

Cfengine and ISO 27002

A Business White Paper

Cfengine can automate several of the controls suggested by the ISO 27002 standard. Even though most of the work on your way to ISO-27001 certification involves human dependent processes and actions, much can be automated and verified using a software like Cfengine.

DISCLAIMER: Under no circumstances will any part of the Cfengine company be held responsible for errors or omissions in this document.

Copyright © 2010 Cfengine AS

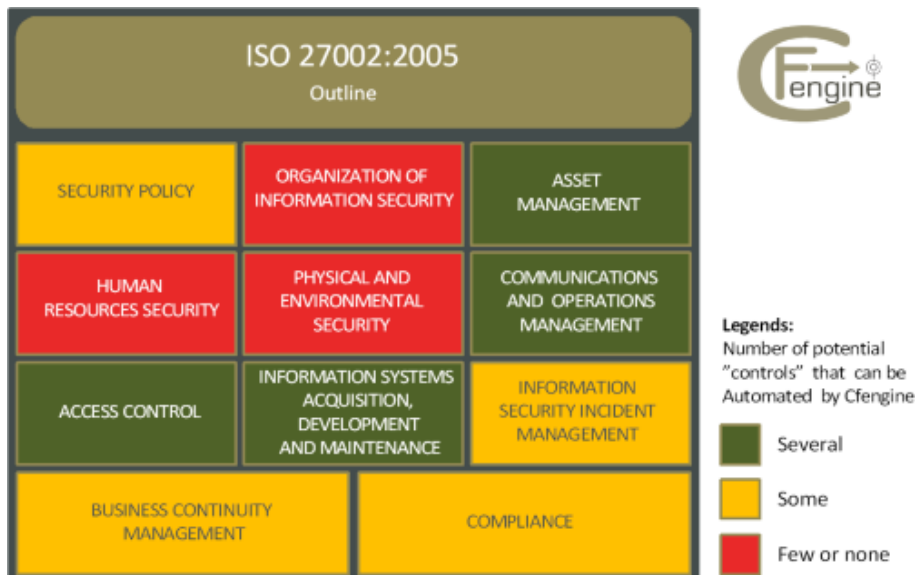
Table of Contents

Cfengine Nova and ISO-27K	1
Desired end-state applications, databases, computer-processes, Firewalls, DMZ, etc.....	1
Comparisons.....	2

Cfengine Nova and ISO-27K

Cfengine can automate several of the controls suggested by the standard. Even though most of the work on your way to ISO-27001 certification involves human dependent processes and actions, much can be automated and verified using a software like Cfengine.

This illustration gives you some ideas on areas in which you can expect Cfengine to help automate your ISO-requirements.



The illustration below shows an outline of the standards and the main areas touched upon in the audit. The yellow and green boxes indicate areas where Cfengine can help you automate some or several of the technical controls and checkpoints as part of your ISO-certification.

Desired end-state applications, databases, computer-processes, Firewalls, DMZ, etc.

ISO27k implementers often suggest a baseline of technical security standards. Cfengine turns this idea on its head, and focuses on the desired-end state instead. A baseline only brings value to the moment it is implemented. As soon as unexpected changes occur, you are out of compliance. Cfengine ensures that the end-state of your system is always in compliance with your policies. ISO27K includes suggestions for baselines and standards laying out the minimum acceptable levels of security by defining configurations or parameters for various technical platforms.

Below is a list of items ISO27K suggest to include in the baselines, and that Cfengine can help you automate by ensuring a desired end-state (automation). Application servers Databases (e.g. Oracle, DB2, Sybase, Access ...) DMZ (Internet-exposed systems and devices installed in the De-Militarized Zone) Firewalls, routers, switches and other network devices (software) Mainframes and minicomputers Operating systems (e.g. Windows XP, Windows 2003, Windows CE, various UNIX, MVS etc.) Third party systems used or installed on-site, and/or connected remotely via the networks

ISO 27002 contains a comprehensive set of 39 key control areas for information security, with a whole lot of "best practice" security controls including registers, policies, procedures and baselines (from IsecT Ltd). The tables below indicate areas where Cfengine can help you out.

Comparisons

ISMS Registers

Backup and Archive Register (details of tapes/disks, dates, types of backup, scope of backup - possibly automated)

Information Asset Inventory Register Database

Information Security Risk Register

Privilege/Administrator Access and Authorization List (details and authorizations for privileged user IDs and access to various 'control bypass' functions)

Software License Register (supplier, type of license, license conditions/restrictions, owner/manager of vendor relationship)

System Patch and Antivirus Status Register (likely to be largely automated)

ISMS Information Security Policies

Access Control Policy

Password Policy

System/data Backup and Recovery Policy

What Cfengine can do

Cfengine can automate your backup procedures and combining the logs with Knowledge Map, you will have full access of every run and output

As of Constellation, Cfengine comes with a fully-fledged CMDB, that keeps track of all your assets

Have Cfengine manage all your security tests, and you will be able to access all the logs and outputs in the knowledge map

Using Cfengine's built-in ACLs (Windows, Linux, Solaris), you can easily get lists of all users and their privileges and access rights

Use Knowledge Map to enter license- and any other meta information about your Software. Cfengine will automatically create lists of active applications and services running on all your machines

You can easily use Cfengine to deploy patches and updates throughout your organization

What Cfengine can do

Cfengine comes with build-in Access Control List features on Windows, Linux and Solaris. Apply your policies, and have Cfengine ensure they are always in compliance

Cfengine can automate your organization's password policy, creating reports and ensuring password changes and strengths (server-side)

Automate the backup and recovery process using Cfengine. Cfengine can do conditional operations based on outputs from third party programs

System Usage Monitoring Policy

Cfengine knowledge map comes with many out-of-the-box reports. Trend-reports and alarms can easily be created. Compliance-reports are only a few clicks away

ISMS Procedures and Guidelines

What Cfengine can do

Security Incident Reporting Procedure

Cfengine can create logs, alarms and reports in case of security breaches defined in the policies. However, Cfengine best-practice is to have Cfengine fix the incident automatically and not disturb the operators/sys.admins

Security Patching and Technical Vulnerability Management Procedure

See Cfengine deployment capabilities above

System Hardening Procedures/System Security Testing Procedure

Have Cfengine manage all your hardening scripts and execute and (if desired report) on the outputs

