Global Information Assurance Certification Paper

Planning a Secure Migration Project
Best Practices for Migrating from Windows NT to Windows 2000

By Ben Eason

This paper discusses the steps involved in migrating from Windows NT to Windows 2000. The scope of this paper is focused on supplying resources and defining basic project planning tips for a successful migration with security as a central theme. This paper is not intended to be a step-by-step walkthrough. This paper assumes that you are familiar with Windows NT 4.0 and Windows 2000. It is important to note that migrating to Windows 2000 requires an extraordinary amount of time, planning, and resources.

Framework for a successful migration
Step 1: Project Planning
Step 2: Research
Step 3: Planning your future network.
Step 4: Test your plan
Step 5: Deployment

Project Planning:

The obvious areas that will require the most time and resources are developing the plan which includes research and testing your proof of concept in your test network. Project planning will be mentioned often throughout this paper. Appendix A is the task list from a very well done Microsoft Project 2000 template that comes with Microsoft Project 2000.

Research:

Most of the information on migration is very dry, mostly due to all of the tedious details and the fact that everything written on migration sounds the same. I have not found any single source that even comes close to being a definitive planning guide. During research, the key pieces of information you will want to pay attention to are, that which will help you plan your schema, your namespace/domains, your Organizational Units, and your delegation of authority. Basically, anything that discusses the Group Policy tool, "domain collapse", Active Directory (AD) replication, and DNS planning should be highlighted. While the focus of your research may initially be to learn the new technologies that exist, as you start creating your vision you should also be researching tools that will help you in migrating to and administering your new domain.

Microsoft's Windows 2000 technical library website is a great place to begin your research if you do not already have a good understanding of Windows 2000. The link below has several white papers from Microsoft specifically on migration. I recommend, "Planning Migration from Windows NT to Windows 2000" as a good starting point. This is also dry reading but gives an acceptable introduction to the issues at hand with the obvious exception of security.
http://www.microsoft.com/windows2000/library/planning/pds-cduadtoc.asp
The next step is to read everything in the technical white papers section and step-by-step guides section that pertains to the services you are currently running or plan on running for a general look at what is ahead. The Windows 2000 resource kit and all of the utilities in the \support\tools folder on the Windows 2000 server installation media should be

researched as well. Often learning about what a specific tool does will give you insight to a potential problem you did not realize you were going to have.

Windows 2000 DNS, published by New Riders, is a fairly well written book that gives an extended overview of DNS's role and implementation under Windows 2000. This is an important book for planning because DNS is a required element of a Windows 2000 network and Active Directory.

Windows 2000 Active Directory from the O'Reilly series is also a comprehensive book to read before planning, especially the chapter on namespace. It is imperative that you understand Active Directory before you begin to migrate your domain. Active Directory is not just a new feature in Windows 2000. Every feature and service of Windows 2000 integrates in some fashion with Active Directory.

For an in-depth view of migration and Active Directory planning, check out Microsoft Press's Notes from the field Series book entitled *Building an Enterprise Active Directory*. This is a strategy-oriented book that has some valuable metrics for calculating replication bandwidth requirements and interesting tips on getting your non-MS DNS servers "borged" into your new 2000 domain.

Make sure you have read all of Microsoft's security bulletins.
http://www.microsoft.com/technet/security/current.asp?productID=6&servicePackId=0

Read the freely available student practical assignments on Windows 2000 security. These practical assignments written by students attempting certification as Windows Security Administrators can be found at: http://www.sans.org/giactc/gcnt.htm
Of particular interest are the following:

> Robert Huie analyzes the security templates that come with Windows 2000 and provides a detailed explanation of what the different templates are and gives suggestions on making changes to them.
> http://www.sans.org/y2k/practical/Robert_Huie_GCNT.doc
>
> Andy Brock's "Hardening Windows 2000 Advanced Server for Internet Participation" is a good resource for looking at the unique security settings needed for these machines. Also this can be applied, with some work, as a group policy object for your old resource domain's new Acitve Directory Organizational Unit.
> http://www.sans.org/y2k/practical/Andy_Brock_GCNT.zip

Subscribe to the SANS newsletters and make sure you are staying up-to-date on all of your application's security news.

Planning your future network:

Developing a Vision:

The actual planning phase is quite extensive. Knowing what your business' IT objectives are and what features exist in Windows 2000 is critical. Flow charts and block

diagrams can be very useful in describing your migration vision to the executives. Hopefully, while researching all of the new technologies Windows 2000 has to offer you were able to see a vision for how 2000 is going to help your network. Keeping things simple and following the strategies outlined below will help make for a substantially easier migration project. This part of the paper will try to follow the Microsoft Project Windows 2000 migration project template shown in Appendix A.

Picking good IT staff and appropriately delegating responsibility, though outside the scope of this paper is a very important part of migration planning and should be taken seriously. Nevertheless it will not be covered.

Start by finding out what your network currently looks like, domain structure, WAN links, subnets, VPNs, domain controller and other network servers, databases, workstation hardware, software, and current configurations. Developing the plan at this point is about clearly deciding what the objectives are. If you did not already know, domain consolidation should be one of your preliminary design objectives. I am mentioning this early so you can think about it while we continue.

Following the Microsoft Project template the next part of developing your plan is where you should give your vision a reality check against what your current network can support and what it actually needs. Microsoft recommends at the completion of this point that you consult your executive sponsor and share the vision. This is a good idea. Typically he or she is going to want to have some input in the project design. This gives the executive sponsor a chance during the conceptual planning phase to make comments or suggestions before in-depth technical planning is made.

Planning the test network:

So now you have learned all about the features of Windows 2000 and you have a vision for what your network is going to become. The next big step is planning how to test your plan. Building a test network can be pretty expensive. It is very important to make sure that the hardware, software and configurations of your test network exactly match that of your production network.

Once you have built your test network and have verified that it is as close to your production network as possible you need to test your ability to bring the entire lab back to this point. In fact, as you get further into testing, your base point for starting each new test will change and you will want to make sure that your lab can restart from multiple points in the migration. Each run-through of the test is going to be very time consuming and you will want to both carefully plan and document everything that you intend to do and everything that happens so redundant testing will not be necessary. Try to design an environment that can be rapidly reverted to its previous state.

Risk assessment and communication strategy development will not be discussed in this paper.

Education planning:

All of the tools to manage and maintain a Windows 2000 network are different from the ones used in Windows NT 4 domains. Everyone will need training both in the test and deployment staff and your regular internal support staff. This is obviously yet another critical part of deploying Windows 2000 successfully. End-user education should be planned at this stage also.

