Peregrine

Desktop Inventory
Planning Guide

For use with Desktop Inventory 8.0

Peregrine
SYSTEMS®

Preface

The guide provides an insight into some of the concepts and ideas behind planning an IT asset inventory. As such it is recommended reading for anyone planning on conducting an IT asset inventory using Desktop Inventory.

Organization of This Guide

This guide is separated into three areas:

Chapter 1: IT Asset Inventory Principles

This chapter outlines some of the basic concepts behind IT asset inventory and what you will need to consider when planning an inventory.

Chapter 2: Planning and IT Asset Inventory

This chapter provides steps that will help bring into focus some of the issues that you may face when planning your IT asset inventory.

Chapter 3: Inventory Planning Form

This chapter contains a preformatted example inventory planning form that you can use as a starting point and customize to suit your organization's needs.

Knowledge Requirement

As a Desktop Inventory user, you need a basic knowledge of the environment in which you are working (Windows 95/98/2000/NT/XP or UNIX).

Contacting Peregrine Systems

For technical support on this or any other product from Peregrine Systems, Inc., refer to the Customer Support Web site at:

http://support.peregrine.com

Contents

1 IT Asset Inventory Principles

CHAPTER

This section provides information on how Desktop Inventory can be used to collect, analyze and maintain current computer inventory data.

You will find information on the following topics:

- What are IT assets
- What is IT asset inventory
- Purposes for conducting an IT asset inventory
- Overview of planning the inventory

These are key concepts that are important to understand before proceeding with an inventory.

What are IT Assets?

An IT asset is any piece of IT equipment or software that your company owns or leases. These assets will become part of your IT asset inventory.

Hardware IT Assets

Examples of your hardware IT assets are:

- Desktops
- Workstations
- Servers
- Portable devices (laptops, PDAs)
- Printers
- Modems
- Monitors
- Keyboards
- Scanners
- Routers
- Bridges
- Switches

Software IT Assets

Your software IT assets are the software and applications that are being run on computers in your organization. Examples of software IT assets are:

- Commercially available software applications
- Proprietary software your company has produced
- Information stored in files

What is IT Asset Inventory?

An IT asset inventory consists of identifying all desktops, laptops, peripherals and servers within your organization and then detecting and collecting their physical configuration and software contents.

An IT asset inventory is conducted for a number of reasons, including licence compliance, but is also an opportunity to gain beneficial information and effective control of costly IT assets.

With accurate and complete IT asset inventory data you can use the data:

- To control and monitor cost.
- As a valuable company resource for other departments such as Service Management and Technical Support.
- To reconcile with the data you may already hold in your central asset repository from a purchasing point of view. For example, reconciling purchase records and actual staff.
- For data management. Keeping track of versions of electronic price lists for consistency, keeping track of databases for business continuity etc.
- To perform spot checks to ensure all changes within an IT asset's life cycle are recorded.
- To manage hardware and software resources efficiently. This results in more effective user support, software purchasing, licensing and better hardware utilization.
- To detect and solve problems such as software piracy, computer pornography and other abuses.
- As a mechanism to ensure compliance with internal standards for software application licensing.
- To standardize maintenance procedures.

Purpose of Conducting an Inventory

It is important to consider various business drivers in order to maximize the benefit of each inventory pass. Once inventory information is available within an organization, interested parties begin to request information for their particular needs. Consider the needs of the following:

- Technical Support (Helpdesk)
- Asset management
- Software licensing
- Business continuity
- IT: Disk and file maintenance
- Disk grooming
- Platform upgrading
- Version control tracking

Helpdesk

Helpdesk inventory data usage can include:

- User and machine information
- Software versions
- Configuration files
- Change control

Inventory data facilitates Helpdesk by:

- Reducing time spent managing users
- Detecting problems earlier
- Giving users better service

Many Helpdesk products offer a link to view the inventory data file. This enables support staff to view the contents of a machine and implement resolutions to the problem.

