Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Implementing/Re-Implementing Change Control Policies

All network environments change over time, whether the change is planned or unplanned. Change Control Policies help to minimize the inadvertent creation of security openings when implementing planned, unplanned, or recovery changes to a company's network environment. All companies have some form of production environment. Depending on the type of organization, there might also be staging and development environments as well. Change control is essential in all environments. A change in a staging or development environme...

Copyright SANS Institute
Author Retains Full Rights

AD

DEEPARMOR®

# Implementing/Re-Implementing Change Control Policies

Derek P. Milroy (Assignment version 1.2e)

All network environments change over time, whether the change is planned or unplanned. Change Control Policies help to minimize the inadvertent creation of security openings when implementing planned, unplanned, or recovery changes to a company's network environment.

All companies have some form of production environment. Depending on the type of organization, there might also be staging and development environments as well. Change control is essential in all environments. A change in a staging or development environment that creates a design flaw will typically be replicated to the production environment. Lack of change control policies for all environments can cause flawed configuration changes or code enhancements in the production environment.

Another danger to production environments is disaster recovery situations. If changes made to a production environment are not properly documented, as per a change control policy, systems that have been recovered might be put into production without having been properly hardened. Without proper change control procedures in place, systems could be placed back into production after planned maintenance has been performed, without having been properly secured. This happened to Western Union. A procedure that included the use of a QC checklist, prior to placing the system back into production, could have prevented the incident. [1]

Implementing change control policies should be done with the same basic methodology as a technology implementation. All implementations can be broken down into four steps/phases: **A**nalysis, **D**esign, **I**mplementation, and **F**ollow-up.

## Phase I – **A**nalysis:

The starting point for analyzing a network environment, in preparation for implementing change control policies, is to learn the IT Department's structure. Understanding the structure of an IT Department is the first step towards learning an organization's IT workflow. Prior to recommending policies, which will in turn be used to create procedures [2], a thorough understanding of how changes are currently made is necessary.

Depending on the size of a company, there could be just one group that does all network support or there could be multiple departments/groups. Companies that have their own data centers and/or in-house custom applications typically have larger IT organizations. In a larger environment you may see the following structure:

- Network Services Department
  - Help Desk
  - LAN Implementations Group
  - WAN Implementations Group
- Operations Department

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Help Desk
- Monitoring Group (HP NNM, Tivoli, or some other product)
- Desktop Applications Support Group
- LAN Support Group
- WAN Support Group

❑ E-Commerce Department
- Help Desk
- Development Group

❑ Development Department
- Help Desk
- Development Group (for non E-Commerce in-house applications)
- Testing/QC Group

As you can see from the example above, many times each department has their own help desk. A thorough analysis would be needed of the help desk environment alone. Items to look for would be how their support tickets are tracked and what the escalation procedures are, especially across department boundaries.

Remember, the goal of the workflow analysis is to determine *who* makes changes to the environment. Analyzing the help desk/support mechanisms in use by an organization will show where (and by whom) most of the "unplanned" changes to the network environment are made.

The next step is to analyze how the company uses its' different environments. Even if there is only a single production environment, its usage must be looked at. For this example we'll use three environments: Development, Staging/Test, and Production. The way applications are deployed into and through these environments should be examined.

<u>Items to examine for all three environments</u>:

- Who does the base OS installs?
- Who installs the application or applications?
- Who installs updates to the custom application(s)?
- How are changes to the environment tracked?
- How is physical access to the environments controlled?
- How is logical access controlled i.e. telnet to routers etc.
- Who has physical and/or logical access to each environment?
- Who performs re-installs or recoveries when needed?

An analysis of any current policies, procedures, and checklists/forms is also needed. They typically show how changes are made or supposed to be made. An analysis of these documents also needs to include a "usage" analysis i.e. are they really used if they exist?

❑ Current Policies to look for:
- Virus Protection
- Enterprise Backup

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- New Host Installation
- Software Implementation
- Internet/E-mail Usage
- Internet/Network Monitoring
- Disaster Recovery
- Software/OS Updates

❑ Current Procedures to look for:
- Virus Response/Quarantine
- Backup, Restore, and Tape Rotation
- Scheduled Maintenance
- Host/Device Recovery/Re-installs
- Incident Response

❑ Current Checklists/Forms to look for:
- Change Control Form(s)
- Host Install/Re-install Checklists
- Backup Logs
- System Change Logs

All the checklists mentioned above could be integrated into a help desk system or implemented via an Intranet.

Phase II – **D**esign:

The first step for designing effective Change Control Policies is to gather the appropriate resources, based on information from the **A**nalysis phase, to create the first revision.

It is important to make sure that key people are involved from each area/department that is responsible for making changes to systems. Typically, this would be the managers from each functional area i.e. the Operations Manager, the Help Desk Manager, the Network Manager, etc. This will ensure "common ownership" of the policy and greatly increase the rate of compliance when the policy is implemented.

As mentioned throughout the GIAC coursework on basic policy [2], items to keep in mind when designing policies are:
- Scope of the policy
- Responsibility identification
- Procedures for compliance
- Mechanisms to measure the effectiveness of the policy
- A mechanism for ensuring timely updates to the policy

Policy Scope:

Change control policies typically cover a lot of ground. Depending on the size of the company, it may be necessary to create more than one all encompassing Change

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Control Policy. In the case of larger companies, it might be best to have a change control policy for each environment i.e. one each for production, staging, and development.

The policy should specify the amount of advance notice that is required for making (planned) changes to systems. The times that changes are allowed for enhancements and/or maintenance should also be covered in the policy. Different environments, i.e. production vs. development, will typically have different maintenance schedules.

A thorough change control policy should also address issues of maintaining service packs for operating systems and applications. A company's failure to monitor needed updates for their operating systems and applications could result in a security breach. This happened to a government health information Web site recently. The issue was ultimately tracked down to a lack of updating the site's shopping cart software. [3]

Identifying Responsibilities:

The first step in identifying responsibilities is to analyze the workflow data gathered during the **A**nalysis phase of the project. In order to determine who should be responsible for the various areas in which changes take place, an understanding of who currently makes the changes is needed. Sometimes the policy will change the "normal" workflow and other times a change control policy is implemented onto the existing workflow, adding forms for tracking/auditing purposes.

Procedures and checklists should reflect the decisions made in assigning authority/responsibility via the signature blocks on them. Again, it is important to have the people who will be signing off on any forms involved in their creation.

Procedures for Ensuring Compliance:

Ensure that the policy outlines the procedures that will be used to aid in compliance. The enforcement mechanisms must cover both planned and unplanned changes.

- Change request forms (electronic and/or hard copy) should have fields for signatures authorizing the proposed changes. It is important to make sure that change request forms are reviewed/approved by all parties responsible for the environments affected. [4]
- Forms need to be created for version control of application and system components. This will insure consistency for patches and software updates across the enterprise. This form should have a field showing the dates of approval for new patches and updates. The version control form results in part from the procedure for checking on vendor's operating systems, software packages, etc. for needed security updates. [5]
- Unplanned change forms will also be needed to document changes that are made during the course of troubleshooting. Instead of a different form, help desk software could have a separate field for system changes on each call ticket. The ticket could then be routed, if necessary, to the appropriate functional area to incorporate the changes into the install documentation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- In addition to documenting the changes as they occur, a mechanism for ensuring change propagation to other systems (affected by the same issues) and standard installation documents should also be put in place.

Measuring effectiveness:

Ways to measure effectiveness must be built into the policy. There are several ways to do this.

- Periodic reviews of the change control logs and the help desk system to verify that entries related to system changes match. The frequency of these reviews will differ for each organization and the frequency may have to be adjusted occasionally. The reviews will need to be conducted by the people who have the signing authority on the systems.
- Syslog servers can also be checked to match the times of the changes on the forms with the actual times of implementation on the systems themselves.
- Inspections of systems against the current installation documents can also be performed to verify that all changes that lead to new install procedures have been propagated to operations/production documentation.

Updating the Policy:

The policy will need to be updated periodically to reflect the current needs of the organization. A procedure for updating the policy and propagating the new revisions also needs to be covered in the policy. The policy should also have a schedule for periodic reviews build into it i.e. each version will essentially have an expiration date on it. Prior to expiration, it needs to be reviewed by all parties, updated if necessary, and re-signed.

Phase III – **I**mplementation:

Implementation begins with putting "version 1" of the change control policy and all it's procedures into place. This is usually done on a departmental/functional area basis. It is important to make sure that all people affected by the new policy understand it completely.

After "version 1" has been implemented, measuring the effectiveness of the policy must begin. Often, policies are forgotten about shortly after they're signed and implemented. Measuring effectiveness will indicate whether or not the procedures to ensure compliance are adequate.

Phase IV – **F**ollow-up:

During the first phase of the rollout, the people that are responsible for making changes to systems may bring up points of concern. These points must be quickly assessed for validity and if a modification (or modifications) to the policy is warranted, they should be made and documented during the initial rollout. Often, version 1.1 of the policy will occur during the **F**ollow-up phase of the project.

**Conclusion**

Change Control is an essential part of all organization's overall security posture. Failure to properly manage change can result in vulnerabilities as well as lost time from

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

resolving issues more than once. A lack of control for both planned and unplanned changes can lead to opportunity for hackers and/or people with ill intent to damage or gain unauthorized access to systems. The process of defining/implementing control policies/procedures for change is continuous, like the changes to an environment.

References

[1] – James Evans and Laura Rhode "Western Union's Web site hacked" 09/11/00
URL: http://www.nwfusion.com/news/2000/0911westhack.html

[2] – Doug Austin, Alexander Bryce, Rob Dinehart, Stephen Joyce, Carol Kramer, Randy Marchany, Stephen Northcutt, John Ritter, Matt Scarborough, Arrigo Triulzi
GIAC Basic Security Policy Version 1.35 September 5, 2000

[3] – Bob Sullivan "Health site exposed customer info" June 25, 2001
URL: http://stacks.msnbc.com/news/578476.asp

[4] – Louis Aiken "Change Control" August 29, 2000
URL: http://www.sans.org/infosecFAQ/policy/change_control.htm

[5] – NIH Application/System Security Plan Template May 4, 1999 (Section C.5)
URL: http://irm.cit.nih.gov/security/secplantemp.html

© SANS Institute 2001, Author retains full rights

Last Updated: April 23rd, 2017

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS MGT433 London April 2017 | London, GB | Apr 24, 2017 - Apr 25, 2017 | Live Event |
| Automotive Cybersecurity Summit | Detroit, MIUS | May 01, 2017 - May 08, 2017 | Live Event |
| SANS Riyadh 2017 | Riyadh, SA | May 06, 2017 - May 11, 2017 | Live Event |
| SANS Security West 2017 | San Diego, CAUS | May 09, 2017 - May 18, 2017 | Live Event |
| SANS Zurich 2017 | Zurich, CH | May 15, 2017 - May 20, 2017 | Live Event |
| SANS Northern Virginia - Reston 2017 | Reston, VAUS | May 21, 2017 - May 26, 2017 | Live Event |
| SEC545: Cloud Security Architecture and Ops | Atlanta, GAUS | May 22, 2017 - May 26, 2017 | Live Event |
| SANS Melbourne 2017 | Melbourne, AU | May 22, 2017 - May 27, 2017 | Live Event |
| SANS London May 2017 | London, GB | May 22, 2017 - May 27, 2017 | Live Event |
| SANS Stockholm 2017 | Stockholm, SE | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Madrid 2017 | Madrid, ES | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Atlanta 2017 | Atlanta, GAUS | May 30, 2017 - Jun 04, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DCUS | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CAUS | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TXUS | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Thailand 2017 | Bangkok, TH | Jun 12, 2017 - Jun 30, 2017 | Live Event |
| SANS Milan 2017 | Milan, IT | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SEC555: SIEM-Tactical Analytics | San Diego, CAUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NCUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, COUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Secure Europe 2017 | Amsterdam, NL | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MNUS | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Philippines 2017 | Manila, PH | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| DFIR Summit & Training 2017 | Austin, TXUS | Jun 22, 2017 - Jun 29, 2017 | Live Event |
| SANS Paris 2017 | Paris, FR | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MDUS | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, AU | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, GB | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, JP | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, DE | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, SG | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS ICS & Energy-Houston 2017 | Houston, TXUS | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Baltimore Spring 2017 | OnlineMDUS | Apr 24, 2017 - Apr 29, 2017 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |