

How Configuration Management Systems Deliver Change and Compliance

KEITH SINCLAIR, CTO OPMANTEK | 25 JANUARY 2018 | VERSION 4

TABLE OF CONTENTS

Executive Overview	1
The Top Causes Of Downtime Explored	2
Why Manage Change And Compliance	2
What Is Change And Compliance Management	2
Configuration Management Requirements	3
What Your Configuration Management System Should Do	3
Key Features Of Opconfig For Configuration Management	4
How To Manage Change And Compliance....	4
Implementing A Configuration Management Solution	4
Opmantek Solution For Configuration Management	4
Gather And Backup Configuration Data.....	4
Extract Operational Information	4
Define Compliance Policies	4
Next Steps	5
Configuration Management Self-Assessment	5
Contact Opmantek	5

EXECUTIVE OVERVIEW

The fundamental capability which configuration management provides is backup and archiving of critical configuration data from network and server equipment. This along with collecting detailed inventory data provide the basis for managing change and compliance.

The ability to detect, report and alert on change in near real time improves overall service availability and reduces the time required to identify the cause of incidents and outages.

This paper is to help Network Engineers, IT Managers and Executive Leadership understand the benefits of configuration management and how it contributes to change and compliance management at the business.

To further explore configuration management, this paper is broken into three main sections:

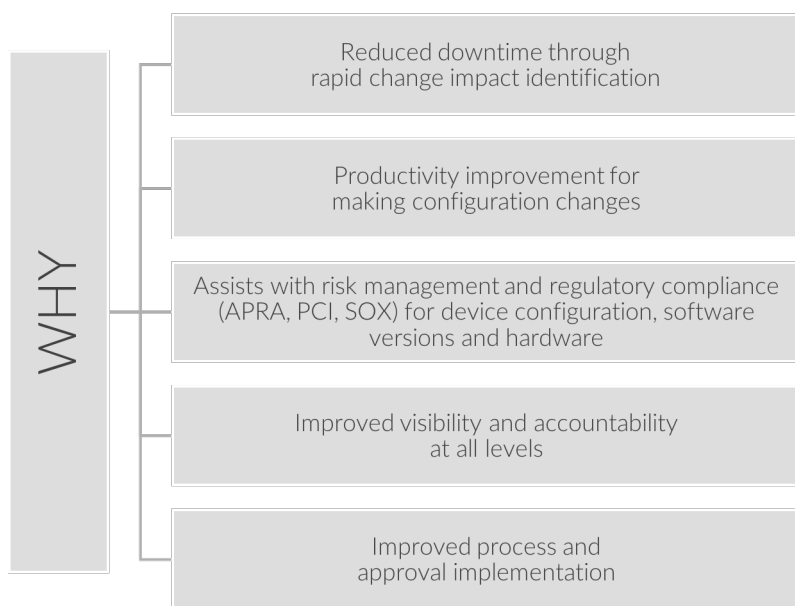
1. Why Manage Change and Compliance
2. What is Change and Compliance Management
3. How to Manage Change and Compliance

Each of these sections will delve into the essential questions and answers people have about configuration management.



WHY MANAGE CHANGE AND COMPLIANCE

What benefits do managing change and compliance provide to the business?

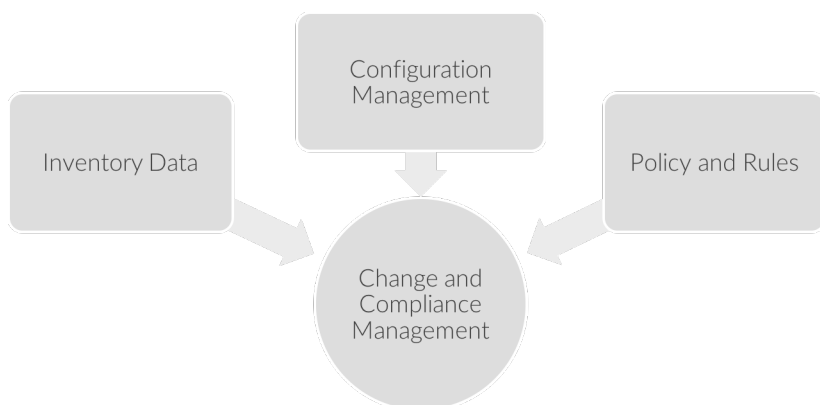


The most obvious tangible benefit is **reduced downtime**. This is achieved by better supporting engineering and operations teams with detailed information about the configuration and what has changed.

WHAT IS CHANGE AND COMPLIANCE MANAGEMENT

IT Change and Compliance Management in its simplest definition is "Managing inventory, configuration, policy, and/or procedure changes that apply to your organization or industry."

Architecturally there are three main elements of change and compliance management, these are:



Inventory Data

An essential input into the system, all the detailed data necessary for the subsequent steps.

Configuration Management

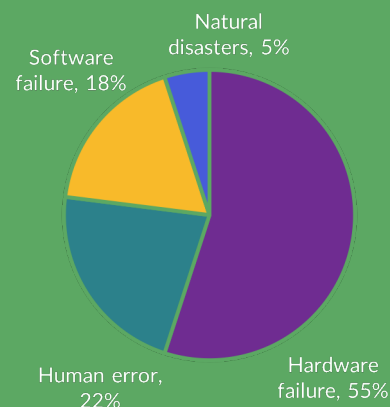
The overall process for managing the configurations from systems, devices and applications. Configuration management ensures that the necessary information is available.

Policy and Rules

Represents what the business needs, the higher-level policies and the resulting rules which are implemented in the system.

THE TOP CAUSES OF DOWNTIME EXPLORED

Some causes of downtime are unavoidable, while others can be avoided through planning and preparation.



Source:
<http://www.continuitycentral.com/news06645.html>

Research has shown human error and software failure directly account for 40% of all downtime.

Monitoring and alerting on configuration changes can effectively prevent or mitigate these failures; generating a significant benefit to the business.

When hardware failures occur, time to restore services is improved by having accurate information and configuration information on hand, along with backups of all the essential data.

Managing change and compliance can provide these benefits to the business.

WHAT YOUR CONFIGURATION MANAGEMENT SYSTEM SHOULD DO

The high level functional capabilities of configuration management are:

- Discovery of elements in your environment
- Collection of detailed data about those elements
- Backup configuration information, and maintain a history of versions
- Storing data for comparison over time
- Reporting on change detected in those elements
- Ability to define compliance policies
- Ability to show elements which are not compliant

These capabilities are foundational to delivering configuration management to the business.

CONFIGURATION MANAGEMENT REQUIREMENTS

To further define what a configuration management system should do it is important to consider what the requirements of that system would be.

Network Discovery - Perform network discovery to find resources and then manage them or report them to be investigated (rogue devices).

Inventory Management - Collect inventory information from the devices including all chassis, modules and their serial numbers.

Configuration Collection and Backup - Collect resource configurations on a regular basis and keep an archive of several generations of configurations.

Resource Change Detection - Detect changes in a device's inventory and configuration; generate event(s) based on these changes, and store information for reporting.

Design Compliance - Provide a means to audit a resource configuration and inventory elements against a defined design policy. Make the information available for reporting.

Security Compliance - Provide a means to audit a resource configuration and inventory elements against a defined security policy. Make the information available for reporting.

High Scale - High scalability platform, able to support 2500+ devices per server.

Compliance Reporting - Provide reports on the status of resources compliance or non-compliance including which policies a resource is not compliant to.

New Device Support - New devices handled without having to update or patch software.

High Scale - High scalability platform, able to support 2500+ devices per server.

Multi-Tenancy Capabilities - allowing device view isolation on a per-customer basis

Single Sign-On - (SSO) preferred and secured login (should support industry standards, such as MS-LDAP)

Activity Logging - Event / transaction logs should show all activities conducted by all users

HOW TO MANAGE CHANGE AND COMPLIANCE

The concept is quite simple, leverage the configuration data to gain knowledge about risk.



IMPLEMENTING A CONFIGURATION MANAGEMENT SOLUTION

With Opmantek products you are able to implement a comprehensive configuration management system which will meet the requirements we have defined in this document, which in turn will deliver value to the business as a whole, by increasing the availability and reliability of the IT Infrastructure.

OPMANTEK SOLUTION FOR CONFIGURATION MANAGEMENT

Configuration management is based on having the necessary data, to collect the necessary data the following products are needed:



opConfig – collects and manages configuration and compliance information



NMIS – collects and manages performance and fault information



Open-Audit – discovers and audits devices found in the environment

These products will ensure that all the necessary data is available to support the overall Configuration Management process.

KEY FEATURES OF OPCONFIG FOR CONFIGURATION MANAGEMENT

GATHER AND BACKUP CONFIGURATION DATA

- Collect configuration information
- Store configuration and keep history of revisions
- Track & display changes between configuration revisions
- Integrates with NMIS & Open-Audit
- Can collect non-configuration information that can be useful for inventory, troubleshooting and performance.
- Works in multi-vendor environments
 - Personalities for how to talk to a device
 - Command sets for what to collect

EXTRACT OPERATIONAL INFORMATION

- Allows comparison of configuration information
 - Compare versions of configs from same device
 - Compare versions of configs from different devices
- Track changes in the network.
- Generate configuration and change alerts
- Provide Change and Compliance Knowledge

DEFINE COMPLIANCE POLICIES

- Ensure risk is managed by knowing exposure
- Compliance works for Windows, Linux, ESXi, routers, firewalls, and just about everything else.

NEXT STEPS

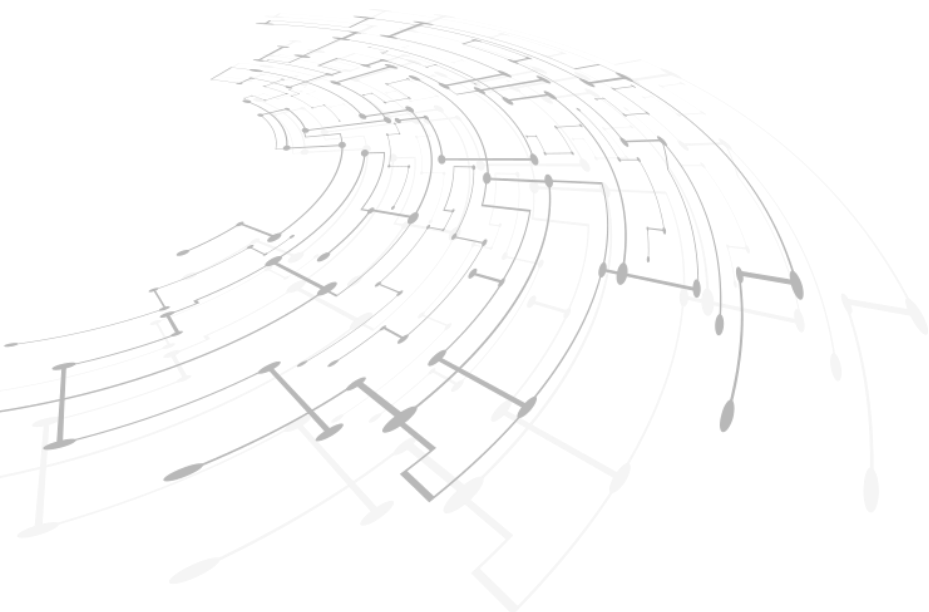
Understanding your current situation is the first step. From this, you can determine what you need to do.

CONFIGURATION MANAGEMENT SELF-ASSESSMENT

Complete these questions and give your organisation 1 point for each answer of Yes.

Question	Y/N	Score
Is inventory information collected from the network including all chassis, modules and their serial numbers, software versions and hardware revisions?		
Are device configurations collected on a regular basis?		
Are changes in device configuration detected, reported, and investigated?		
Is there a well-documented base configuration template?		
Can running configurations be audited against configuration templates?		

Total the number of points you have and if it is 3 or less you need to act to improve your overall configuration management capability and reduce the risk to the business.



CONTACT OPMANTEK

If you need help with configuration management, please contact Opmantek and we will be more than happy to help assess your current situation and recommend a solution to help your business.

E: contact@opmantek.com

W: <http://opmantek.com>