Migration Strategy:

Every book that you read on migration will spend a lot of time talking about domain restructure and domain collapse and various other conceptual migration strategies. Allow me to simplify. Everyone that has more than one domain should as a preliminary design objective, plan to reduce their network to as few domains as possible. The reason for this is because Microsoft, with Active Directory, has redesigned how domains are managed.

The only real migration strategy that you need to think about in this sense is whether or not you want to actually perform an upgrade. You might decide to install and configure your new domain next to your current one and then use the movetree.exe utility to move your users and their current SIDS (Windows NT Security Identifiers) to the new domain. While appealing to those of us acclimated to scrapping old Microsoft systems and starting over now and again this technique only works if your new domain will be in native mode.

In the past you might have used multiple domains for delegation of authority or because of the size limits the Windows NT 4.0 SAM database had. The only reason in Windows 2000 to separate domains is for replication/bandwidth reasons. AD, which is just a file, is replicated between all of your Domain Controllers (DCs). However, not every DC has every part of the AD because it is too big. And this is in fact the problem. So much information must get replicated across the entire network that special DCs are needed, called Global Catalog servers (GCSs). GCSs are responsible for replicating their domain's information and replicating information in the AD that is from domains other than the one they control. GCSs and replication will be covered later when we get into Active Directory. Nevertheless, a single domain is the goal. As you look at your current network map, look at the network links the different segments of your network are using and figure out which domains could easily become organizational units. Once you have done all of this the namespace has, for the most part, already been determined.

The next planning step involves looking at your domain controllers. DCs have several new features that need to be considered at this point, multi-master replication and the FSMO services. Multi-master replication effectively means you can no longer leave your BDCs lying around in unprotected rooms. The multi-master nature of Windows 2000 DCs really describes the way the DCs replicate the AD database to each other; a change in one will be replicated to all. However, this does not mean that all domain controllers are created equal. There are five Flexible Single Master Operation roles. These roles are not suited to a multi-master environment but still use the replicated active

directory database to store their data such that if one server goes down permanently, a different server can be forcibly promoted. It is recommended that at the very least the RID master and PDC emulator roles be separated. More on FSMOs will be discussed in Appendix C.

Once you have a handle on what order you are going to upgrade your domains in and what strategy you are going to use, you can begin developing your back out strategy. Even more important than carefully planning your upgrade is carefully planning and exhaustively testing your back out strategy. Things go wrong even with the most robust test labs and best thought out plans. It is quite likely that you will have to take a couple shots at migrating specific parts or your network.

Native Mode:

Determining when to go to native mode is one of the least important of all of the planning decisions to make. Microsoft makes going native equally appealing and scary. Many security benefits are gained at the switch. Namely, you can drop support for the NetBIOS protocol and finally protect yourself from null user sessions. However, switching to native mode is a one-way switch and many of your current network applications will break because support is gone for everything pre-windows 2000. Many of Windows 2000's features can still be taken advantage of even while in mixed-mode.

Active Directory:

Within the scope of the planning of Active Directory and the services that depend on it, I will not be following the MS Project template in Appendix A.

To begin AD planning you need to go back a step and look more closely at the way you redesigned your domain structure. In order to do this, you need to run-through some definitions, which I expect you to already be familiar with. If you do not understand the following definitions, please stop and refer to one of the resources aforementioned in the section on research. All of the Windows domains in a particular namespace belong to what is called a Forest. Domains in a forest all have two-way transitive trusts and share a common schema. The schema is the blueprint for Active Directory; it determines the structure and properties of the Active Directory objects. Lastly, a Site is all of the computers on a subnet that have at least a 256kbps connection with each other with at least 128kbps of that connection free. To be clear, a site is not a part of Active Directory or Windows 2000 domains at all. Sites are the layout of the physical network that the forest and domains are built on.

All of these definitions are important to understand when you start looking at how replication will work in your planned network. Every DC in a particular domain is going to replicate the part of AD that pertains to its domain to every other DC in its domain. GCSs replicate the AD database for their domain as well as store pieces of information on the other domains and the information that is domain independent such as universal groups. The reason for this partial inter-domain replication is to speed up searching of the AD. Approximately 55% of the AD's size is GC data. This situation gets a little more complicated when sites are introduced. Intersite replication requires manual

configuration. Also, a workstation participating on a native mode Windows 2000 domain must be able to see a Global Catalog server in order to logon, thus one must be available on every site.

After having planned the general overview of your network and looked at how your DCs will replicate the Active Directory between each other, it is time to look at the specific organization of your new AD. Organizational units (OUs) are the containers AD uses for users, computers, printers, shared folders and many other objects including other OU containers. OUs are the main way in which authority is delegated in Windows 2000. OUs become even more important when you look at Group Policy. Group Policy objects (GPOs) can be assigned to OUs. This means that if you want a group of workstations to all be configured the exact same way, all you have to do is put them in the same OU and then create a GPO for that OU with all of your preferred settings. Each time the computer logs onto the domain, its GPOs will be applied.

Group Policy:

Group Policy is a combination of the Security Configuration Editor and System Policy tools of Windows NT 4.0. Configuring the security settings of your entire network is as simple as defining a GPO linking it to the OUs to which you want it to apply and clicking OK. At the next bootup, user logon, and/or scheduled interval the appropriate GPOs will be applied. Because GPOs are not linked only to OUs knowing the order in which they are applied is important: (1) the NT 4.0 system policies get applied, (2) the local GPOs are applied, (3) the site GPOs are applied, (4) the domain GPOs are applied and (5) the OU GPOs are applied.

The OUs' GPOs settings applied last override any conflicting settings made earlier. GPOs are applied in nested order thus, the innermost OU has precedence over the more general OU. Because a User logon takes place after the machine boots up, the GPOs for the user are applied after the GPOs for the computer and thus the GPOs for the user have precedence. This way, settings can follow a particular user or group of users from machine to machine. For machines where a GPO is defined that adjusts user type settings that you do not want replaced when a user logs in you need to enable "User Group Policy Loopback Processing Mode" with the "Replace" option. While group policy can do much more than set security policies and preferences this should be enough to get an initial idea on how to design your OUs.

In AD, the authority of every property of every object can be delegated. This is great security improvement over NT 4 because it allows you to more tightly control the power individual administrators have. Remember that disallowing permissions to be inherited creates orphaned objects in AD just as it does with NT file system. A network with lots of orphans becomes very difficult to manage very quickly. Remember, while setting up OUs around your needs to delegate authority, do not create OUs that are nested deeper than 5 levels. Logon times get longer with each GPO that has to be applied during boot and user logon.

Planning the location of your DNS and DHCP servers is very important but outside the scope of this paper. Remember the two January denial of service attacks on

Microsoft's network as a lesson that placement of your DNS servers is very important. If DNS does not work or is not available, your DCs will not be able to perform most of their functions.