An after-work inventory performed on a computer allows the Helpdesk to maintain an accurate record of its configuration.

Asset Management

Asset management inventory data usage can include:

- User and machine information
- Software versions
- Change control

This data can be used to:

- Analyze the computer estate
- Reduce software license infringement and down-time
- Improve asset management and utilization
- Improve supplier leverage

Asset management products require a minimum set of data fields to populate database files. Traditionally, these products have focused on hardware information. Today, more and more products are also concerned with the software assets.

Business Continuity

Data necessary for business continuity is:

- User and machine information
- Software versions
- Change control

This information is used to:

- Use stored files to aid computer configuration
- Check restored data for versioning

Business continuity is an important aspect of asset management. One concern is recovering machines critical to the organization, after a failure. Another issue, is change. As users are re-deployed within an organization, knowing their previous equipment capability makes it easier to assign a machine with the same or better specification. If new equipment is needed, the previous specifications are available.

By comparing the inventory of a rebuilt machine with its original fingerprint differences in software versions and additional data files can be highlighted. When an inventory is complete, an accurate status of changes in assets, hardware, software or deployment can be maintained. Key files can be embedded into the inventory data so that they are available from an alternative resource to the specific machine.

IT: Disk and File Maintenance

To assist IT in disk and file maintenance, consider the following data:

- Current configurations
- File lists
- Rollout program progress

Disk Grooming

Inventory data provides disk grooming information, such as:

- Duplicate file and application installations
- Multiple versions
- Small and empty files
- Unbalanced directory structures
- Mixed data and program directories
- Space available on accessible drives

Disk drives tend to accumulate superfluous files, such as, old versions of programs, more than one copy of a local file and old installations that were incompletely removed. Empty and small files consume at least 1K of disk space per file, and even the contents of the recycle bins can impact disk space.

Duplicate applications can have licensing implications. Some vendors do not permit more than one version of their software on a computer without an additional license. This can happen when upgrades are installed and a previous version remains on the machine during the migration period.

Applications, particularly graphical and multi-media applications, consume a significant amount of disk space. If applications are to be migrated to a server, then it is vital that odd data files are not mixed with the executable files as they might be given access rights preventing user updates.

By making periodic inventories, disk usage can be tracked and remedial action taken. This will help users organize data more effectively and increase their productivity.

Platform Upgradings

Inventory data facilitates platform upgrading in:

- Determining current configurations
- Comparing current configurations with target requirements
- Controlling rollout programs

When upgrading software or migrating data, it is necessary to know the current and the target configurations. By comparing current and inventory data with target requirements, it can be determined which machines meet specifications, which need to be upgraded and which need to be replaced. Re-inventory of machines after they are upgraded can identify what 'standard builds' are compromised and provide a check on the progress of a rollout program.

Software Licensing

Inventory data can be critical to:

- Identifying applications and versions
- Producing summary counts
- Updating software indices for local applications
- Checking license breaches

Due to the number of phases involved in the process, software licensing needs to be handled as a specific project. Since many applications occur as software suites, inventory data is useful for matching software licenses to application counts and can help companies avoid the over-purchasing of licenses.

Establishing ownership of software may require input from sources such as suppliers. Even if unlicensed software is detected, the user should not hesitate to consult suppliers. Software publishers are generally pleased to know that users are taking steps to mitigate the problem.

Virus Impact Assessment

Inventory software is not a replacement for virus detection; however, an important use of inventory data is to check the current version of the anti-virus software deployed. Sometimes the most current version is not fully deployed leaving the computer unprotected against new viruses.

Inventory data provides support information for virus detection. For example:

- If a boot sector virus has been detected and cleaned, it may leave that boot sector inoperable. A standard inventory embeds a copy of the boot sector in the data it collects, and this information can be used to rebuild the damaged sector.
- Some viruses create a time stamp of 62 seconds. The file list can be searched for such an occurrence.
- Some viruses create or rename files. By knowing the file names, a search can be undertaken.
- If a file has been infected, it's size could have changed. Re-running the scan may result in different data being produced.

