwords anywhere. There are no group members that shouldn't be in high-security groups. There are no unsecured settings that shouldn't be set on critical servers. Knowing your infrastructure is also quite useful for disaster recovery. You don't want to be in a position where you have to wonder about just what was on that server that crashed yesterday; you'll know ahead of time. This might even give you the time to automate its recovery.

But good documentation doesn't only support security and disaster recovery; it also helps with change management. By documenting your infrastructure, you can begin to provide reports when they're needed. This helps with change tracking and even event auditing, letting you know both how your infrastructure is being used and how it evolves over time.

The question is: "How do you bring it all together?" That's what this paper is all about.

2. Key Focuses for Configuration Management

OK, so now you've been assigned the task to document your infrastructure and just basically know where you stand. But where do you start? What do you need to cover? The best way to identify where to start is to look at which factors drive your need for documentation. There are several, but some of the most important are:

- Improved Security
- Compliance
- Proactive Management
- Standards Implementation
- Improved Control over the Network

All of these are keys to improved network services.

2.1 Improve Your Security Levels

Security is a major issue today. Everyone is talking about proper patch management, proper antivirus systems, proper spam detection systems, just to name a few. All of these elements are a very small part of an overall security plan, but each has its own place. Documentation plays a very important role in any security strategy because it's hard to protect what you don't know you have.

One good example is laboratory environments. How many times have we heard about major security flaws discovered because someone forgot to add a password to a critical administrative account? Even Microsoft has been a victim of this. It seems that technical staff thinks less of security when testing out new technologies. Fortunately, new versions of operating systems are becoming more secure by default, but we can't just rely on the features of our systems; we need to go far beyond that if we want to have a more secure infrastructure.

New default security features in systems won't help if we don't have proper procedures to support them. For example, there's no point in having complex passwords if someone leaves a post-it note on the server's screen in the server room. Anybody you know? Not that anyone will attest to it, but this is a practice that still goes on even today. And then, people will complain about users!

The best way to determine what to document is to use a model. The model proposed here is the Castle Defense System (CDS)[1]. In medieval times, people needed to protect themselves and their belongings through the design of a defense system that was primarily based on cumulative barriers to entry. If you've ever visited a medieval castle or seen a movie with a medieval theme, you'll remember that the first line of defense is often the moat. The moat is a barrier that is designed to stop people from reaching the castle wall. Moats often include

[1] The Castle Defense System first appeared in *Windows Server 2003, Best Practices for Enterprise Deployments* by Ruest and Ruest.

dangerous creatures (alligators, piranhas) that will add a second level of protection within the same barrier. Next, you have the castle walls. These are designed to repel enemies. At the top of the walls, you will find crenellated edges allowing archers to fire on the enemy while still being able to hide when fired upon. There are doors of various sizes within the walls, a gate and a drawbridge for the moat. All entry points have guards posted. Once again, multiple levels of protection are applied within the same layer.

The third defense layer is the courtyard within the castle walls. This is designed as a "killing field" so that if enemies do manage to breach the castle walls, they will find themselves within an internal zone that offers no cover from attackers located either on the external castle walls or within the castle itself. The fourth layer of defense is the castle itself. This is the main building within which are found the crown jewels. It is designed to be defensible on its own; stairways are narrow and rooms are arranged to confuse the enemy. The fifth and last layer of protection is the vault held within the heart of the castle. It is difficult to reach and highly guarded.

This is, of course, a rudimentary description of the defenses included in a castle. Medieval engineers worked very hard to include multiple defense systems within each layer of protection. But it serves its purpose. An IT defense system should be designed in the same way as a Castle Defense System (CDS). Just like the CDS, the IT defense system requires layers of protection. In fact, five layers of protection seem appropriate. Starting from the inside, you'll find:

- **Layer 1: Critical Information** This is the information vault. The heart of the system is the information you seek to protect.
- **Layer 2: Physical Protection** Security measures should always begin with a level of physical protection for information systems. This compares to the castle itself.
- **Layer 3: Operating System Hardening** Once the physical defenses have been put in place, you need to "harden" each computer's operating system in order to limit the potential attack surface as much as possible. This is the courtyard.
- **Layer 4: Information Access** When you give access to your data, you'll need to ensure that everyone is authenticated, authorized and audited. These are the castle walls and the doors you open within them.
- **Layer 5: External Access** The final layer of protection deals with the outside world. It includes the perimeter network and all of its defenses. It is your castle moat.