Upgrading Workstations:

Determining when to upgrade your workstations is the next big decision in planning. Weighing the need to support legacy applications that will not run on Windows 2000 and all of the powerful features of the 2000 domain that can only be utilized by 2000 workstations is difficult. Not upgrading everyone leaves a handful of legacy machines that will be increasingly more expensive to support as you retrain your staff to administrate the new network. Windows 9x machines on your network will become relatively even more difficult to manage and more difficult to secure. The quicker all of your workstations can be upgraded the better.

Upgrading Network Services:

Legacy software is not only a problem on your workstations, your current backup software, network management software, and network based anti-virus products on your network servers will probably break when the domain switches to native mode. Replacing those systems are projects in themselves.

Microsoft Exchange, IIS, and DFS will not be covered in this paper. However, many issues with each of these pertain to AD and PKI and need to be thoroughly researched and planned. Refer to Andy Brock's practical assignment mentioned in the research section for an in-depth view of locking down your IIS boxes.

Planning your public key infrastructure (PKI):

General PKI concepts will not be covered here. More information can be obtained from Microsoft at http://www.microsoft.com/WINDOWS2000/library/operations/security/windows2000csoverview.asp. Then general planning decisions that need to be made start with determining how you intend to use your PKI. Once you know what you want to use it for, you can plan how you will structure it. Certificate Authorities (CAs) can be installed on any of your stand-alone or DC servers that participate on the domain by installing certificate services. In large organizations a hierarchy of CAs is generally used however, several models exist. If securing Internet E-mail is one of your goals, you will need to get a subordinate CA certificate from a trusted company like VeriSign for your root CA.

In planning your CA structure determining how certificates will be issued, who will be delegated authority over the different certificate servers, and how to secure the private keys will be the biggest design challenges. If you are going to use EFS, recovery agents, backup servers, and protecting the recovery agent's keys are the major design decisions that should be considered in developing your EFS strategy. Protecting private keys should also be incorporated into your security audits if a PKI is used. 100,000 bit encryption is only as strong as the measures that have been taken in protecting the private key.

Securing your new plan:

Planning your security is the final step before testing. Because security is a process that affects every facet of your plan rather than a patch or an encryption algorithm, I have decided to make it the last step of the planning phase. While Appendices B and C cover the check box, patch, encryption, and best practice information that is required to secure a 2000 network, this section is focused on the security process.

One of the largest security problems your plan has to deal with is the tendency of the implementers to create security holes while debugging problems. Because permission problems often look similar to program bugs or other configurations mistakes, administrators often create the security holes themselves. Documenting every setting for every server that deviates from your organization's standard security setup is necessary. Performing routine security audits on all of your machines is also necessary. Make your administrators accountable. It is important they know security is a concern of your organization, and that while being fair, consequences will result for administrators who allow known security vulnerabilities to exist in areas for which they are responsible.

The planning phase is also when you need to plan your new security audit procedures, they will also be tested during the testing phase of migration. While some systems need to be routinely audited, much of your organization's systems can be randomly sampled for auditing purposes. This process will be much easier with well-implemented GPOs. This is also a good time to determine what if any changes need to be made to the way hot fixes and service packs are tested and distributed. With GPOs and scripts it is possible to verify the current patch level of each machine and install fixes as needed. Remember these scripts will need updated each time a new update is released.

Test your plan:

Once your entire plan has been reduced to a stack of checklists, you are ready to plan your testing. It is highly likely that you have actually developed different variations of the same strategy and will use the test network with performance monitoring tools to determine which strategy will work better for you. Given the experimental nature of this testing and the amount of time a single run-through and restore requires, it is very important that each test be carefully planned. The trick is to test as many variables as possible without testing two variables that might affect each other.

Once your test network is ready and everything is documented and your test procedures are precise and efficient, you will most likely spend the first several tries fighting problems. Make sure everything is documented and any changes made are incorporated into the plan and checklists for future tests.

Testing your exit strategy:

Testing migration should present you with many natural opportunities to test your exit strategy as well. As mentioned before, having an exhaustively tested exit strategy developed for each step of the migration plan is required for a safe and secure Windows

2000 upgrade. The costs of backing out also need to be assessed during testing. The potential threat of losing user's SIDs or having to have all of your Windows 2000 workstations leave and rejoin the domain because of a botched upgrade needs to be quantified and calculated. This information will allow for more intelligent decision making later when problems actually occur during deployment.

The tools you used earlier with your proof of concept should now be used again as indicators of stability. The expected results from these performance monitors should be known and documented. As a checklist item, these performance monitors should be verified to be within a specified range at specific points during the test. These early warning indicators can help

The last test should be a pilot run. The entire migration should be like clockwork at this point and no changes should have been made from the previous successful run.

Deployment:

Deployment should go smoothly at this point if the previous steps have been executed correctly. If problems do occur during deployment, well-tested exit strategies can be used if necessary. Technical support arrangements made during the planning and testing stages should also be available to help during deployment. All training arrangements should have been performed and staff tested. Once goals of design plan have been implemented successfully the "as installed" system should be documented. Finally, feedback should be collected to help evaluate the perceived changes in the network.

Appendix A
Microsoft Project's Windows 2000 Migration Template

ID	Task_Name	Duration
1	**Microsoft Windows NT Server to Windows 2000 Deployment Template**	365 days
2	**Vision/Scope**	21.75 days
3	Evaluate Windows 2000 features	1 wk
4	Evaluate corporate business objectives	1 wk
5	Determine technology goals and objectives	1 wk
6	Formulate preliminary cost/benefit analysis	1 wk
7	Determine project scope (lab, pilot, international/regional deployment, coexistence strategies, etc)	1 wk
8	Determine major milestones	2 days
9	Secure executive sponsorship/funding	1 day
10	Vision/scope complete	0 days
11	**Planning**	72.25 days

12	**Assemble Project Teams/Define Roles**	5.5 days
13	**Core Roles**	0.5 days
14	Project manager	4 hrs
15	Infrastructure administrator	4 hrs
16	Deployment administrator	4 hrs
17	Desktop administrator	4 hrs
18	Intranet/internet administrator	4 hrs
19	Database server administrator	4 hrs
20	Browser administrator	4 hrs
21	Messaging administrator	4 hrs
22	Network administrator	4 hrs
23	Testing/quality assurance team	4 hrs
24	User education/training/communication	4 hrs
25	Logistics management	4 hrs
26	Core roles complete	0 days
27	Establish subteam roles and responsibilities (infrastructure, security, server, etc.)	1 wk
28	Assemble project teams/roles complete	0 days
29	**Detail Current Computing Environment**	10 days
30	Detail business organizational requirements	1 wk
31	Detail geographic considerations	1 wk
32	Detail key business processes	1 wk
33	Detail information architecture/flow	1 wk
34	Detail application requirements	1 wk
35	Detail technology architecture	1 wk
36	Detail server hardware and software inventory	1 wk
37	Detail client hardware and software inventory	1 wk
38	Detail current and future information technology standards	1 wk
39	Detail current administrative/service delivery model	1 wk
40	Document current computing environment	1 wk
41	Detail current computing environment complete	0 days
42	**Preliminary Design Objectives**	12 days
43	Map vision/scope to current computing environment	2 wks
44	Review preliminary design objectives with executive sponsor	2 days
45	Preliminary design objectives complete	0 days
46	**Identify Coexistence Strategies**	3 days
47	Identify interoperability issues within the company (operating systems supported, topology, protocol, etc.)	3 days