Reusing Inventory Data

Once inventory data is collected, it is necessary to keep the data current. Managing upgrades is one re-use of inventory data, others are:

- Producing management reports of product usage
- Cutting out non-essential product evaluations
- Supplier leverage

Overview of Planning the Inventory

For an inventory to be successful, front-end analysis should be done to fine-tune the objectives, determine the ultimate use of the data and specify exactly what data is needed. Well conducted front-end analysis coupled with effective project management practices ensures the successful implementation of the IT asset inventory with minimum disruption to your business.

Basic Questions

There are a series of questions that you must ask yourself in order to identify what is necessary for a successful inventory.

Why   Why is the inventory being performed?

Is it to gain a better understanding of the computer population of the company?

What
- What data is needed? Is it hardware data, software data or both?
- What specific user information is needed (for example, first name, last name, department, floor)?
- Is information on peripherals like CD burners or scanners needed?
- Does specific information need to be extracted from the registry, DMI layer or environmental variables on the machine?
- Do specific files such as **autoexec.bat**, **win.ini** or **boot.ini** need to be copied to facilitate your Helpdesk in the future?
- Which computers and servers are going to be included in the inventory?

Overcoming the data mountain
Data requirement selection is an on-going process. It takes place:
- Before the inventory
- During the inventory
- After the inventory

When
- When is the inventory scheduled for?
- Is there a time frame for the completion of this inventory?
- Is this a one-time inventory, or will it be continual?

Basic rule: MADC – Moves, Additions, Deletions, Changes

Apart from the logistical considerations of when to conduct the initial inventory, the golden rule for an inventory is: If there are any changes in your population, perform an inventory.

Ensuring effective recording processes is an important part of asset management. Inventory data can act as an electronic change control record.

How
- How will the initial and subsequent inventories be performed?
- Will the initial inventory be a walk-round inventory, or will it be conducted over a network?
- Are there adequate permissions in place to gain access to a network share to execute a Scanner or deposit the collected data?
- Is there an asset numbering scheme in place, allowing each computer and monitor to have its own unique identifier?
- Will employees be notified of the inventory and how will they be informed?
- Is the computer population networked to facilitate subsequent scheduled automated inventories?
- Will data be migrated to a larger asset management application for permanent housing, such as Peregrine AssetCenter?

Where
- If the inventory is performed by a walk-round to each computer, where are the computers and servers located? Are they located on one floor, one building or multiple sites? If they are located at different sites, how far are the sites from one another?
- Are there any security clearance issues facing the inventory team?

Who
- Who will be responsible for the inventory? The IT department? Finance? Facilities?
- Who is responsible for moves, additions, changes and deletions of property?

Overcoming the Data Mountain

At the start of the inventory, the exact data requirement may be unknown. Once the user begins looking at the inventory data, there is a temptation to start investigating all sorts of ancillary issues. For example, what about those stored outdated computers? As a result, the people performing the inventory may mistakenly employ the 'if in doubt, inventory it' approach.

While there may be a short-term tactical need for specific information, or the inventory might be an opportunity to gather information that is difficult to capture, redundancies can be eliminated by ascertaining exactly what information needs to be extracted.

For example, machines awaiting disposal may not need to be inventoried, but may simply need manual asset recording. Also, consider whether mice and keyboards need to be recorded.

As a general guideline, focus on achieving specific objectives before investigating special interests. If the data collected is not going to be maintained, then its inventory capture should be questioned.

The goals of an IT Asset Inventory

The major goals of an inventory might be:

- Listing all known applications – indicating how many licenses are needed.
- Listing all unknown software – highlights any threats.
- Reporting asset deployment – assists with asset management.
- Listing all computer and server hardware – aids in future upgrade plans.