In order to become a complete Security Policy, this five layer system must be supplemented by two elements: People and Processes. These two elements surround the CDS and help complete the security strategy picture it represents.

Once the strategy has been established, you need to design and implement your defenses, monitor them on an active basis, and regularly test and update them. These four security management activities—policy design, defense planning, monitoring and testing—make up the Security Plan. These interact with the Castle Defense System to complete the practice of security management. The five-layer Castle Defense System and its relationship to security management activities are illustrated in Figure 1.

Tools to Protect Information

You need to ensure that the tools you choose to gather and store information, especially information about your systems, are secure at all times.

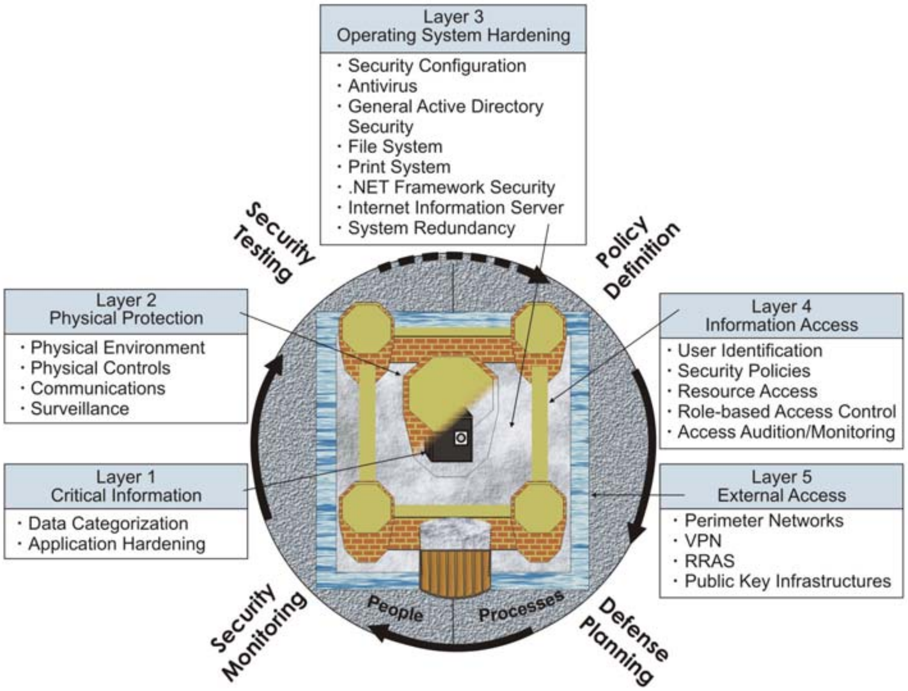

Figure 1: The Castle Defense System and the security management activities that surround it.

Security Documentation

Ecora Enterprise Auditor offers can help generate the documentation you require to be able to properly protect your systems.

The key to the security plan is in knowing what to cover and knowing why it needs to be covered. The first part—knowing what to cover—is outlined in the Castle Defense System. It identifies all of the areas that require coverage by the security policy and helps you be prepared for any eventuality. Next is defense planning; it is focused on identifying which types of attacks you can expect. Once this is done, you pass on to security monitoring, or auditing security events to ensure nothing goes awry. The final management activity, security testing, is as vital as all of the others because it helps you ensure your systems effectively protect your environment.

The core element that ties all of the components of your security plan together is documentation. It is impossible to protect and control your environment if you do not know what you have. This is why the very first place to start with your security plan is to gather information about your network and the systems it holds. Ideally, you'll already have some of this documentation in hand, but if you don't, you might want to seriously consider looking at automated tools that can help gather information about your network and the systems it contains.

2.2 Meet the Compliance Acts

In addition to security, documentation is now required for compliancy to new legal obligations that have emerged in light of recent events. Four key acts affect the type of documentation you now require:

- 21 CFR Part 11
- Gramm-Leach-Bliley Act
- HIPAA (Health Insurance Portability and Accountability Act)
- Sarbanes-Oxley Act

Each act has its own requirements.

2.2.1 21 CFR Part 11

Compliance Support

Ecora Enterprise Auditor offers specific support for compliance documentation.

Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11) is part of the Food and Drug Association's guidelines for trustworthy electronic records and requires organizations to employ procedures and controls that are designed to ensure the authenticity, integrity and if necessary, the confidentiality of electronic records. If called upon to validate a system, you would have to provide documentation on the way your systems have been installed and configured to prove that three specific processes were completed. These include:

- Installation Qualification
- Operation Qualification
- Performance Qualification

These processes are necessary to support the FDA's regulations which require the following controls and requirements:

- Limiting system access to authorized individuals
- Use of operational system checks
- Use of authority checks
- Use of device checks
- Determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- Appropriate controls over systems documentation
- Controls for open systems corresponding to controls for closed systems bulleted above
- Requirements related to electronic signatures

Evaluation is based on five factors. Each one must be met for compliance to these guidelines.

- The first is validation. You must be able to prove that you have evaluated the potential of a system to affect product quality and safety, and record integrity.
- The second is auditing. You must be able to trace the changes that have been applied to the systems.
- The third deals with legacy systems. According to 21 CFR Part 11, a legacy system is one which was in place before the regulation became effective. Unfortunately, that was August 20, 1997. With the rate of change in IT, few systems that were put in place in 1997 are still operational today.
- The fourth relates to copies of records. You must be able to provide valid copies of your records.
- The final factor is record retention. You must store records of your system changes and you must be able to prove that these records have not been tampered with.

While you may or may not be affected by this rule, you don't want to learn the hard way that as far as an auditor is concerned, if you don't have an item documented, it hasn't happened in real life. In this regard, it's always better to be prepared beforehand.

2.2.2 The Gramm-Leach-Bliley Act (GLB Act)

If you're in a financial institution, you need to safeguard the confidentiality and integrity of your customer information. This is no longer just a best practice, it is now a legal requirement—a requirement enforced by the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act. This act mandates that your institution establish appropriate security standards to protect private customer and employee data from internal and external threats. This data also has to be completely protected from unauthorized access.

This means a complete and accurate auditing trail of all events related to this data as well as well-documented configuration information on the systems you put in place to protect it.

The GLB Act gives authority to some federal agencies and each state to administer and enforce two regulations: the Financial Privacy Rule and the Safeguards Rule. These rules apply to financial institutions which, according to the Federal Trade Commission, include not only banks, securities firms, and insurance companies, but also companies providing other types of financial products and services to consumers. These products and services include lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities.

If you're in any of these categories, you need to properly document how you protect this data and what measures you have taken to ensure that it remains protected.

2.2.3 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) has had a major impact on how health care providers do business electronically. The implications of this act are not only limited to the providers themselves but also affect their business partners. This act addresses four particular areas of electronic health care provision:

- Electronic transactions and code sets
- Security of the systems
- Use of unique identifiers for patients
- Privacy of patient and other critical information

Not all operations need to be performed electronically, but if they are, they must be performed in accordance to the standard format outlined in the act. If you contract a third-party organization to conduct a service for you, for example, electronic billing, it is your responsibility as the health care provider to ensure that this third-party organization comply with the requirements of the act.

HIPAA applies mostly to any organization that conducts one of the following in relation to health care:

- Claims
- Payment or Remittance Advice
- Claims Status Inquiry or Response
- Eligibility Evaluations
- Referral Authorizations

This means that if your organization is in this category, you need to fully document your systems and how your systems and processes protect the information outlined above. In fact you have to:

- Notify patients about their privacy rights and how their information may be used
- Adopt and implement privacy procedures
- Train employees in your privacy procedures
- Designate an individual as the privacy agent responsible for overseeing how these rules are adopted and followed
- Secure patient records containing information pertaining to specific individuals

Once again, this has a lot to do with standards and documentation. This is another occasion where you can’t simply say “I don’t have time for documentation!”