48	Identify interoperability issues with the organization's partners (topology, protocol, etc.)	3 days
49	Identify coexistence strategies complete	0 days
50	**Establish Test Lab Environment**	32.75 days
51	Review current configuration documents and define a lab model	2 days
52	Select one or more lab locations	1 day
53	Determine lab space and environmental requirements	1 day
54	Determine power and network connection requirements	2 days
55	Design and document logical and physical configuration for the lab	2 days
56	Determine hardware requirements	2 days
57	Determine software requirements, including business applications and tools	3 days
58	Determine who needs to use the lab	1 day
59	Determine database requirements	1 day
60	Determine wiring and network tap plans	1 day
61	Acquire hardware, including cables and software	3 days
62	Acquire workspace equipment, such as desks, chairs, white boards, cork boards, lamps, telephones, and shelving	3 days
63	Build and configure the network	3 days
64	Test network connectivity	1 day
65	Build and configure the servers	2 days
66	Install applications and build databases on the servers	2 days
67	Install testing and administrative tools	4 hrs
68	Build and configure the client computers	2 days
69	Install applications on the client computers	1 day
70	Test all the lab components	2 days
71	Assign a lab manager	2 hrs
72	Define a change control process for the lab	4 hrs
73	Create, test, and document the lab restore process	2 days
74	Establish test lab environment complete	0 days
75	**Perform Risk Assessment**	12 days
76	Identify mission critical applications	2 days
77	Identify and analyze potential risks	4 days
78	Quantify potential impact of the risk	2 days
79	Detail escalation processes	2 days
80	Document risk assessment	2 days
81	Risk assessment complete	0 days
82	**Define Communication Strategy**	13 days

83	Define communication strategy for each phase	3 days
84	Define audiences	1 day
85	Define communication delivery mechanism	3 days
86	Establish communication timeline	4 days
87	Document communications strategy/standards	2 days
88	Communication complete	0 days
89	**Define Education/Training Strategy**	9 days
90	Define education strategy for deployment demographics (admins, help desk, end-users)	2 days
91	Define education delivery mechanism	2 days
92	Establish education timeline by phase	3 days
93	Document education strategy/standards	2 days
94	Education complete	0 days
95	Planning complete	0 days
96	**Development**	148 days
97	**Evaluate Migration Strategies**	15 days
98	Determine your migration roadmap	1 day
99	Determine supported upgrade paths	2 days
100	Examine your existing domain structure	2 days
101	Determine the reasons for restructuring domains	2 days
102	Determine when to restructure domains	1 day
103	Determine your strategy for upgrading domain controllers	2 days
104	Determine the order for upgrading domains	2 days
105	Develop your recovery plan	2 days
106	Determine when to move to native mode	1 day
107	Evaluate migration strategies complete	0 days
108	**Active Directory**	69 days
109	**Active Directory and Domain Namespace**	56 days
110	Review Active Directory features	3 days
111	**Design Active Directory Forest Plan**	53 days
112	Determine the number of forests for the network	2 days
113	Define a forest change control policy	2 days
114	**Document Impact Considerations of Changes to Forest after Deployment**	3 days
115	Define schema change policy	2 days
116	Define configuration change policy	1 day
117	Document impact considerations of changes to forest after deployment complete	0 days

118	Document forest plan	2 days
119	Design Active Directory forest plan complete	0 days
120	**Design Active Directory Domain Plan**	12 days
121	**Determine the Number of Domains in Each Forest**	5 days
122	Evaluate single-domain model	3 days
123	**Evaluate Multiple Domains Model**	2 days
124	Evaluate preserving existing Windows NT 4.0 domains	2 days
125	Evaluate administrative partitioning considerations	2 days
126	Evaluate physical partitioning considerations	2 days
127	Multiple domains model complete	0 days
128	Assign a forest root domain	4 hrs
129	Assign a Domain Name System (DNS) name to each domain to create domain hierarchy	4 hrs
130	Plan a DNS server deployment	2 days
131	Optimize authentication with shortcut trusts	2 days
132	Document impact considerations of changes to domain after deployment	2 days
133	Design Active Directory domain plan complete	0 days
134	**Design Active Directory Organizational Unit (OU) Plan**	6 days
135	Define OUs to delegate administration	2 days
136	Define OUs to hide objects	1 day
137	Define OUs to apply Group Policy	1 day
138	Document impact considerations of changes to OU structures after deployment	2 days
139	Design Active Directory OU plan complete	0 days
140	**Design a Site Topology Plan**	26 days
141	**Define Sites and Site Links Using the Physical Network Topology**	12 days
142	Obtain physical network topology map	4 hrs
143	Create site for each LAN or set of LANs connected by high-speed backbone	2 days
144	Create a site for each location lacking direct connectivity (SMTP mail)	2 days
145	Record internet protocol (IP) subnets for each site	4 hrs
146	**Site Links**	7 days
147	Define site connections with site links	2 days
148	Define replication schedules	2 days
149	Define replication intervals	1 day
150	Define replication transports	1 day
151	Define link costs	1 day
152	Site links complete	0 days

153	**Define Server Locations Within Sites**	11 days
154	Define domain controller location per physical partition design	1 day
155	**Define Additional Domain Controllers**	6 days
156	Analyze failover requirements	3 days
157	Analyze domain controller client workload	3 days
158	Define additional domain controllers complete	0 days
159	Define location of global catalog servers	2 days
160	Define location of DNS servers	2 days
161	Document impact considerations of changes to site topology after deployment	3 days
162	Design a site topology plan complete	0 days
163	**Evaluate Synchronizing Active Directory with Exchange 5.5**	13 days
164	Examine your domain structure and Exchange site topology	1 day
165	Review your network for Active Directory Connector (ADC) deployment	1 day
166	Consider specific network requirements	1 day
167	**Determine Which Directory Service You Will Manage Objects From**	2 days
168	Evaluate Administration of Objects from Active Directory	2 days
169	Evaluate Administration of Objects from Exchange Server 5.5 Directory Service	2 days
170	Define objects for directory synchronization	2 days
171	Map Exchange containers with Windows 2000 OUs	1 day
172	Design connection agreements	2 days
173	Document your ADC connection plan strategy/standards	3 days
174	Synchronizing Active Directory with Exchange 5.5 complete	0 days
175	Active Directory complete	0 days
176	**Client Strategy, Standards, and Management**	40.5 days
177	Define client administration strategy	2 days
178	Define client application requirements based on job function	3 days
179	Define client configuration restrictions based on job function	3 days
180	Configure approved client hardware (laptops and desktops) to run Windows 2000	2 days
181	Configure basic Windows 2000 user interface options	2 days
182	Logon/logoff options	4 hrs
183	Start menu options	4 hrs
184	Desktop options	4 hrs
185	Multilanguage options	4 hrs
186	Accessibility options	4 hrs
187	Configure applications based on client requirements and administrative guidelines	1 day

188	Mandatory applications	1 day
189	Optional applications	1 day
190	Document client strategy/standards	3 days
191	**Change Configuration Strategy**	20 days
192	Define user and organization change and configuration management needs	2 days
193	Evaluate and select desired Windows 2000 change and configuration management features	3 days
194	Evaluate other applications for software distribution, etc. For example, SMS, Tivoli,)	3 days
195	Plan for using remote OS installation to install Windows 2000	4 days
196	Configure Group Policy to enable IntelliMirror software installation and maintenance	4 days
197	Configure server shares and Group Policy for user data management	2 days
198	Configure server shares and Group Policy for user settings management	2 days
199	Change configuration strategy complete	0 days
200	Client strategy, standards, and management complete	0 days
201	**Application Compatibility with Windows 2000**	37.5 days
202	Review detailed application inventory document	2 days
203	Consider reducing the number of applications you use and developing desktop standards	1 wk
204	Develop a system for prioritizing applications	2 days
205	Prioritize the applications by how critical they are to running your business	1 day
206	Write a test plan, including test methodology, lab and test resource requirements, and schedule	4 days
207	Develop a test tracking system for capturing and reporting test results	1 day
208	Schedule test events	1 wk
209	Test applications and record results	2 wks
210	Report on testing progress	2 wks
211	Resolve application incompatibilities	1 wk
212	Application compatibility with Windows 2000 complete	0 days
213	**Security Considerations**	64 days
214	Identify the security risks that apply to your network	1 wk
215	Assess solutions for identifiable security risks	3 days
216	Ensure that all access to network resources requires authentication using domain accounts	2 days
217	Determine what part of the user community needs to use strong authentication for interactive or remote access login	1 day
218	Define the password length, change interval, and complexity	1 day

	requirements for domain user accounts, and develop a plan to communicate these requirements to the user community	
219	Determine if public key security for smart card logon is required if strong authentication meets your security objectives	1 day
220	Define policy for enabling remote access services	2 days
221	Develop procedures/communication regarding remote access procedures, including connection methods	2 days
222	Define user groups and establish conventions for group names and how group types are used	3 days
223	Define the top-level security groups you intend to use for broad security access to enterprise-wide resources	1 day
224	Define your access control policies with specific reference to how security groups are used	2 days
225	Define the procedures for creating new groups and who will have responsibility to manage group membership	1 day
226	Identify which existing domains belong in the forest and which domains will use external trust relationships	1 day
227	Describe your domains, domain trees, and forests, and explicitly state the trust relationships among them	1 day
228	Define a policy for identifying and managing sensitive or confidential information and your requirements to protect sensitive data	1 day
229	Identify network data servers that provide sensitive data that might require data protection	1 day
230	Develop a deployment plan for using Internet Protocol Security (IPSec) for protection data for remote access or for accessing sensitive application data servers	2 days
231	If using Encrypting File System (EFS), describe your data recovery policy, including the role of recovery agent in your organization	2 days
232	If using EFS, describe the procedures you will use to implement data recovery process and verify the process works for your organization	2 days
233	If using IPSec, identify the scenarios for the way it will be used in your network and understand the performance implications	2 days
234	Define/communicate domain-wide account policies	3 days
235	Determine the local security policy requirements for different categories of systems on the network, such as desktops, file and print servers, e-mail servers, and define the Group Policy security settings appropriate to each category	3 days
236	Define application servers where specific security templates can be used to manage security settings, and consider managing them through Group Policy	2 days
237	Apply appropriate security templates for systems that upgrade from Windows NT 4.0 instead of a clean install	1 day

238	Use security templates as a means of describing the level of security you intend to implement for different classes of computers	1 day
239	Develop a test plan to verify your common business applications run correctly under properly configured secure systems	1 wk
240	Define what additional applications are needed that provide enhanced security features to meet your organization security objectives	1 day
241	State the levels of security you will require for downloaded code	1 day
242	Deploy internal procedures for implementing code signing for all in-house developed software that is publicly distributed	2 days
243	State your policies for securing the administrator account and the administration consoles	1 day
244	Identify the situations where you plan to delegate administrator control for specific tasks	1 day
245	Identify your policies regarding auditing, including staffing	2 days
246	Document security strategy/standards	1 wk
247	Security considerations complete	0 days
248	**Public Key Infrastructure**	19 days
249	Identify certificate requirements	2 days
250	Define processes for issuing certificates	1 day
251	Define certification authority trust hierarchy	2 days
252	Define security requirements for certificate authorities (CAs)	2 days
253	Define certificate lifecycles	1 day
254	Define certificate enrollment and renewal processes	2 days
255	Define certificate revocation policies	1 day
256	Define maintenance policies	2 days
257	Define disaster recovery strategies	3 days
258	Create design documents	2 days
259	Create a rollout plan and schedule	1 day
260	Public key infrastructure complete	0 days
261	**Member Servers Migration (Nondomain Controllers)**	7.5 days
262	Determine capacity planning	2 days
263	Plan for network interruptions	1 day
264	Read pre-install or pre-upgrade checklist	4 hrs
265	Read hardware checklist and Hardware Compatibility List (HCL)	1 day
266	Check third-party software compatibility	2 days
267	Document detailed member server migration strategy/standards	1 day
268	Member servers migration (nondomain controllers) Complete	0 days
269	**Terminal Services**	15 days
270	Select remote administration or server application mode	2 days

271	Determine licensing requirements	1 day
272	Determine how Terminal Services benefit the business environment	2 days
273	Document the existing computing environment	1 day
274	Develop a plan for implementing Terminal Services including networking, security, and domain structure	3 days
275	Establish guidelines and standards for server deployment including CPU, storage, and so on	1 day
276	Document detailed Terminal Services strategy/standards	1 wk
277	Terminal Services complete	0 days
278	**High-Availability Applications/Services (Clustering)**	28 days
279	Identify specific high-availability needs for mission-critical applications and services	2 days
280	Determine your cluster requirements	2 days
281	Identify the network risks	1 day
282	Address the network risks	1 day
283	Determine which applications to use with network load balancing	2 days
284	Perform capacity planning for network load balancing	2 days
285	Optimize network load balancing clusters	2 days
286	Identify component services or Microsoft Transaction Server (MTS) applications in your organization	1 day
287	Choose a component load balancing solution	1 day
288	Perform capacity planning for component load balancing	1 day
289	Test and tune the component load balance performance of your applications	2 days
290	Choose applications to run on a server cluster	1 day
291	Identify the network risks	1 day
292	Determine failover policies for groups	1 day
293	Choose a domain model	1 day
294	Choose a cluster model	1 day
295	Perform capacity planning for cluster service	2 days
296	Document clustering strategy/standards	4 days
297	High-availability applications/services (clustering) complete	0 days
298	**Storage Management Strategies**	9.5 days
299	**Evaluate Windows 2000 Disk Management Strategies**	1 day
300	Basic storage	4 hrs
301	Dynamic storage	4 hrs
302	Evaluate volume management	1 day
303	Evaluate mount points	2 days
304	Evaluate disk defragmentation strategies	4 hrs

305	Evaluate removable storage strategies	1 day
306	Evaluate remote storage strategies	1 day
307	Document storage management strategy/standards	3 days
308	Storage management strategies complete	0 days
309	**Remediate Risk Assessment**	7 days
310	Review risk assessment document	1 day
311	Identify solutions	3 days
312	Communicate to project sponsor, senior management, and project members	1 day
313	Evaluate risk as part of day-to-day project management	2 days
314	Remediate risk assessment complete	0 days
315	**Develop Communications**	11 days
316	Review communications strategy/standards	3 days
317	Develop communication materials	1 wk
318	Review communications materials	2 days
319	Approve communications strategy and materials	1 day
320	Communication complete	0 days
321	**Develop Education/training**	9 days
322	Review training strategy/standards	1 day
323	Develop/acquire training materials	1 wk
324	Review education materials	2 days
325	Approve education strategy and materials	1 day
326	Develop training complete	0 days
327	Development complete	0 days
328	**Proof of Concept (POC)**	30.5 days
329	**POC Preparation**	3.5 days
330	Prepare a test plan and checklists based on development/design solutions	3 days
331	Document features and components to test	2 days
332	Secure resting personnel	4 hrs
333	**Ensure the Testing Lab Environment Simulates the Proposed**	3 days
334	Server hardware and drivers	2 days
335	Services and configurations	1 day
336	User accounts	1 day
337	Domain structure (simulated domain hierarchy)	2 days
338	Server function/strategy	2 days
339	Mixed environment	1 day
340	Client computer configuration	2 days
341	Network topology and protocols	2 days

342	WAN connectivity	2 days
343	Remote connectivity	1 day
344	Peripherals	3 days
345	Interoperability with other operating systems (UNIX, mainframe, etc.)	3 days
346	Administrative tools	1 day
347	Fault tolerance techniques	2 days
348	Terminal Services	2 days
349	Ensure the testing lab environment simulates the proposed complete	0 days
350	POC preparation complete	0 days
351	**Deploy Development Solution to POC Lab Machines**	20 days
352	Perform tests to test plan specification	2 days
353	Analyze results	4 days
354	**Mitigate Results**	14 days
355	**Test Case Problem**	14 days
356	Document in POC tracking system	3 days
357	Revise test case	3 days
358	Rerun the test	3 days
359	Document results/changes	1 wk
360	Test case problem complete	0 days
361	**Lab Setup Problem**	6 days
362	Document in POC tracking system	1 day
363	Follow lab change control process	1 day
364	Reconfigure lab	1 day
365	Rerun test	1 day
366	Document results/changes	2 days
367	Lab setup problem complete	0 days
368	**Development/Design Problem**	4 days
369	Document in POC tracking system	1 day
370	Escalate development/design issues	1 day
371	Prioritize/risk analysis	1 day
372	Track resolution	1 day
373	Development/design problem complete	0 days
374	Deploy development solution to POC lab machines complete	0 days
375	**Perform Full-Cycle Risk Assessment**	7 days
376	Document lessons learned	3 days
377	Document modifications	2 days
378	Address readiness to proceed to pilot	2 days
379	Perform full-cycle risk assessment complete	0 days

380	POC complete	0 days
381	**Pilot**	55 days
382	**Planning**	24 days
383	Identify pilot scope and objectives	4 days
384	Identify pilot groups/individuals/resources/equipment	2 days
385	Document resources and tasks	2 days
386	Develop communications materials for user community (FAQs, Web site, e-mails, etc)	1 wk
387	Develop the user support plan	3 days
388	Develop the training plan	4 days
389	Ensure POC lab stable	2 days
390	**Develop the Rollout Process**	14 days
391	Identify tools and supplies the installer needs	2 days
392	Identify lists of scripts and their location	3 days
393	Identify Backups to be taken prior/during Deployment	1 day
394	Document steps for migrating to the new domain structure	3 days
395	Document steps for performing manual and automated computer upgrades	2 days
396	Document installer acceptance tests	2 days
397	Document operational procedures installers and administrators are to perform (resetting permissions, changing passwords, etc.)	3 days
398	Document steps for backing out if pilot fails	3 days
399	Develop the rollout process complete	0 days
400	Identify known risks and contingency plans for them	2 days
401	Develop rollback plan	2 days
402	Pilot planning complete	0 days
403	**Deployment**	12 days
404	Communicate with pilot users	4 hrs
405	Conduct user training	1 wk
406	Ensure support organization is prepared	4 days
407	Prepare pilot site or sites	2 days
408	Deploy the rollout process	1 wk
409	Pilot deployment complete	0 days
410	**Evaluate the Pilot**	8 days
411	Conduct desktop test scenarios	1 wk
412	Conduct server test scenarios	1 wk
413	Conduct third-party application test scenarios	1 wk
414	Conduct custom application test scenarios	1 wk

415	Conduct coexistence test scenarios	1 wk
416	Identify scope changes	3 days
417	Identify cost factors	2 days
418	Identify interoperability issues	3 days
419	Identify unanticipated downtime	2 days
420	Pilot test complete	0 days
421	**Post-Pilot Evaluation**	11 days
422	Obtain user feedback	1 wk
423	Evaluate lessons learned	2 days
424	Modify items as necessary	2 days
425	Document recommendation for next steps	2 days
426	Post-pilot evaluation complete	0 days
427	Pilot complete	0 days
428	**Deployment**	25.5 days
429	**Communications**	2.5 days
430	Review communications strategy document	2 days
431	Start communications	4 hrs
432	Communications complete	0 days
433	**Education/Training**	11 days
434	Review education/training strategy document	1 day
435	Conduct administrative training	1 wk
436	Conduct user training	1 wk
437	Education/training complete	0 days
438	**Domain Migration**	13 days
439	Review domain migration strategy/standards document	2 days
440	Restructure existing Windows NT 4.0 domains	1 wk
441	Upgrade PDC to Windows 2000	4 hrs
442	Upgrade BDCs to Windows 2000	1 day
443	Upgrade resource domains	1 day
444	**Member Server Migration**	3 days
445	Review member server migration strategy/standards document	1 day
446	Backup files on servers to be upgraded	4 hrs
447	Upgrade member server	4 hrs
448	Test member server on network	1 day
449	Member server migration complete	0 days
450	Establish trusts	4 hrs
451	Domain migration complete	0 days
452	**Active Directory**	3.5 days

453	**Synchronizing Active Directory with Exchange 5.5**	3.5 days
454	Review ADC connection plan strategy/standards	1 day
455	Set up connection agreements	4 hrs
456	Test connection agreement configurations	1 day
457	Determine a schedule for directory synchronization	4 hrs
458	Back out of a synchronization in progress	4 hrs
459	Synchronizing Active Directory with Exchange 5.5 Complete	0 days
460	**Security Infrastructure**	4 days
461	Review security strategy/standards document	4 hrs
462	Create secure boundaries	1 day
463	Deploy strategies for everyone	4 hrs
464	Deploy strategies for company staff	4 hrs
465	Deploy strategies for users of company applications	4 hrs
466	Deploy strategies for partners	1 day
467	Security complete	0 days
468	**Public Key Infrastructure**	10 days
469	Review public key strategy/standards document	1 day
470	Providing training and support for production users	1 wk
471	Install Cas	4 hrs
472	Install/configure support systems or applications	4 hrs
473	Configure the certificates to be used	4 hrs
474	Configure certificate revocation lists publication	4 hrs
475	Configure public key Group Policy	4 hrs
476	Configure certificate renewal and enrollment	4 hrs
477	Issue certificates to users, computers, and services	1 day
478	Public key infrastructure complete	0 days
479	**High-Availability Applications/Services (Clustering)**	6.5 days
480	Review high availability applications/services (clustering) document	1 day
481	Optimize Windows 2000 cluster service	1 day
482	Choose tools to help you automate the deployment of Windows 2000 cluster service	4 hrs
483	Optimize your clusters	1 day
484	Plan for fault-tolerant disks	1 day
485	Test server capacity	1 day
486	Plan a backup and recovery strategy	1 day
487	High-availability applications/services (clustering) complete	0 days
488	**Storage Management Strategies**	8.5 days
489	Review storage management strategy/standards document	1 day

490	Review business requirements for storage	4 hrs
491	Design storage management solution	2 days
492	Design storage utilities (backup, restore, defragmentation)	1 day
493	Design disaster recovery plan	2 days
494	Document storage management strategy/standards	1 day
495	Storage management strategies complete	0 days
496	Switch to native mode	1 day
497	Deployment complete	0 days
498	**Post-Implementation Review**	12 days
499	Obtain user feedback	1 wk
500	Evaluate lessons learned	4 days
501	Modify items as necessary	2 days
502	Establish ongoing infrastructure planning team	1 day
503	Post-implementation review complete	0 days
504	Microsoft Windows NT to Windows 2000 Deployment Template complete	0 days

Appendix B
Known Security Issues During Install

MS00-099 "Directory Service Restore Mode Password"

Vulnerability: The "Configure your server" wizard, when used to promote a machine to a domain controller, sets a blank Directory Service Restore Mode password. To exploit this bug a hacker would require physical access to the machine, which shouldn't be possible for a Windows 2000 domain controller anyway.
For more information visit: http://www.microsoft.com/TechNet/security/bulletin/MS00-099.asp

Frank Monroe reported an issue involving the unattended installation of Windows 2000 using the OEMPreinstall option where permissions are improperly set such that the All Users and Default Users directories are writeable by unprivileged users.

While Windows 2000 is being installed, the network interfaces are configured and started before the Administrator password is applied and someone could connect to one of the administrative shares without a password. I was able to confirm this bug by typing in "net use x: \\ipaddress\c$ "" /USER:"Administrator"" during the installing components phase of installation. Microsoft discusses the issue (Q260927) Read Armoring NT by Lance Spitzner to learn one technique that would solve this and other similar problems. You can find Armoring NT at http://www.net-security.org/text/articles/spitzner/armoring_nt.shtml

Another setup password issue has to do with the asterisk *. If you start a password during installation with an asterisk, either in attended or unattended mode, the password will be blank. This is because the asterisk is what Windows 2000 uses to symbolize a blank password. Knowledge base article (Q257442) discusses the issue further.

Appendix C
Best Practices for Administering and Configuring a Windows 2000 Network.

General Best Practices

- Service Pack before you install. (Q271791)
- Migration is a good time to reevaluate all of your security policies. If your security policy is such that it is more difficult for your users to do their jobs, they will take actions that will compromise security policies, like writing down their password and taping it to their monitor. When that happens, you have effectively created a weak policy. If your environment is such that security needs are very high, then make sure security education is a part of each employees' training. Reminding employees periodically about the company's security practices is good way of ensuring that employees know what they should be doing.
- Runas.exe is a wonderful tool and a security improvement to Windows 2000. This utility allows you to run programs in the context of another user. This is useful for administrators who follow the best practice of having two accounts, one with administrative powers and one without, and use the normal account to log in to their computer. With runas.exe you can run a particular administrative program with your administrative account without having to logoff and log back on. This is also useful for users who need local administrative access to their workstations. They too can have normal user accounts and run programs in the context of the local administrator without having to be inconvenienced.
  **Recognize that the runas.exe utility has some vulnerabilities and should not be used in certain cases. This utility when used can in some cases allow a user to escalate privileges on the network and the local machine. Specifically, these problems are linked to Internet Explorer's window reuse feature and a FrontPage bug. However, this problem probably applies to many other applications and will hopefully be fixed in the next service pack.
- Use network time synchronization. This is valuable when you are digging through event logs. It is also important for Secure DNS updates to work properly.

Pre-Domain Upgrade Best Practices

- Upgrade RAS, tape backup, network management, and any other critical servers that use null user sessions. This is almost required but definitely good sense. If for instance, you plan to upgrade your backup server during domain migration and the backup server upgrade failed, you would be unable to continue backups even if the rest of the migration went smoothly.
- Secure physical access to your BDCs. Because of the multi-master nature of domain controllers in Windows 2000 mentioned earlier, it is important to make sure that these

machines have places that they can be moved to if they are currently in insecure environments.