2 Planning an IT Asset Inventory

CHAPTER

The steps outlined in this chapter will help bring into focus some of the issues you may face when planning your IT asset inventory. You will find information on the following topics:

Step 1: Identifying Your Existing Data Collection Process and Current Environment

Throughout your organization you will find that different departments will be using different methods for the collection of their data.

For example:

- Your HR department may be using a spreadsheet that contains all the data for employees (Employee names, functions, departments, software contracts etc.).
- Your IT department may use an in-house database that contains data on the machines the company owns.

Identifying existing data collection methods is also an important first step in identifying the data needs of your various departments.

The Current Environment

- Have previous scans been undertaken?
- Are there any existing electronic identifiers?
- Are there any facilities for application deployment?
- What percentage of machines are networked?
- How many servers?
- What operating environment do they use?

Step 2: Planning the Collection of This Data

The data collection processes identified in Step 1 will become a source of one-time input into your repository.

Step 3: Designating and Training Members of Staff for the Maintenance of the Data

You must designate tasks to employees who can ensure that the data accuracy and consistency is maintained regularly.

In order to ensure data accuracy and consistency, both across the organization and over time, it is important that ownership of these issues is assigned early in the process.

These tasks must be considered a vital part of the overall asset management effort, as accuracy of the data is an absolute requirement if later analysis is to be of significant value.

It is vital that there are staff nominated as contact points to answer both project and technical questions. There may be more than one person in each category depending on the size of the project.

Step 4: Deciding What Data is Needed and Determining How to Source That Information

You will need to take a detailed look at the data that is required and then determine how you will source that information - electronically or manually.

Bear in mind that the data needs will be different from department to department. Step 1 will have already provided some indication as to what these departmental data needs are.

This can have a significant bearing on how a project is undertaken and the amount of data to be collected. Also consider whether the data will be forwarded to other applications, if so, how is this envisaged.

Most data requirements have the following lowest common denominators:

For a User
- Name
- Department
- Location

- Phone
- Cost center

For an IT Asset
- Asset number
- Product maker
- Product name
- Product serial number or other identifiers

In addition, data from the following groups are often of interest:

- CPU
- Disk
- Cards, etc.

Further Information
For information on what data the Scanners collect refer to the document entitled 'Data collected by the Scanners'.

Step 5: Configuring the Scanners

Configure a Scanner that collects this data for the various platforms used by the computers in your company using Scanner Generator.

Note: Hardware detection is fast - typically 10-30 seconds. The main areas that need configuring in Scanner Generator are Software and Asset data collection. For almost all purposes, you can use the default Hardware detection settings.

If possible, avoid configuring more than one Scanner for each platform. Running different Scanners for different departments can become a labour intensive exercise and should be avoided if possible.

Further Information
For more information on creating customized Scanners, refer to the Desktop Inventory User's Guide.

Step 6: Creating the Asset Questionnaire

Mandatory (Required) Asset Questionnaire fields provide you with an opportunity to keep certain data items consistent.

When carrying out the initial IT asset inventory we strongly recommended that the asset questionnaire is filled out. The questionnaire data should automatically be refilled each time the scan is executed to maintain consistency in the data collected.

You will need to decide which fields should be **Required**. This provides a means of ensuring that data is consistent and adheres to a standard. This is especially relevant when you want to transfer the data to an asset management system such as Peregrine AssetCenter.

For example, the Scanner Asset Questionnaire can be configured so it is **Required** to have the following fields filled-in:

- Asset tag
- Employee
- Department
- Location
- Telephone extension

Note: Required means that the field cannot be left blank.

The Asset tag field must be a Required field in the Asset Questionnaire because it uniquely identifies a particular IT asset.

Further Information
For more information on creating customized Scanners, refer to the Desktop Inventory User's Guide.

Step 7: Deciding How You Will Gather the Data

Use a combination of walk-round and automated methods when carrying out your initial inventory. This will ensure that you capture the most accurate, up-to-date and complete data.

For both automatic and walk-round inventories, keep a separate record of how many scans were launched and how many were successful, so that any exceptions can be monitored and dealt with.

