

IMAGINE THAT YOU HAD TO DO A “SUDDEN DEATH” PC AUDIT?

IMAGINE you are an auditor in an organisation covering a large number of PC's

The manager has just asked you to verify that the software installed across the organisation is legal and authorised.

You embark on the audit using one of the many audit tools at your fingertips and start discovering the following widely occurring across the PC base as you conduct audits;

- Many PC's do not have any longer the Standard Operating Environment (SOE) that was rolled out ages ago, with Y2K efforts been and gone.
- The software installed seems to be varying wildly between PC to PC depending on the needs and Internet access levels of the user.
- There seems to be a large amount of “additional software” installed since the last time an audit was done.
- There seems to be software that has changed or has even been deleted since the last audit.

..... and so on.

The reality dawns on you that it is almost impossible to identify what is installed, whether it is legal or not can only be determined by examination of end-user licence agreements, and evidence of purchase etc

Other reality issues to face are;

- The effort required by you and your team is immense in terms of analysing the results of the audit and identifying and naming the files
- It is going to be very hard to justify and explain to management, stakeholders, directors that it is hard to control the desktop unless you take the draconian step of locking down the desktop to deny all extra access to the system base.

Imagine if you had to do a "sudden death" audit of PC's in your organisation?

.... as in, you have had a raid by the anti-piracy police who are looking for illegal software.....
.....they can do this via an Anton Pillar order from a court of law.

How would you verify what has been added since the last audit was valid and legal?

You know that the hardest part about doing software audits is the baseline keeps changing on you as soon as you have conducted the audit!

Of course this assumes you have been doing regular audits on your PC's..... haven't you?

If the organisations you deal with and consult to have concerns over illegal software being installed on PC based systems then this may be of vital interest to you and them.

There is a solution!

AUDIT-Baseline is an affordable audit software tool that enables auditing BY EXCEPTION both hardware and software and provides automatic naming of executable files (to the extent that is afforded by current vendors) with the capability to provide a detailed comparison report which shows ADDITIONS, CHANGES and DELETIONS to both hardware and installed software between audit cycles!

AUDIT-Baseline is not an audit lockdown tool in the sense that it will lock or delete data etc, it simply highlights in the first instance the configuration of a workstation/server on production (both hardware and software).

This software can be loaded to a workstation on build, or rollout of a Standard Operating Environment and a printout delivered to the end user client with the PC detailing exactly the base hardware and software state on delivery. The IT Manager then has a baseline configuration status of his assets. The end-user also can be made aware that what has been delivered will be monitored at irregular intervals “by exception reporting”.

The product then can be used at a later stage as part of a normal administrative task to audit the configuration of machines in the future.

This audit would be a standard 5% of the client base check - or something along those lines. This secondary audit is a differential audit, and will highlight changes from the last audit as taken.

Therefore the IT Manager or Auditor can:

- a. Determine any hardware configuration changes to the workstation/server and ensure these have been authorised
- b. Check for any software additions -
 - i. Ensure all software as added is licensed
 - ii. Ensure that software has been added against a set rollout/configuration change
 - iii. Ensure no software has been loaded that has components that may affect the operation of a SOE (ie changed .dll files etc)

Asset management is a difficult task. The use of this product can have far reaching affects within an organisation when realisation hits that the IT manager has visibility of what is on a machine (which after all is a company, not personal asset). This should reduce administrative overheads, prevent the loss/theft of hardware, lower piracy rates, remove offensive or inappropriate software etc. Of course if a user deletes the software the manager can also ask why?

Make sure you check out the power, functionality and capability of AUDIT-Baseline at <http://www.pcprofile.com/baseline.htm>

You can DOWNLOAD an interactive tutorial on AUDIT Baseline at http://www.pcprofile.com/Audit_Baseline_Overview.exe

The FULL user manual can be downloaded here http://www.pcprofile.com/USER_Manual_AUDIT_Baseline.PDF (Acrobat Reader is required)

Sample reports from live audits are located at; <http://www.pcprofile.com/samplelreports.zip>

For the first time you will be able to LOWER your costs of doing software audits and reduce your risk of being caught with illegal and unauthorised software.

There is an example of a comparison report located at http://www.pcprofile.com/AUDIT_Baseline_Comparison_Report.PDF generated between two separate audits at different times of the same PC and this shows clearly the additions, changes and deletions. AUDIT-Baseline uses the same naming and detection technology as AUDIT-Manager WITHOUT the use of any database naming technique.

You should be able to LOWER the cost of repeated audits using AUDIT-Baseline!

AUDIT- Baseline

(PC Software Compliance Auditing by exception)

IF YOU WANT TO LOWER THE COST OF REPEAT

AUDITS ON PC's THEN AUDIT-Baseline CAN ASSIST THAT GOAL!

NAMING & IDENTIFYING FILES

If you are auditing PC's containing Windows 3.1, 3.11, Windows NT 3.51 or 4.0, some application details may not be retrievable by **AUDIT-Baseline**. Application executable's version information is identified using standard Windows naming conventions and where applications do not follow this format then it is NOT POSSIBLE to have this detail identified and displayed. To assist you in this manner the audit file generated (yyyymmdd.RTF) will show files first by IDENTIFIED APPLICATION name, and then will list those files detected BUT NOT named.

OTHER POINTS OF REFERENCE:

How To Tell If You Have Genuine Microsoft Windows Branded Product

=====

In the ongoing fight against anti-piracy, Microsoft OEM have launched the following "How to Tell" campaign to assist organisations to easily recognise genuine Microsoft Software through features such as the Certificate of Authenticity (COA) label and the edge-to-edge CD-ROM hologram: For more information, visit: <http://www.microsoft.com/piracy/howtotell/how/e2e.asp>

Anti-Piracy & Auditing Articles

Busted - Anti_Piracy news you need to hear! <http://www.pcprofile.com/busted2.htm>

Your PC Isn't a Patch on what it used to be! <http://www.pcprofile.com/patches.htm>

"One in 3" - Software Management Issues <http://www.pcprofile.com/1in3.htm>

and

Hands-Up for Year 2000!

Getting caught with illegal software will cost you!

Will your PC survive the Year 2000 bug if you have illegal software?

Microsoft Aust offers \$AUD 5,000 reward for "dob-in-a-pirate"!

Software Copyright & You

16 Steps to Software Compliance

Accountants

CD Writer increases risk of illegal software

The above are all accessible from <http://www.pcprofile.com/sitemap.htm>

Copyright © 2000 Rob Harmer Consulting Services Pty Ltd PCProfile, AUDIT Baseline, AUDIT Manager, Software Inventory System are all registered business names and trademarks of Rob Harmer Consulting Services Pty Ltd A.C.N. 053 134 400 A.B.N 77 053 134 400 All Rights Reserved Worldwide.