Tracking Changes in the Network

Ecora Enterprise Auditor can automatically gather information about change in your network. In addition, if the change is critical, it can alert you directly.

2.2.4 The Sarbanes-Oxley Act

Probably the single most important act affecting information technology in publicly-traded companies is the Sarbanes-Oxley Act enforced by the Security and Exchange Commission. This act outlines that all public organizations demonstrate due diligence in the disclosure of financial information. In addition, organizations are responsible for the implementation of internal controls and procedures that ensure that the data is protected at all times. This includes protection of the data during transmission as well as where and how the data is stored.

It is particularly section 404 of this act that applies to IT controls. This section, entitled "Management Assessment of Internal Controls" requires that each annual report of any publicly-traded organization contain an internal control report. This report must:

- State the responsibility of management for establishing and maintaining this internal control structure and the procedures for financial reporting.
- Contain an assessment of the effectiveness of the internal control structure and procedures used for financial reporting.

You must also indicate if you have adopted a code of ethics for senior financial officers and if you have, you must disclose the contents of that code.

In the event of an audit, you must give auditors documented evidence of data storage, protection mechanisms and identify the internal controls you have applied to this data. Once again, this is a specific requirement for documentation, one that you have to comply with.

The Sarbanes-Oxley Act went into effect for larger organizations with market capitalization of $75 million on November 15th, 2004. But don't feel you're off the hook because all other publicly-traded company must comply with this act in the first annual report produced after July 15th, 2005.

2.3 Implement Standards

One of the most important aspects of any IT environments is the standardization of all approaches. Too many organizations rely on key individuals and how these key individuals perform their tasks instead of ensuring that all processes are documented and streamlined so that if this key individual is not available, business can still continue as usual. But, of course, given that you keep putting out fires all the time, how can you take the time to implement standards in your organization? One good answer is the Information Technology Infrastructure Library (ITIL).

Support for ITIL

Ecora Enterprise Auditor is based on best practices derived from ITIL processes to help ease the implementation of ITIL standards in organizations.

ITIL is the acronym for the guidelines developed by the Office of Government Commerce in Norwich, England, for the British government. In time, ITIL has become the de-facto global standard in the area of service management. ITIL contains comprehensive publicly accessible specialist documentation on the planning, provision and support of IT services. It can help form the basis for the implementation of standards within any IT infrastructure. ITIL was developed by a series of service organizations, IT employees, suppliers, consultants and trainers. This set of documentation describes the architecture for establishing and operating IT service management. ITIL information is available in book form, but also in the form of training and coaching, certification exams and even on a consultancy basis.

ITIL provides best practice guidelines for service management. These practices describe what to do rather than how to do it. This is because service management practices often become bogged down in internal structures that can become rigid. ITIL takes away from this by focusing on the service itself, not corporate history. At first glance, implementing ITIL may seem daunting, but keep in mind that it is the standardization of all processes that is the most important aspect of this implementation, not the establishment of a rigid structure for operations management. A standard checklist for any given activity is just as good if not better than the implementation of a complex service structure.

Implement a few standards and you'll soon reap the benefits of improved service delivery.

3. How To Move Forward

In the end, documentation and standards can only help improve the control you have over your IT infrastructure. You now understand why you need both. You also understand what you need to document, but how can you proceed? There are two methods that can help lead to better knowledge of the systems you manage:

- In the first, you proceed with manual documentation and manual implementation of standards
- In the second, you automate the process of gathering information about your systems and you supplement this information with change tracking

Both have merit. The one you choose will depend on two factors: the size of your organization and your willingness to invest in standardization and documentation.

3.1 Manual Documentation Processes

Another very useful reason for documenting your systems and the information they contain is proactive management. Aren't you tired of always having to put out fires when the happen? This type of reactive management puts an enormous strain on information professionals. It doesn't allow them to perform at their peak because they rarely have the time to develop their own skills. That's because they're always busy catching up and patching the systems that help run your business.