The Scan Repository

Regardless of whether you carry out a manual or automated scan, the scan files will end up in your repository. The repository should be designed to hold all your scan files and should be cleaned up periodically.

Further Information

Refer to the Desktop Inventory User's Guide for more information on the various methods used for gathering inventory data and the deployment of Scanners.

Automatic Inventory

This type of inventory will allow you to collect information about hardware and software assets and pinpoint basic information about where those assets are located, who is logged into them, and what operating systems they are running on etc.

This information can serve as the basis for the initial walk around inventory as it helps define and establish "what is there".

The Scanners are distributed to individual machines. You can set up a schedule using command-line options or login-in scripts dictating which machines should be scanned and at what frequency. The retrieved scan files are placed in a central repository.

You can then use the data for use in asset management systems, such as Peregrine AssetCenter.

Further Information

Further information on how Desktop Inventory is used to deploy Scanners is covered in detail in the Desktop Inventory User's Guide.

Manual Inventory

A walk-round inventory captures data about assets that are not connected to your network (i.e. stand-alone).

In these cases a floppy disk with the Scanner executable will ensure that all important configuration items about that PC (such as installed software, and hardware), monitors and Asset Tags, etc. are known.

During the course of the inventory you may come across unused and surplus assets. These surplus assets can be re-deployed to other employees or should be properly removed from the inventory.

A walk-round inventory also allows each asset to be physically inspected. The state of the machine can then be stored in an asset field.

The results of the Scan should then be saved to the central repository.

Step 8: Creating and Maintaining a Set of Methodologies

Inventory capture is not a one time event.

Once the initial asset inventory and asset reconciliation is complete, you should create and maintain a set of processes that are designed to keep your inventory up-to-date.

- Any time a machine has had changes made to it, for example, software and hardware upgrades, it has been allocated to another member of staff etc., a scan should be initiated.

  The fields about the user and asset can then be updated and automatically reconciled again against the data in your asset management system for example.

- Spot-check practices should be established that verify automatically-collected data samples for accuracy.

- Non-networked assets must have a process for the manual entry of new data initially and then follow-up inventories must also ensure that these assets are included and the data is kept up-to-date.

- Scans should be run on networked systems at least once monthly to keep the data about these systems up-to-date.

Re-inventory

The regularity of re-inventory depends on a number of factors, including:

- How often assets change condition - moves, upgrades, additions etc.
- How often information needs to be reported. For example, is it necessary to perform a daily inventory check if the results are only reported quarterly?
- How often the people in charge are likely to have the time to look at it.
- What it is used for.
  - If for asset management - then rarely
  - If for services/support - then more often.

3 Inventory Planning Form

CHAPTER

This chapter contains a preformatted example inventory planning form that you can use as a starting point and customize to suit your organization's needs. You will find information on the following topics:

- The inventory planning form - overview
- Instructions for completing the planning form
- The inventory planning questionnaire

The Inventory Planning Form - Overview

The planning form serves three purposes:

- Determines what data is to be collected and how it will be used.
- Determines the user asset information that will be recorded along with the electronically collected hardware and software information.
- Extracts the information necessary to plan the logistics of an inventory.

See page 33 for a preformatted example inventory planning form that you can use as a starting point and customize to suit your organization's needs.

The Desktop Inventory scanning software records three types of information from each scanned machine. The combined information is stored in a scan file which is unique to each scanned machine and is suffixed **.fsf** or **.xml.gz** (depending on how you configured your Scanner).

The user asset information is either entered manually at the computer screen during the scanning process or data can be extracted from electronic resources such as text files or Windows registry.

Typically the information recorded as User Asset data is that which cannot be detected electronically and might include the following:

- name of the user
- user's department
- location
- make, model and serial number of the computer and attached peripherals.

Instructions for Completing the Planning Form

This planning form is the first step in defining the requirements for an IT asset inventory project. Depending on how the project is to be implemented, further requirements will need to be defined to deal with the detailed logistics. For example, site access for engineers, security clearance etc.

