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.

Change Control Process for Firewalls

Change is one of the inevitable facts of life we must deal with. Firewall objects and rulesets are constantly evolving in response to new threats, vulnerabilities and services. In order to provide defined Service Level Agreements to our Information Technology customers we are required to maximize availability while maintaining confidentiality and integrity of corporate data assets. As we adapt new enabling technologies for our customers' growing business requirements a high level of internal security must be maintained...

Copyright SANS Institute
Author Retains Full Rights

AD

Paul Maschak
June 22, 2003
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4B - Option 1

Title: Change Control Process for Firewalls

Abstract

Change is one of the inevitable facts of life we must deal with. Firewall objects and rulesets are constantly evolving in response to new threats, vulnerabilities and services. In order to provide defined Service Level Agreements to our Information Technology customers we are required to maximize availability while maintaining confidentiality and integrity of corporate data assets. As we adapt new enabling technologies for our customers' growing business requirements a high level of internal security must be maintained.

A critical but frequently glossed over part of security practice is Change Control (CC). This is the process of implementing change while controlling its environmental impacts. This paper covers the fundamentals of Change Control and Procedures as it applies to the management of Firewalls. Using careful process and planning it is possible to reduce risks associated with changes thereby minimizing the likelihood of detrimental impacts on business operations.

Why Change Control

Information Technology (IT) customers are defined as company employees, internal services and external partners. A primary goal for IT is to provide services that enable our customers to improve their efficiency and effectiveness. A Change Control Policy (CCP) should be an integral part of your organization's written Security Policy (SP). This implies that all implemented security changes must be in compliance of the SP.

> Without a security policy, the availability of your network can be compromised. The policy begins with assessing risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. [1]

The CCP should be well developed and distributed. The purpose of a CCP is to "ensure a uniform change control process, achieve better performance, reduce time and staff requirements, increase the reliability…"[2] and improve the distribution of communications. By maintaining strict control over how change is implemented we maximize the benefits of change while reducing the risk of introducing unwanted problems.

Firewall (FW) operations are ultimately based upon rules acting on objects and data flow. Rulebases range from the simplistic - block all traffic (the perfect set for the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

absolutely security minded administrator) to hundreds of rules with thousands of objects for a diverse organization. CC practices become essential in environments where firewall rules and objects grow beyond a simple few. From my experience caution is warranted in that the predictability of results from a change decreases rapidly as the number of rules and objects increase in complexity. A FW change may create effects which are difficult to predict given limited time constraints and resources necessary for implementation to satisfy a customer's requirements.

Working for an international corporation operating 24/7 with follow-the-sun firewall support teams necessitates solid communication with strict adherence to the control of any implemented changes. Solid methods for information transfer of change details must be available between Security Administrators (SA's) as it may not be possible to make direct contact with customers reporting a problem or even other SA's involved in a change. Failure to work within the boundaries of the CCP can have terrible consequences for not only the SA but IT customers as well.

Our multiple firewalls over time have developed into complex rulesets (over 350 rules) and thousands of objects. Some readers may even comment this is far too large to manage and a rule reduction using CC methods is called for. "The more rules you have, the more likely you or someone else will make a mistake". [3] I will personally attest to having made mistakes so that "someone else" just might be me. Even a simple typographical error can have dramatic effects such as disabling an unwanted IP address range.

FW changes may extend over multiple SA shifts and be completed by another SA team. In an effort to minimize interruptions of active services FW changes tend to be pushed during quiet hours or scheduled maintenance windows. Frequently the impacts of a change made by one SA are observed in logs or called into the Help Desk by affected customers well after the initiating SA has left for home. Inspection of FW logs alone may be insufficient in determining incident cause and resolution thus maintaining solid change documentation for review will assist in timely solutions.

Maintaining firm cost control has become very prevalent for businesses especially now during this economic downturn. Every attempt to judiciously allocate resources helps the bottom line. During the initial stages of CC process a change request is assessed with respect to risks, impact, costs, business case and priority so that a management decision whether to proceed or not can be made before committing valuable resources. [4] Without having controls in place it is easy to waste valuable finite resources.