Proactive management relies very heavily on infrastructure knowledge and standard operating procedures (SOP). SOPs especially are a key component of this management approach. How can you tell what has been done on your systems or in your network if each technician performs the same task in a different manner? The answer is simple: you can't. SOPs do not have to be complex to be implemented. They can be as simple as a proper checklist for a specific operation.

Take for example installation instructions. There are a lot of methods you can use to standardize installations. One of the best is automation. If you use a script or an automated batch file to perform an installation, you can be guaranteed that it will be performed in the same manner every time. Automation doesn't work in every situation, but it is a start. It needs to be augmented with manual checklists for operations that can't be automated. For example, you can completely automate the installation of Windows Server 2003, but to do so, you need to begin with at least one manual process for the initial configuration of the machine.

That's the nature of manual documentation: it has to be done before you perform an activity. Then once the activity has been performed and your documentation has been validated, you can move to automation of certain processes. You can, of course, try to reverse the process, but you better make sure your installation tests are in a laboratory environment and not in your production network.

You can also rely on the manufacturer's documentation, but it's often not enough. Take for example the installation of a complex product such as Microsoft Content Management Server 2002 (MCMS) on a Microsoft Windows Server 2003 server. This might seem fairly straight forward at first, but there are several "gotchas" in this installation. First of all, MCMS was released prior to Windows Server 2003 so you can't rely on the documentation that is included in the installation CD because it predates Windows Server. Second, Microsoft complied with legal rulings regarding its Java Virtual Machine since the release of MCMS 2002, therefore, it had to change some code in the product. This change is evidenced in a new release of MCMS, version 2002 with Service Pack 1a. In addition, though the installation is in Windows Installer format, it does not include comprehensive scripts for both prerequisite installations and prerequisite configurations. This means that there are quite a few manual operations that must be performed prior to the installation of MCMS.

As you can see, preparing a proper installation of a complex product in a complex IT environment requires careful planning and lots of testing. But once, you've got it, you better make sure you document it properly because this is one thing you won't find on the Internet.

3.2 Automated Documentation

The second method for documentation is through automation. This usually means acquiring a product that can perform many of the documentation tasks for you. For example, if you have a tool that can scan all of your systems, no matter which platform they reside on, and produce detailed reports of their current status, it can be an easy step to produce change documentation when you install a new product. This is done by scanning the state of a system prior to installation, then scanning it after installation.

Ecora Enterprise Auditor

Ecora Enterprise Auditor has been designed to automate the documentation and compliance processes for organizations of all sizes.

This is a familiar method, especially for IT professionals that focus on software installation packaging. The core engine for most software packaging tools uses a "scan for status first, and then scan for changes later" approach. But a software installation tool isn't enough to keep track of everything that is in your network.

What you need is a tool that will perform constant and regular scans of all systems to identify the current state of each component as well as list deltas from previous states. There are several tools that provide this type of information, but the best will focus on agent-less information gathering techniques and will rely on native strategies for information collection. In addition, such a tool will also provide you with a comprehensive set of reports that meet all of your needs and requirement.

Ideally, this tool will support your change and configuration management practices and will also audit all changes in your network, even alerting you to critical changes. Implementing an automated tool will not relieve you of the burden to standardize your operations and implement proper processes, but it will help you get a head start on the entire process by giving you a starting point you can use immediately. Comprehensive information on your existing environments can be gathered in a matter of minutes. You'll be surprised at what you find. In fact, you may well identify a number of issues that require immediate attention, especially if you need to maintain compliance to the standards mentioned above.

4. Configuration Documentation Best Practices

In the end, you know you need to proceed but you might have been wondering where to start. There are two places to start:

- Implement best practices in terms of documentation
- Determine whether an automated tool would be best for you

Armed with these two concepts, you'll be able to move forward into an environment where your systems are standardized and managed in a proactive rather than reactive manner.