General Questions

Question	General instructions
Project staff details	On projects such as these, there is often a project co-ordinator who is separate from the technical resource.
	The technical resource needs to be someone who has the necessary skill and access rights to set up directories and files at the correct level.
Inventory Objectives	Pinpoint the business drivers for conducting the Inventory. Include as little or as much information as you want. This can be used to list the information you seek to gain from the project
Project Timing	An inventory project is not an instantaneous event. Sufficient time needs to be given to the development of a deployment plan as well as testing.
	If the data is required for other parts of a larger project, the sooner the work is started the better.
	Inventory should progress in parallel with the rest of the project, rather than being left as an afterthought.
	The business driver should be specified so that interfacing to other parts of a project can be evaluated to see if the time-scale is realistic.
Current Environment	What is currently available for asset identification and for deploying software such as Scanners?
	It is important to identify if any existing facilities are available that can be used in the new project.
	Unique asset identification is crucial to differentiate machines. If nothing exists, then time and effort needs to be given to considering how this identification is achieved.
	Manual entry of asset data is the most obvious route but becomes impractical with large volumes.
Site information	Knowing the split of locations and the estimate of machines at each site is necessary to establish how much work is required at each site and the amount of space required for storage of the data.
	This leads to discussion of whether all the data is stored locally at each site and uploaded in bulk or push all the data back to one central repository.

If the data is to be uploaded, how fast are the network connections?	Checking whether there is any anti-virus or other security software running is important because it can have a profound impact on the speed of the scan.
	If a file has to be opened for signature, a real-time Scanner would intercept the request and check the file before releasing it for scanning.
	To avoid opening a file it may be necessary to configure the scanner to ignore file information. In this instance directory information about the file would still be captured – file name, size, attributes etc. but version information would not be captured.
What Data is to be collected?	The Scanner can be designed to run completely hidden from the user, minimized or as full screen display.
	If hidden or minimized, then if there any required fields that have not been populated, the scan will display a message prompting the user for input.
	If the Scanner is to be run full screen, there is the option to have an information screen that can be used to provide information to the user on what is happening.
	This can be augmented with a bitmap for a company logo etc. This is limited to 64Kbytes.
	The next choice is how fast to run the Scanner. It can either be run full speed to complete the scan as quickly as possible, or at low priority to minimize performance degradation for other applications. Electronic scans can be undertaken on Intel chip based PCs, HP/UX, Solaris, Linux and AIX.
	However, additional information can be recorded manually for asset management purposes. Items such as stand-alone printers, scanners, modems can be recorded manually.
	The Scanner can be configured to select various combinations of Hardware, Software and Assets.
	For example, the first scan of an asset may only be concerned with Asset Information and Hardware details. Whereas, some machines may only require a Software scan on subsequent rescans.

■ **Hardware**
Normally, the default selection of all hardware tests data is sufficient. The tests take very little time to run and unless there is a known problem it is best to leave the settings as they are.

■ **Software**
The software choices determine how many and what types of files to both scan and store in the resulting scan file. Exclusions may be because of known scanning problems with a particular file.

To assist with software recognition, it is useful to have at least one sample set with signatures. The file signature is a calculation on the first 8K bytes of a file. This requires the file to be opened. If the file is opened, then it is also possible to extract the version information (same as properties under Windows). This header information can provide vendor and application details.

The Scanner has the ability to store the contents of ZIP files as directories. This allows the display of the file names that have been compressed, but it cannot extract version information or open the individual compressed files.

■ **Asset Information**
Asset information is either manually entered data or data that has been extracted from files and/or Windows registry. The type of data entered here is user or product information that is not stored electronically. To help with data entry, picklists can be created to provide pre-defined options for data entry. For subsequent scans, the asset data can be read from a previous scan file and loaded into the fields.

■ **Stored Files**
These files can be embedded in the scan file. They are usually configuration or other data files.

Scan Admin	Knowing how often the scan is run will identify traffic flow and when the transfer activities will take place. If there are any current network performance issues, these need to be understood before additional activity is added to the current load.
Special conditions?	Special users, remote or standalone need to be considered along with any non-working equipment. You may decide to leave these out or perform the work manually.
Are there any issues concerning site access?	Consider whether there might be physical constraints when gaining access to the sites. Are parking facilities available?
Are passes required for access?	Are passes needed for access to locations within the sites. Are swipe cards used? Will they be made available to your project team members?
Access times	Check access times for your inventory team. You can often expect that access can only be granted to certain locations/departments outside of these times. This can assist with estimating the time taken to complete each site and hence the overall project.

Computer Population Details

Question	General instructions
Total population	Enter the total number of workstations and servers that are to be included in the inventory project. Also include whether this number is believed to be accurate to within 5%, 10%, or greater.
Percentage Networked	Indicate the percentage of machines that are, or are likely to be network connected during the inventory.
Approximate Number of machines with 5.25" of 720K DD Drives	Indicate if there are likely to be any machines that have only the older 720K DD 3.5" drives or 5.25" drives. This is relevant for manual scans only. The Scanner is usually run from 1.44 Mb 3.5" HD disks.
Number of Laptops	Indicate the approximate number of laptop within the overall population. Often special arrangements need to be made to ensure that these are on site during the period of the data collection.
Predominant Makes and Models	Make extensive use of drop-down pick lists when entering the user asset data during the scan. This ensures maximum consistency of the information entered. Consider the contents of these pick lists and typically these will include the makes and models of the computers, monitors and peripherals within the population.
Operating Systems (% of populations)	The scanning software can be configured for the following operating systems: Dos, 16 bit Windows, 32 Bit Windows and OS 2. Indicate the percentage of differing operating systems, i.e., Dos, Win 3.x, Win 95, Win 98, NT x.x, and OS 2. From this you can determine the number of different Scanners likely to be needed.
Network Types	Include the network operating software and speed of network if available.
Policy on passwords	Indicate whether power on (boot-up) and/or screensaver passwords are used. If possible, consider not only company policy but the likelihood of individual departments/persons making use of them.
If NT will "audit" logins be provided?	In order to fully scan NT machines, local administrator access rights to the machine are required.
Security Software Installed?	Indicate whether security software is installed which would prevent an executable file from being run from the floppy drive. If such software is installed, identify.
Floppy disk locks in place?	Indicate whether floppy disk drive locks are fitted. Also consider whether any of the floppy drives might be either disabled or not-connected.

Asset Labels

Each scan file needs to be uniquely identified during the data collection. The easiest and most efficient way of doing this is to use an asset number assigned to that equipment.

If you do not have a system of asset labelling in place you might like to consider introducing one during the data capture, as the labels can be fitted as each PC is visited.

The Inventory planning questionnaire

Client Details and Contacts

Client name	
Address	
Phone	
Project Contact	Name:
	Phone:
	Email:
Technical Contact	Name:
	Phone:
	Email:

Reasons for Data Collection

1	
2	
3	
4	
5	

Project Timing

Desired start date for project

Target implementation date (move to Production)

Business driver for target date

The Current Environment

Is there an existing asset control system in place with unique identifiers?   Yes ☐ No ☐

If yes, is this information stored electronically?

If no, what identifier is to be used?

Is there an existing software deployment system in place?   Yes ☐ No ☐

If yes, what system?

If no, how are applications distributed currently?

Site Information

Locations

1

2

3

4

5

Locations	1	2	3	4	5	Total
Workstations						
PCs DOS 3.0 – 6.22						
PCs Win 3.x (Win16)						
PCs Win 95/98/NT/2000 (Win32)						
Solaris workstations 2.5, 2.6, 7, 8						

HP/UX workstations 10.2, 11.0
Linux Kernel v2.2, 2.4
AIX 4.3, 5.0
Servers
NT Servers
Netware Servers
Site totals

Note: Novell Netware servers need to be scanned in two phases.