Service Level Agreements (SLA's) define the IT services and under which conditions they are provided to customers. A Service Catalogue is the repository for all SLA's. Having a clear definition of what IT is providing to the customer through an SLA reduces the possibility of confusion and mistaken expectations while maintaining fairness for all parties. "The SLA defines the roles of both the client and the provider. As a result, the client understands exactly what they are expected to do and what the provider is agreeing to do on the client's behalf. The SLA should be as precise as possible." [5]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Furthermore, I have found that a written end-user oriented IT reference guide translating specific details and reasonable expectations of SLA's to be invaluable during the change procedure should a user's request be denied. Since the customer always has the right to appeal a denied request, management endorsed SLA's may prove to be very valuable in pre-empting unwanted confrontations. The onus of creating a justified business case will then lie squarely with the customer.

If services are created, modified or removed by implementing a change then the SLA must be amended. This is one of the final steps of CC. Please ensure documentation including SLA's, reference guides, etc. are always up to date!

Requirements of Change Control

I have separated CC requirements into 4 categories: Organization, Trouble Ticket system, Firewall and Document Revision Control System (RCS). This list is by no means an exhaustive one but rather a guideline for individuals to decide what level is appropriate in their implementation of a CC environment.

RCS practices have long been associated with software development and most UNIX installations are delivered with either RCS or Source Code Control System (SCCS) [6]. User comfort level will dictate which version control systems are used as they are equally adequate in tracking changes. I highly recommend further research on the Internet to gain knowledge on how to use RCS/SCCS or alternatively read the first 4 chapters of "Applying RCS and SCCS" by Don Bolinger & Tan Bronson. Even though the book was written in 1995 the principles of version control have remained stable.

- Organizational Requirements:
  - management buy-in and support of CCP and security practices
  - adherence by SA's to work in accordance with CCP
  - SLA to be published and maintained
  - published end-user guide explaining the SLA
  - If ISO 9000-3 is a corporate requirement then change management procedures must be complied with (seek assistance from you Quality Assurance personnel)
  - Clearly define responsibilities and authorities for all persons involved in the change process
- Trouble Ticket (TT) system:
  - system to track changes, incidents and request for services (RFS) – this may range from a full enterprise level helpdesk system to a simple data base
  - maintain a history of implemented changes in the TT
  - relate changes to specific person or in the case of a service the affected Service Owner

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

    - tie in of the TT system to a Configuration Management Database -CMDB to provide additional configuration details specific to the end user (i.e. hardware assets, operating system, user location…)
    - allow for multi-user update and retrieval of information
- Firewall
    - restrict modification to rules, objects and services to one SA at a time
    - strict adherence to procedure will prevent multiple simultaneous modifications to a Firewall rule base if not available as part of the FW software
    - archiving of previous rule sets
    - list the changes made with each revision
    - store multiple versions of Firewall configuration data
    - browser enabled rulesets, objects and services
    - report revision history
    - roll back changes to a prior state
    - enable multi-site support
- Document RCS - "This process tracks the changes made to an individual file so that previous versions can always be reviewed or replaced" [7]
    - restrict modification of document to a single SA at a time
    - report revision history
    - store delta changes rather than complete versions
    - show who locked file and when
    - list the changes made with each revision
    - cross reference change to TT and requesting user
    - robust Check-out check-in procedure for RCS documentation
    - allow documentation to be retrieved for view only mode if another user has checked out document for change
    - ability to browse documentation file with XML viewer
    - roll back changes
    - enable multi-site support
    - an audit trail must exist for every change made [9]
    - items to be documented in RCS
        - modifications to FW rules
        - modifications to FW groups
        - what Rule ID is affected by change
        - do not document creation of objects, groups or services
        - explain the changes implemented
        - enter requestor's name, applicable TT, change implementer

<u>Benefits of Change Control</u>

- maintaining a Document RCS as part of the CCP can reduce response time to identify incident causes by enabling inspection of documented changes made to environment that was previously deemed to be stable
- minimize risks of altered, stolen, inaccurate data by formally assessing changes for probable outcome

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- following CMP helps to guarantee integrity of information
- maintain availability of resources for needed by customers for business operations
- implement Security “best practices”
- CC practices assist with compliance of ISO 9000-3 part 6.1.3.2
- maintain SLA levels for the customer
- satisfy and service customer business needs in a timely manner
- eliminate changes that do not meet written Security Policy guidelines
- minimize the risks of altered, stolen, inaccurate, destroyed data. Set baseline rules and standards to optimize confidentiality and integrity of the company
- it is not realistic for any SA to be able to remember all changes made to a firewall rule set
- audit changes made with the ability to review historical changes.
- following CC management procedures help maintain network security with the integrity of information
- partners requesting connectivity frequently request proof of SP and CCP before allowing network connectivity
- a centralized repository for documentation of changes
- ability to continue change process over multiple SA’s
- backup of previous rule sets
- protect intellectual property
- “Tying in an approval Process to the change tracking process ensures that changes receive authorization before they are put into production, thereby enabling users to improve the quality of their delivered product” [7]

Overview of Change Process

The change process may be divided into 2 categories: General and Crisis/Emergencies. General Changes, if warranted, may require an additional stage of creating a Change Plan (see Appendix A) and a formal approval process through a Change Control Board.