Domain Upgrade Best Practices

- Do not upgrade only one Domain Controller if you have Windows 2000 of any version already deployed on your network. Once a Windows 2000 computer authenticates with a Windows 2000 domain controller, it will not be able to authenticate with an NT 4.0 domain controller unless it leaves and rejoins the domain. Additionally, because of this, special load considerations need to be made. Since all of the already deployed Windows 2000 machines will be authenticating only to Windows 2000 DCs, you need to plan for that demand on these servers.
- During installation, deploy the high encryption pack and keymigrt.exe on all domain controllers. This will improve the security that all of your services will use.
- Once all DCs have been upgraded, use Group Policy to require strong session keys and digitally encrypt secure channel data for the secure channel.
- Enable auditing on all DCs \NTDS and \SYSVOL folders.
- Separate the FSMO roles across your DCs. At a minimum put the RID Master and PDC Emulator roles on different computers.

DNS/Namespace Best Practices*

- Do not use your company's registered DNS domain name for your Windows 2000 root domain. Instead, use a subdomain such as windows.anycorp.com.
- Require secure dynamic updates. If non-secure updates are allowed, everyone has access to change any record they choose.
- Reserve DNS records for critical machines manually by creating the DNS record and then locking down the permissions with AD Users and Computer so that it cannot be changed later.
- Do not install DHCP on a domain controller and configure DHCP to only update if client requests or if the client does not support dynamic updating.
- If all DNS zones are AD-integrated, disable zone transfers on all DNS servers.
- Secure your DNS server's against cache pollution.
- Log the "notify" and "update" events and increase the size of DNS log file.

Active Directory Best Practices*

- Do not enable schema changes on the FSMO schema master until required.
- Only temporarily add administrators to the Schema Admins group when changes need to be made, remove when done.
- Use the restricted groups feature of Group Policy to enforce proper membership in the Schema Admins group, audit changes to this group.
- Use inheritance as much as possible and avoid creating orphans.
- Try not to modify the general default OU structure too much.
- Try not to use the specific permissions too much. Keep things simple follow the NTFS read, change, full control permissions.

PKI Best Practices*

- Protect your private keys:
    - Install the high encryption pack on workstations before they request certificates.
    - Install the high encryption pack on certificate authorities before the certificate service is installed.
    - Use keymigrt.exe to force then encryption of private keys in protected storage.
    - Use syskey.exe to move the system key off the CA.
    - Use the "Store Private Key with Strong Protection" option and require a password, whenever it is accessed.
    - Enforce strong password policies for all users who will be getting certificates.
    - Use smart cards to store private keys.
    - Root and intermediate CAs should be installed as off-line stand-alone CAs. Never connect these computers to the network and do not allow them to participate on the domain. Store hard drives in a safe place when not in use.
    - Do not allow users with roaming user profiles to have private keys, especially not EFS recovery agents.
    - Lock down the local \RSA and \Protect profile folders so that only the owner and administrators can access them.
    - Require authentication, encryption, and a strong session key on secure channels with group policy.
    - Do not attempt to use EFS to encrypt private keys or any file with the system attribute.
- EFS specific best practices
    - Change the default recovery agent, export the private keys of the new agents to secure media, and delete the recovery agent's private keys from all computers. Keep multiple copies of the agents' private keys, with at least one copy offsite and secure.
    - Consider having more than one recovery agent. A single enterprise-wide recovery agent key could be stored off site in a box with two locks where one key is given to one administrator and a different administrator keeps the other key. Then recovery agents for each OU could be assigned and their keys could be secured as needed based on the sensitivity of information in each respective OU.
    - After creating new recovery agents, set permissions on the EFS Recovery certificate template to deny access to everyone. Administrators will be able to take ownership and change permissions when needed. Remove the template from the Policy Settings container in the CA snap-in for all CAs. Enable auditing of all access to the template.
    - When exporting recovery keys save them as PFX files and use the "Delete Private Key If Export Is Successful" option.
    - When creating EFS recovery agent certificates, use the "Strong Private Key Protection" option and require a password whenever the agent's

private key is used for Recovery. Write the password down and store it with the exported key.
  - Do no use recovery agent accounts for anything except recovery.
  - Try to encrypt folders rather than files. Because of the transparency of EFS naming folder "Secured" or "Encrypted" should help. My Documents and its subfolders is a good folder to encrypt.
  - Encrypt the TEMP and TMP folders to make sure plain text files are not leaked there.
  - The paging file cannot be encrypted but with group policy this can be cleared when the system shuts down. This may be a bit extreme for normal workstations but is a great idea for laptops that have a high potential for being compromised.
  - Encrypt the spool folder. \%systemroot%\System32\Spool\Printers

Helpful Tools (unsorted)*

- movetree.exe is a utility that allows you to move users, groups, and computers from one Windows 2000 domain to another, preserving permissions and access rights.
- Cloneprincipal scripts are a set of scripts that allow you to mirror a forest to another forest, in terms of users, computers, groups, and SIDS. The scripts are Clonepr.dll, Clone-gg.vbs, Clone-ggu.vbs, Clone-lg.vbs, Clone-pr.vbs, Sidhist.vbs, AdsSecurity.dll and AdsError.dll
- Netdom.exe is a command-line utility for managing NT 4.0 domain trusts and the netlogon channels they use.
- Ldifde.exe and csvde.exe are command-line utilities which can connect to a DC using LDAP and import/export data using attribute and object filters, the latter using comma-delimited files.
- DSACLS is a command-line utility for managing AD permissions
- Enumprop.exe is a command-line utility for listing AD permissions on objects and containers.
- Review the Windows 2000 resource kit and support\tools folder on the Windows 2000 installation media for more scripts and tools.

*These sections, though paraphrased, are from Jason Fossen's books referenced immediately following.

Credits and References

Windows 2000 Active Directory. Alistair G. Lowe-Norris. O'Reilly, January 2000.

Windows 2000 DNS. Roger Abell, Herman Kneif, Andrew Daniels, Jeffrey Graham. New Riders, April 2000.

Windows 2000 Active Directory, DNS, and Group Policy. Jason Fossen, The SANS Institute GIAC Training, 2001.

Windows 2000 PKI. Jason Fossen, The SANS Institute GIAC Training, 2001.

Windows 2000 Hot New Vulnerabilities. Jesper Johansson, The SANS Institute GIAC Training, 2001.

Building an Enterprise Active Directory Notes from the Field. Microsoft Consulting Services. Microsoft Press, March 2000.