1. Assets and Hardware only after downing the server and restarting under DOS.

2. Software only scan – if volumes compressed, run scan without signatures

Data Storage Estimates

If sample files are available from previous scans, use their average size as an indicator.

Locations	1	2	3	4	5	Total
Workstations						
Mbytes/ Workstation						
Servers						
Mbytes/Server						
Site totals Mbytes						

Do all client machines map through to the target server? If No, how many servers are involved?	Yes ☐ No ☐
Any Anti Virus/ Security products which may impact audit?	Yes ☐ No ☐
Are there high speed network connections between sites?	Yes ☐ No ☐

Data Collection

How is scanner to be run?	Full o Minimized o Hidden o

If scanner run Full screen	
Front screen information	Yes ☐ No ☐
If yes, show detail	
Bitmap (Max size 64Kbytes)	Yes ☐ No ☐
If yes, filename	
Speed of scan execution	Full ☐ Minimized ☐

Scanner Configuration

Hardware only	Yes ☐ No ☐
Hardware, Assets	Yes ☐ No ☐
Hardware, Assets, S/W	Yes ☐ No ☐
Software only	Yes ☐ No ☐

Hardware

Use default setting of all tests?	Yes ☐ No ☐
If No, which tests to remove?	

Software

All file data to be stored, only Executable files, Selected files	All ☐ Executables ☐ Selected ☐
If Selected, which file types?	_____; _____; _____; _____;
Any specific exclusions?	Yes ☐ No ☐
If yes, detail files and/or directories	
Will file scan include signatures?	Yes ☐ No ☐

If Yes, will version information be extracted?	Yes ☐ No ☐
Will ZIP files be stored as directories?	Yes ☐ No ☐

Assets

Field descriptions and field order can be altered to suit the client situation

Pick list is a list of entries from which a user can choose.

Sample Scanner Configuration

Asset Entry Screen Fields	Data Type	Content
Description (22 chars max)		
Scan File Description	Combination	
User Name		
Ext. Number		
Department	Pick list	
Site	Pick list	
Network Port Number		
Building	Pick list	
Floor	Pick list	
PC Asset No		
PC Type	Pick list	Desktop/Laptop
PC Make	Pick list	
PC Model	Pick list	
PC Serial Number		
Monitor Asset No		
Monitor Make	Pick list	
Monitor Model	Pick list	
Monitor Serial Number		
Peripheral Type	Pick list	Printers/Modems/Scanners
Peripheral Asset Number		
Peripheral Make	Pick list	

Peripheral Model

Peripheral Serial Number

Files to be Collected by the Scanner

Default files collected

Config.sys, Sms.ini, Drvspace.ini, Autoexec.bat, System.ini, Win.ini, Boot.ini, Infrtool.ini, Exclude.fp, Net.cfg, Protocol.ini

For UNIX

fstab, group, hosts, inetd.conf, inittab, profile

File	Location	String for file extract

Scan Administration

Where are scan files to be stored?

Where are Scanners to be stored?

How often will the scan be run?

Any current network performance problems?

What systems will be fed with scan data e.g. [Connect-It]?

Special Considerations

Contractors/Special Users

Are they to be scanned?   Yes ☐ No ☐

Contractors/Special Users

If yes, will a restricted Scanner be used?	Yes ☐ No ☐
Any other considerations?	

Remote Access Users

Are they to be scanned?	Yes ☐ No ☐
If yes, will a restricted scanner be used?	Yes ☐ No ☐
Any other considerations?	

Standalone Users

Are they to be scanned?	Yes ☐ No ☐
If yes, will a restricted scanner be used?	Yes ☐ No ☐
Any other considerations?	

Non-operational equipment

Are they to be scanned?	Yes ☐ No ☐
If no, will data be captured manually?	Yes ☐ No ☐
Any other considerations?	

July 6, 2004