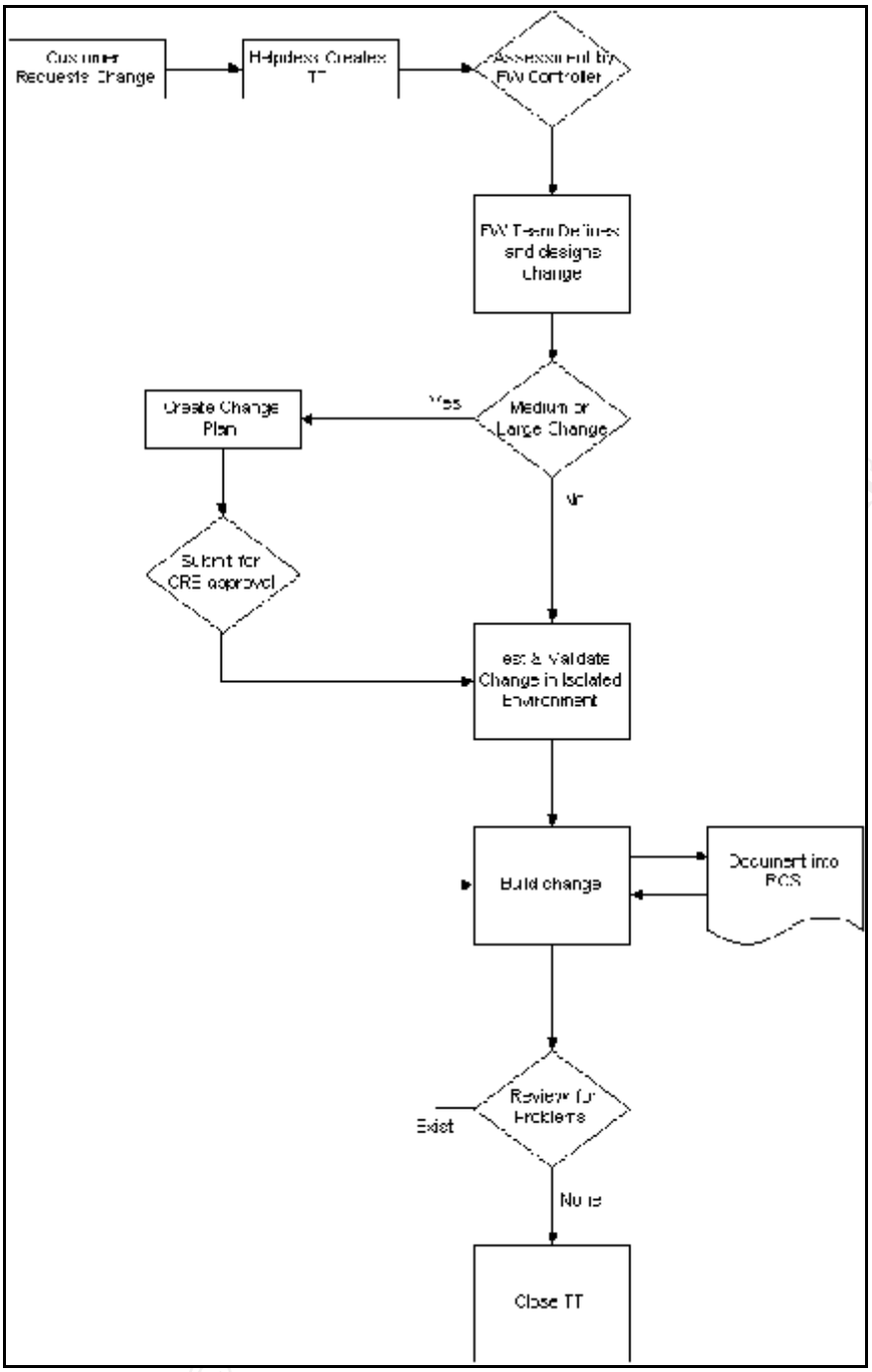
General Change Process:

Step	Activity
1.	Customer requests a change at the Help desk. This may be from a customer or an internally requested change (i.e. address a new vulnerability, patch maintenance or simplification of the rule base)
2.	To track the request the Help desk creates a Trouble Ticket (TT). For some organizations the TT may range from a simple entry in a log book or database to that of an Enterprise Help Desk tracking system such as CA’s AHD
3.	The customer is notified via email of the creation of the TT so they may reference it for status updates and progress. The TT is then passed over to FW team on duty
4.	The request must now be assessed by Firewall Change Controller or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

	a member of the firewall support team for the Integrity of the change with regards to: a. Is there a justified business case exists to support the change. If necessary they will consult management or information owner for approval b. Risk assessment impact to both existing risks and new risks that would be created by the change. Quantify the risk into High/Medium/Low. “Assign all potential changes a risk prior to scheduling the change… Identify risk levels for software and hardware upgrades, topology changes, routing changes, configuration changes …Assign higher risk levels to non-standard add, move, or change types of activity.” [8] c. Time and cost analysis – are there sufficient funds and resources available to implement the change
5.	At this point the TT may be rejected or a decision made to proceed with the change.
6.	FW implementation team • creates a technical definition of the issue and designs the change for the Firewall. • For large or high risk changes further steps are required of creation of a change plan (see Appendix A for sample Change Plan outline) and formal review before a Change Review Board. • Analyze and create proposed solution change for Firewall Rules
7.	FW Team test and validate the change in an isolated environment if possible
8.	Open RCS to document the change
9.	Build the Change into the firewall
10	Document the change in RCS with specific cross reference to the TT
11	Document the change in the TT
12	Push the Firewall change during quiet time or scheduled update windows
13	Review and monitor the firewall change. If problems exist options are: a. analyze and redesign the change, continuing with step 7 b. back out the change. Analyze the situation and continue at step 6
14	If no new problems are encountered and traffic appears to be as expected, notify the customer of a satisfactory conclusion. If necessary document any SLA changes, additions or deletions then close the ticket.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Flow Diagram – General Change Process

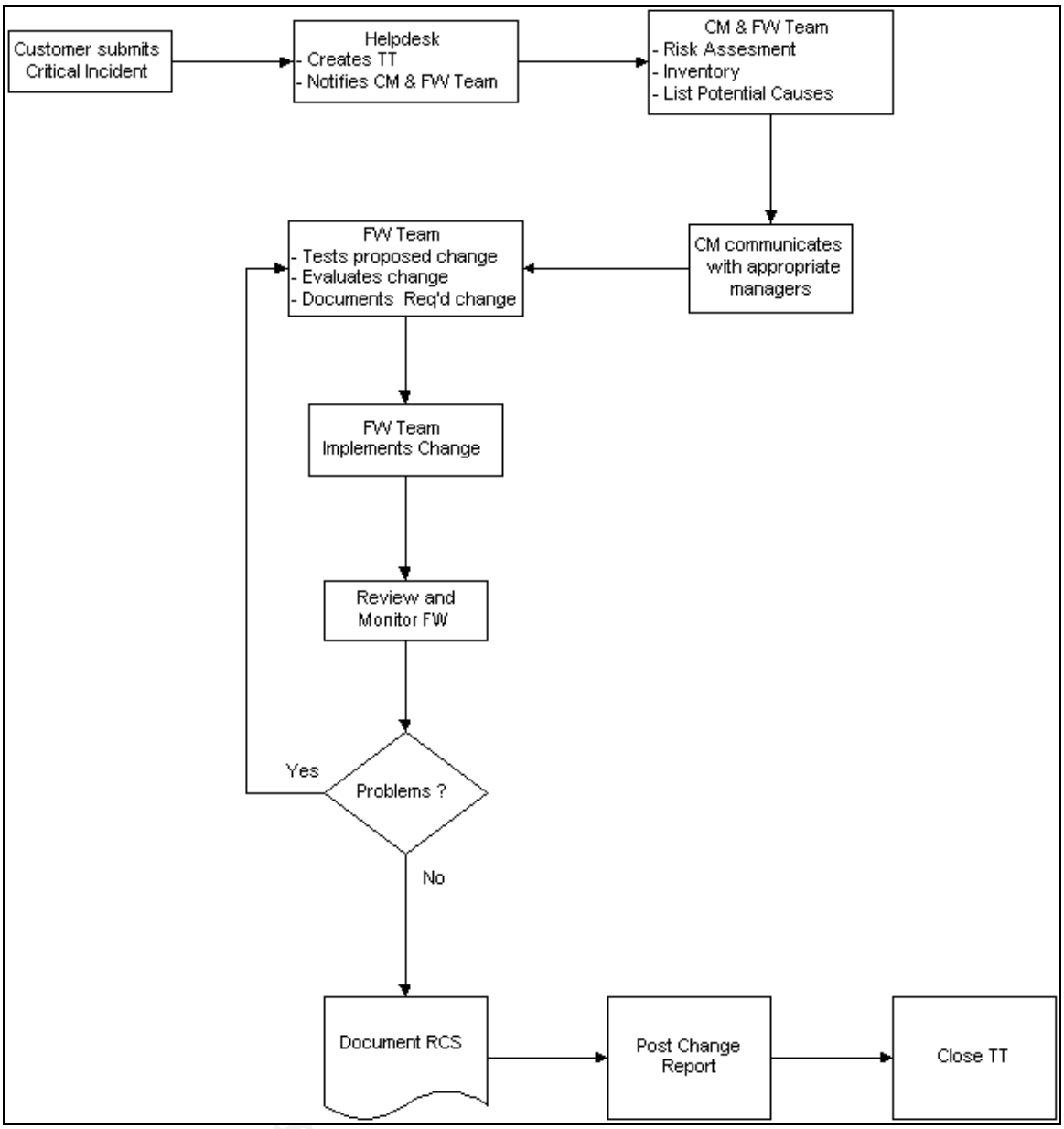
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Overview of Change Process – Emergency/Crisis Change:

A crisis occurs when SLA's can not be maintained within the time limits as agreed upon in the document. The Crisis Manager (CM) is appointed and placed in charge of resolving the situation. CM is given the responsibility and granted resources necessary to resolve the issues during the emergency. It is important to note that all activities are required to be logged throughout the duration of the crisis.

Step	Activity
1.	Help desk or Information owner submits a critical incident. (An information owner is defined as the person responsible for an application)
2.	To track the request the Help desk creates a Trouble Ticket (TT), notifies FW duty person and Crisis Manager. The Crisis Manager retains control of the TT through to resolution of the incident and is responsible for organizing all forces necessary to solve the crisis.
3.	FW team with assistance of the Crisis Manager perform a. a limited risk assessment and a priority level (1.Calamity, 2.Urgent, 3.High, 4.Medium, 5.Low) which is based on: I. urgency – the number of affected users II. severity – importance of a service for business processes b. Inventory – register all facts and activities that have led up to the crisis c. list all potential causes that could have created the crisis
4.	Crisis Manager initiates communication with appropriate affected managers.
5.	FW team tests, evaluates and documents the required change
6.	FW team implements change and pushes out new FW rulebase
7.	FW team reviews and monitors the firewall change. If problems still exist continue back to step 5.
8.	FWT documents changes in RCS
9.	Post Change Report a. Full review and analysis of escalation is published. The report covers history, approach, activities, causes, solutions and recommendations b. Evaluation of all actions performed during the crisis c. Document actions required for a permanent solution

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Flow Diagram – Emergency/Crisis Change Process

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

The extent that you incorporate Change Control largely depends upon your needs. For some there will be no choice as those decisions have been made prior to your start of employment. Others will be able to pick and choose what and how to implement. The benefits of change practices must be carefully weighed against the costs of implementation with the risks of partial solutions. It is essential that there is complete buy-in from all levels of management otherwise you may be easily stopped or thwarted.

Change control is itself subject to change and review. When you audit for security also ensure that the change processes and procedures are reviewed. The most important issue of all is solid documentation. This will enable all security administrators to identify problems and analyze the operation of the firewall now and in the future. The concept of job security through obscurity really is not applicable when it comes to firewalls. By increasing your efficiency you will have time to address more important and hopefully interesting issues rather than have to figure out entire functional operations time and time again.

