Global Information Assurance Certification Paper

How to check compliance with your security policy

Introduction:

In an age were security is becoming more important to many organisations, it is important for such organisations to document their security policy, just as they would document their marketing policy, client service policy or accounting policies.
But the effort of just documenting policies is insufficient, since it is no use going through the effort and costs of developing a security policy and not implementing or updating it.
By that same token once it is implemented, it is no use not monitoring compliance with the policy.

Control Objectives for IT Governance (Cobit) refers – Appropriate procedures exist to ensure policies and procedures are being complied with.

Infoworld article – "Policy over policing" indicates that security policies should be enforced via regular audits.

White paper on "Why Security Policies fail" indicates that performing regular audits helps ensure the success of your security policy implementation.

The three sources cited above indicate that not monitoring is a recipe for failure of your security policy.

- **Who is responsible for checking compliance with a security policy**

  RFC 2196 – Regular compliance with the security policy should be performed by persons independent of defining or implementing the security policies.

  As cited above the persons responsible for monitoring compliance with the security policy should be independent of the persons implementing the policy. The concept of independence dictates that the person performing the work should be seen to be independent from any relationship to the item in question. This allows the monitoring to be unbiased.

  The business unit which best fits this profile are the internal auditors. The internal audit department would also be unable to make any decisions based on the findings and as such the report of findings should be forwarded to a management level that is capable of enforcing that the policy is complied with in all respects.

  From a logistics and cost perspective, Internal audit are constantly involved in performing audits at various branches or departments of larger organisations. To add an additional aspect of checking security policy compliance would seem logical and cost effective.

  Thus it is crucial to add checking of security policy compliance to the Internal audit scope.

- **How to design audit procedures based on a security policy**

Compliance procedures ensure that the control is operating e.g.
Control -The e-mail policy dictates that all mail must be scanned for executable attachments.
Operation of control - There must be a mail content scanner in use that searches for the above condition.
To check compliance with the above control the Internal Auditor would review the rules included in the content scanner to ensure that it makes provision for executable attachments.

The International Auditing Standards dictate that compliance procedures commonly used are as follows:

a. Inspection: Involves examining records, documents and tangible assets. E.g. Reviewing backup logs to ascertain if there were any unsuccessful backups.
b. Observation: Physically looking at a procedure being performing by other persons. E.g. Observing physical access control to the server room.
c. Computation: In the accounting environment this involves checking the mathematical accuracy of information. However, in the security policy compliance environment, the procedure involves using security tools like Omniguard, ISS system scanner, Kane or Bindview to ascertain the security vulnerabilities in the operating system. These findings can be compared to the organisations security policy on operating system configuration.
d. Analytical procedures: Involves analysing information to detect trends. Once a trend has been established the internal auditor would look for deviations from the trend. E.g. Analyising the Intrusion Detection System log with a data extraction and analysis tool like IDEA or ACL to ascertain a trend. Any item that does not comply with the trend indicates that there could have been an intrusion.

Example:

Security policy:
NCSA security policy on backups:
User and production systems are backed up frequently. Scratch and temporary areas are not backed up. Backup tapes are stored in alternate secure areas.

Compliance Procedure:
Inspect the backup schedule to ascertain the frequency of the backups. Inspect the backup log to ascertain what was backed up. Ensure that the backup excluded scratch and temporary areas.
Observe the area where backup tapes are stored to ensure that it is secure. Inspect the manual log to ascertain if the backup tapes are sent to secure areas to be stored. Confirm with the personnel at the

alternate secure area that the backup tape from the department in question is stored with them.

- **How to assess the risk of non-compliance:**
  Once internal audit has performed the compliance procedures, an audit report on the findings has to be issued. However, the report has to provide meaningful information. In certain environments there may be numerous findings and it is not possible for management to implement all the security policies within one period. In these environments, the report has to list the risk of the findings. This allows management to prioritise and implement the policies addressing the areas of the highest risk.

  The risk manifests itself in the threat or vulnerability that faces the organisations IT infrastructure e.g. an overfull audit log that results in a denial of service.

  The risk would be based on the amount of loss to be incurred by the organisation if the security policy item were not implemented. Loss can be categorized as follows:

  1. Loss of valuable information e.g. Losing debtors balances may impede the ability to collect the outstanding debts.
  2. Loss of assets or increase in liabilities e.g. A malicious hacker processing payments to himself via the electronic banking facilities of the organisation.
  3. Loss of reputation e.g. Litigation against the client due to inaccurate advertising material being posted on their site. This would lead to a loss of reputation in the market place.
  4. Loss of profit e.g. Design specifications being leaked to competitors. This would lead to a loss in market share which manifests itself in a loss in sales. Hence this affects profitability.

  Real life example:
  My client is a mining foundry and they place a large value on the design of their articles. Thus they go to great lengths to secure the server which hosts the Computer Aided Design program. This server is also used to store design specifics. Only engineers are allowed access to this server and all designs are encrypted. If this server had to be compromised they would lose market share as their competitors would gain access to their designs and this would impede their ability to stay in business.
  They also have tons of metal which has a large monetary value, but they don't go to great lengths to protect information regarding the metal as this is not as important as the design specifications.

  The moral of the story is that an asset does not have to be of a large monetary value to be of significance to the organisation.

- **Miscellaneous Items**
  Besides checking compliance with the security policy, it is just as important to review the procedures surrounding the update and review process of

the security policy. E.g. Ensuring that a site updates their backup policy to include new hosts.
It is also important to follow up on previous findings to ensure that management has been proactive in implementing outstanding policies.

- Sample Compliance Program

No.	Security Policy Item	Compliance Procedure	Checking Compliance on NT	Checking compliance on Windows 2000	Checking compliance on Linux/Unix
1.	Backups				
	Ian Soapy should perform full backups weekly and incremental backups daily.	Review the scheduler to ascertain when full and incremental backups are scheduled. Compare the schedule to the security policy.	Review the AT/WINAT command. To display the scheduled tasks type in the following command: AT \\ LOCAL > c:/schedule.txt Where local is the name of the server and schedule.txt is the name of the output file. Review the output file to ensure the following appears: Every M fullback.bat Every T,W.Th,F incbak.bat Review the ASCII file of the fullback.bat and incbak.bat files to ensure that they have been appropriately written for full and incremental backups respectively.	Review the 2000 GUI scheduler. Ensure that an entry exists for a full backup weekly and incremental backup daily. Path: Start/Settings/ Control Panel/ Task Scheduler/ Ensure that Backup is one of the scheduled tasks. Review the backup schedules by double clicking - on the incremental backup scheduled task and ensure the following: Run = Incremental Schedule = Daily - On the full backup scheduled task and ensure the following: Run = hc:off /m normal	Review /etc/cron.daily and /etc/cron.weekly. Ensure that the dump command is set to run as follows: In the daily cron schedule – Dump with levels 1-5 and In the weekly cron schedule – Dump with 0 level.

				Schedule = Weekly.	
	Two copies of the backups must be made. DLT tapes are to be used for the backup operation.	Observe the backup process to ensure that two copies of the backups are made and that DLT tapes are used.			
	The tapes must be labelled as follows: Date: Type: Full/incremental Host backed up: Hostname Drive backed up: C/D/E	Observe the labelling on the tapes to ensure that it has been labelled appropriately.			
	One copy of the full and incremental backup should be sent off-site to the Security storage vendor.	Confirm with the security storage vendor whether a copy of the backup is sent offsite.			
	The other copy of the full and incremental backup must be stored in the fireproof safe.	Inspect the fireproof safe to ensure that one copy of the backup is stored in here.			
	A manual log of the backup should be maintained with the following	Review the manual log of the backups to ensure that it is			

	information: Successful Unsuccessful Tapes overwritten by accident When and where tapes taken offsite Attempted and successful restores Bad tapes.	maintained with the appropriate information.			
2.	Password and Account Policy				
	Passwords must: Be a minimum length of 8 characters, Have a mixture of alpha, numeric and special characters, Be changed every 30 days, The last 5 passwords cannot be reused. Account lockout is after 3 bad access attempts.	Review system settings to ensure that the password restrictions are implemented. Compliance with these settings can be identified by using a tool like Kane and Bindview (for NT and 2000 servers) or ESM Omniguard and ISS System Scanner (for NT, 2000 and Linux/Unix servers).	Review the account policy (path: Start/Programs/ Administrative Tools/User manager for domains/Options) on the NT domain controller to ensure the setting is as follows: Password length = 8 characters Password History = 5 previous passwords Account lockout = 3 bad attempts Lockout duration = Forever until administrator unlocks Maximum password age = 30 days.	Review the password policy (path: Start/Run, type Gpedit.msc, OK – Computer Configuration/ Windows settings/security settings/account policy/password policy). Ensure the following: Password history = 5 passwords remember Maximum password age = 30 days Minimum password length = 8 characters Passwords must meet complexity requirements = enabled User must log on to change password = enabled Review the account lockout policy (path: Start/Run, type Gpedit.msc, OK – Computer	From root, run Linuxconf as follows: [root]#linuxconf Review the password policies under User account/policies/ Password and account policies. Ensure the following: -minimum length for the password = 8 characters -Number of non-alpha characters = 2 -Must change after # days = 30

				Configuration/ Windows settings/security settings/account policy/lockout policy). Ensure the following: Account lockout duration = 30 minutes Account lockout threshold = 3 invalid logon attempts Reset account lockout counter after 30 minutes.	
	Passwords must not be written on post-its and stuck to the monitor.	Walk through the office and observe if any users have post-its or other pieces of paper attached to the screen. Enquire from those users whether the post-its or other pieces of paper have the passwords.			
	Names should not be used as a password. Passwords should be developed using the first or last letter of each word in a phrase and to substitute certain alphabets with	Enquire from a sample of users their process of establishing passwords. Compare their responses to the security policy.			

	numbers e.g. To be or not to bed 2BON2B				

Sources:

1. "NCSA Security Policies and Procedures", March 19, 1998, http://www.ncsa.uiuc.edu/people/ncsairst/Policy.html
2. "Request For Comments 2196", September 1997, http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html
3. Enterprise Computing, "Policy over policing", August 19, 1996, http://archive.infoworld.com/cgi-bin/display\
4. Control Data, "Why Security Policies Fail", 1999, http://www.cdc.com
5. Information Systems Audit and Control Association, "Control Objectives for IT Governance", IT Governance Institute, July 2000
6. Chamber, Andrew, et al. "Auditing the IT environment – Assessing and measuring Risk and Control", Pitman Publications, 1994
7. Linda Locher, et al. "Microsoft Windows 2000 Security Technical Reference", Microsoft Press, 2000
8. Red Hat, "Red Hat 6.2 Manual", http://www.redhat.com
9. Charles Perkins, et al. "MCSE: NT Workstation Study Guide", Network Press
10. International Auditing Statements, "Statement of Auditing Standard's"