4.1 Best Practices for Configuration Documentation

Use the following best practices for the implementation of new documentation practices:

1. **Begin small**. Start with the core components of your network. Usually a graphical representation of the network is best.
2. **Choose a specific starting point**. This may be as simple as ensuring that installation processes are fully documented and all machines that are prepared from this point on are prepared through this new or updated process.
3. **Develop a documentation plan**. This plan should include standard formats for both long and short documents as well as presentations and graphics. This should also include standard datasheets for specific documentation requirements.
4. **Develop a strategy for standard operating procedures**. You need to make sure everyone is on the same wavelength. To do so, standardize your procedures. Lots of information on SOPs is available on the Internet.
5. **Create documentation roadmaps**. Identify what you want to document and which documentation format would suit it best.
6. **Determine if you need compliance**. If you need compliance, you'll need to ensure that the standards you need to comply with are included in your documentation strategy.
7. **Communicate your new standards**. Make sure both current and new staff know about your new strategy. New staff should have a "Welcome Booklet" that outlines how your organization works.
8. **Train your staff**. Make sure your staff has the skills required to properly document your environment.
9. **Track changes**. Make sure you update your documents whenever there are changes applied in your environment.
10. **Don't be afraid to use expert help when you need it**. Expert help can be in the form of consultancies or automated tools. If the proper tool can give you a head start, then perhaps that's where you need to start.

4.2 Automated Configuration Documentation Tool Selection Criteria

If you decide that an automated tool is where you need to start, make sure it meets the following criteria.

1. **Does the tool support all of your infrastructure?** Use the 80/20 rule. Make sure the tool covers at least 80 percent of the components in your infrastructure. That leaves only a small portion of the infrastructure to address manually.
2. **Does the tool include the reports you require?** If you're going to use an automated documentation tool, you better make sure it produces the type of information you need.
3. **Does the tool explicitly support compliancy standards?** If you're faced with having to address one of the compliancy acts, can this tool provide the specific information you require?
4. **Does the tool track changes as well as provide initial infrastructure documentation?** Make sure you can track all changes in the network with this tool.
5. **Does the tool support alerts?** Having the automated tool provide you with notifications at the moment of a critical change will help ensure you maintain standards in your infrastructure.
6. **Does the tool include best practices?** Best practices such as those based on ITIL should be embedded into the tool to help you move forward with standards implementations.
7. **Does the tool help protect the information it gathers?** Is the security interface provided by the tool sufficient to protect the data it generates?
8. **Does the tool require the deployment of agents?** Ideally, the tool would operate from a central console using native features and functionalities from the infrastructure components you include in the information collection. Having to deploy agents to each device only complicates matters and often defeats the purpose of the tool itself.
9. **Does the tool work in heterogeneous environments?** Few organizations have a single integrated infrastructure. The tool you select must support the technologies you have selected to embrace.
10. **Will the tool provide additional help in your standardization efforts?** Find out if the tool can help support your standardization efforts. After all, you want to simplify your workload, not add to it.

If the tool you choose answers to each of these requirements, you'll find that you're quickly on your way to fast and efficient compliance. There, documentation isn't so hard is it?

Appendix A — References

- *Windows Server 2003, Best Practices for Enterprise Deployments*, Ruest & Ruest, McGraw-Hill Osborne, ISBN: 0-07-222343-X
- *Windows Server 2003, Pocket Administrator,* Ruest & Ruest, McGraw-Hill Osborne, ISBN: 0-07-222977-2
- *21 CFR Part 11, FDA* http://www.21cfrpart11.com/index.html
- *Gramm-Leach-Bliley Act* http://www.ftc.gov/privacy/glbact/
- *HIPAA (Health Insurance Portability and Accountability Act)* http://www.hhs.gov/ocr/hipaa/
- *Support for HIPAA* http://www.hipaa.org/
- *The Sarbanes-Oxley Act* http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
- *A Summary of the Sarbanes-Oxley Act* *http://www.aicpa.org/info/sarbanes_oxley_summary.htm*
- *Information Technology Infrastructure Library* http://www.itil.org/itil_e/index_e.html