Change Control practices enable you to peel back layers of change much like an onion and throw out the bad layers. Hopefully during this process you won't shed too many tears. Now is an excellent time to begin putting together Change Control Process to protect the availability, confidentiality and integrity of your infrastructure.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A – Sample Format of a Change Plan

Change: *Title of Change Plan*

Purpose: *One line description of why the change plan needs to happen*

Subject:	*Subject of change Plan*
Date:	*January 1, 2035*
Version:	*1.00*
Author:	*My Name*
Document Changes:	*Date, Name person who made changes*
Related Trouble Ticket Change number :	*412345*

Need: *Explain in brief detail why the change is necessary*

Risks: *Summarize the risk assessment. Be sure to cover what the risks will be if:*

a. The change is implemented

b. The change is not implemented

Change: *Briefly outline what the change will do*

Affected Users: *List who will be affected by the change. Describe severity, start time and duration of any expected outages*

Technical steps preparation

Date & Time	Action	Action by	Remarks
11/08/01	*Change Plan Created*	*Dr. Who*	*DONE*
11/08/01	*Change Ticket Created*	*Help Desk*	
11/15/01	*Upgrade procedures written*	*A. Person*	
12/01/01	*Detail any preliminary steps need before the change.*	*B. Person*	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Technical steps implementation

Date & Time	Action	Action by	Remarks
12/12/01 2300hrs	*Detail all technical step of implementing the changes. Including user interaction and commands issued.*	*A. Person*	

Technical steps checks

Date & Time	Action	Action by	Remarks
12/12/01	• *List necessary steps to check change is functioning properly*	*A. Person*	

Technical steps release

Date & Time	Action	Action by	Remarks

Technical steps rounding off

Date & Time	Action	Action by	Remarks
	• *List any other steps after the change. Especially any communications to people.*		

Back-out

If necessary procedures and plans not complete – then complete NO-GO procedure

Date & Time	Action	Action by	Remarks
	• *List all steps necessary to roll back changes to a state before the change process began.*		
	• *Verify steps to test that all services / operations are functional as prior to the change*		

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

People:

Requestor: *Name of person(s) that requesting the Change*
Change builder: *Names of all persons implementing the change*
Future users: *Name who will use the change*

Communication:

Preparation: e.g. informing the support departments, future users

Date & Time	Action	Action by	Remarks

Implementation: e.g. informing the change builders

Date & Time	Action	Action by	Remarks

Rounding off: e.g. informing all users

Date & Time	Action	Action by	Remarks

Remarks:

Any additional comments go here.

Approval:

Role	Name	Approved (Yes/No, date)
Change Controller Team		
Change Mgr		
Configuration Mgt		
Helpdesk		
Others as required		

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix B - Abbreviations used in this paper

CC	change control
CCP	change control policy
CM	crisis manager
CMDB	configuration management database
CRB	change review board
FW	firewall
ISO	International Standards Organization
IT	information technology
RCS	revision control system
RFS	request for services
SA	security administrator
SCCS	source code control system
SLA	service level agreement
SP	security policy
TT	trouble ticket
VPN	virtual private network
XML	extensible markup language

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[1] "Cisco- Network Security Policy: Best Practices White Paper". 12 Jan 2001. URL: http://www.cisco.com/warp/public/126/secpol.html (17 May 2003)

[2] Information Technology Services, College of the Holy Cross, "Change Control Policy and Procedures, Excerpted from the Holy Cross IT Security Handbook". 22 Feb. 2000.
URL: http://www.holycross.edu/departments/its/network/change_control.pdf (17 May 2003)

[3] Lance Spitzner, "Building Your Firewall Rulebase", October 16,2002, URL: http://www.secinf.net/firewalls_and_VPN/Building_Your_Firewall_Rulebase_.html (17 May 2003)

[4] Central Computing and Telecommunications Agency (CCTA). "Managing Successful Projects with PRINCE2." The Stationary Office for CCTA, 2000. 81-83

[5] Carnegie Mellon Software Engineering Institute, CERT Coordination Center, "Practice 3: Content Guidance for an MSS Service Level Agreement" URL: http://www.cert.org/security-improvement/modules/omss/j.html (18 May 2003)

[6] Don Bolinger & Tan Bronson, "Appying RCS and SCCS", O'Reilly & Asscociates, Inc., 1995

[7] Computer Associates, "White Paper – Enterprise Change Management 101" URL: http://www3.ca.com/Files/WhitePapers/enterprse_change_wp.pdf (17 May 2003)

[8] "Cisco – Change Management: Best Practices White Paper". 04 Jan 2002. URL: http://www.cisco.com/warp/public/126/chmgmt.shtml (18 May 2003)

[9] Q&A Clinic, Harold W. Lockhart – "How detailed should procedures be documented for firewall change control…". 16 Jul 2001. URL: http://www.itsecurity.com/asktecs/jul1601.htm (18 May 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: February 14th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced