# Compliance to Code

# Product Capabilities

HKM Consulting

# C2C - Compliance to Code

## Product Capabilities

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data, also known as the CIA triad, while maintaining the focus on efficient policy implementation, all without hampering organization productivity.
This is largely achieved through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan.

An important cornerstone of information security covered by our solution is availability. Many compliance mandates require permanent availability as well as seamless monitoring of all components of the infrastructure. For this purpose, correspondingly resilient evidence must also be provided. Our solution can help meet these requirements.

In detail, this is achieved through monitoring, actions, reporting as well as other solution features.

### Remote Monitoring

Remote Monitoring:
Monitoring remote servers, even across firewalls and the Internet.

SNAP Tunnels:
Safely send data to remote networks using SNAP Tunnels.

Remote Support:
Securely connect to monitored servers with Remote Desktop even through firewalls and across the Internet with Compliance to Code Monitor.

### Monitors

Action Scheduler:
Automate common IT tasks with the Action Scheduler. It will run your defined Actions when you specify.

Active Directory Change Monitor:
Monitor creation, deletion, and changes of the Active Directory objects.

Active Directory Login Monitor:
Monitor login and other security-related activity in Active Directory, even for local logins.

The All-Systems-GO:
Reports to the All-Systems-GO service which can notify you if the monitoring installation is affected in any way that would prevent its from alerting.

Bandwidth Monitor:
Monitor bandwidth, network error counts, broadcasts and other values from SNMP-based devices as well as from Windows Performance Counters.

Calculated Status Monitor:
This monitor lets you calculate its status by running a script on the statuses of other monitors.

Citrix Presentation Server Monitor:
Monitor and alert on Citrix XenApp (Presentation Server) client connect and login response times. Alert if too slow, and record times for historical charts.

Database Monitor:
The Database Monitor can watch that individual databases are up and running, keep an eye on the transaction log size, and alert if databases are added or deleted from a server.

Directory Quota Monitor:
The Directory Quota Monitor keeps track of directory sizes, and executes actions if the directory sizes are over the quota. End users (directory owners) can be notified via eMail with the Monitor-Directed eMail action. Includes reports.

Disk Space Monitor:
Monitor the free disk space on server drives. You can set the warning threshold in absolute size, or percentage of disk space. Includes reports and auto-configuration.

DNS Monitor:
Monitor the results of a DNS lookup, or a reverse DNS lookup. You can specify which DNS server the request should be sent to. If an unexpected result is returned, actions are fired.

Dynamic Server List:
Dynamic Server Lists are groups of serves that meet your criteria. Once the list is known, you can define Dynamic Groups based on the list, and use that group everywhere else groups are used.

eMail Monitor:
Monitor eMail messages in a POP3 or IMAP4 mail box for messages that contain specific text. When a match is found, alerts are fired.

Environment Monitor:
Connects to an Esensors EM01b websensor on the LAN and monitors the current temperature, humidity and luminescence, and notifies you if the values go above thresholds that you set. Historical reports as well.

More information on EM01b sensors can be found at: https://eesensors.com

Event Log Monitor:
Checks any specified Windows Event Logs (Application, System, Security plus custom event logs) and executes actions you specify if a source you're interested in adds an event to the log.

Event Validator Monitor:
Verifies that specific events, such as backup succeeded or anti-virus pattern file updated events are in the event log. If they are missing, fire alerts.

Execute Scripts:
Execute your custom written scripts written in the Visual Basic Scripting Edition language. You can use custom or 3rd party ActiveX controls. The script determines whether to trigger actions using your own logic.

File Age Monitor:
Monitor file ages and alert if the files become too old (good for watching server queues, spool directories, etc.).

File/Directory Size Monitor:
Track the size of a directory or a set of specific files within a directory. Includes reports.

File & Directory Monitor (CIFS Monitor):
This monitor is a host-based IDS (Intrusion Detection System) that will notify you when the date, size or even content of a file changes on local files, or files on any CIFS share. File creation and deletion is also monitored. A good tool to help with configuration management as well. Auto-configuration functionality is available.

FTP Server Monitor:
The FTP Server monitor can login to FTP servers (including SSL-enabled FTP servers) to make sure they are up and running.

Hardware Monitor:
Monitor the hardware status of ESX, Dell DRAC/iDRAC, HP iLO, IBM RAS and other IPMI-based devices.

Inventory Alerter:
Alerts on inventory data collected by the Inventory Collector monitor.

Inventory Collector:
Collects inventory information (hardware information, pending Windows Update, anti-virus status, etc.) from a variety of sources including WMI, SNMP and an optional System Details application.

Log File Monitor:
Periodically checks the content of one or more log files for target text. Target text and be a simple text phrase or a regular expression.

Mail Server Monitor:
Monitor your mail servers (POP3, IMAP & SMTP) and validate that they are running and accepting incoming connections.

Network Scan:
The Network Scan monitor will periodically perform a ping scan of a specified IP address range looking for new devices that are not already being monitored. They can automatically get added to the system and configured for monitoring.

Performance Monitor:
The entire breadth of the system Performance Counters can be monitored allowing you to set actionable thresholds on CPU usage, memory usage, NIC traffic, etc. Performance counter values are stored in a database so you can view historical counter reports and understand trends.

Ping Monitor:
Tests a connection/device by periodically testing it with a ping. No response or too great a delay triggers actions. Ping response times are recorded in a database for reporting and graphing.

Plugin Monitor:
Runs an executable or external script launched via Windows, or via SSH, and parses the output to determine whether alerts should be fired. Plugins can also return values that are recorded to the database and can be charted.

Process Monitor:
Monitor that specified processes are running on Windows or Linux servers.

Remote Desktop Gateway:
Monitor Remote Desktop Gateways and show currently connected sessions on a dashboard.

Server Temperature Monitor:
Using the free SpeedFan utility, the Server Temperature Monitor will watch the values from the various temperature probes on your server and notify you if they go above the thresholds you set.

Service Monitor:
Watches system services and runs customized actions (including restarting the service) if they are not running.

SNMP Monitor:
Connects to local or remote SNMP agents and queries SNMP object values. Custom MIBs are supported. The value is compared to a threshold that you set and actions are fired as specified. SNMP values are also recorded to a local database for reporting purposes. Supports SNMP v1, v2c and v3.

SNMP Trap Monitor:
Receives SNMP Traps and optionally filters on trap text before running attached actions.

Syslog Monitor:
Receives Syslog log events and optionally filters on incoming log text before running attached actions.

Task Scheduler:
Monitors the enable/disable status and the Last Run Result value of Windows Task Scheduler tasks.

TCP Port Monitor:
Makes a TCP connection on a specified port. Optionally send command text and check response text. Timing data is recorded for reporting purposes.

Web Page Monitor:
Monitor one or many pages on a web site. Checks for positive cases (text that must be found), negative cases (alerts if error text found) and if the page has changed at all. Response times are checked and recorded, and reports can be generated to understand trends.

**Action List**

Action List:
Groups of actions for common notifications, group notifications, etc.

Call URL:
This action will call a URL you specify, optionally posting information about the current alert. This makes it easy to connect to a helpdesk/ticketing system.

Desktop Notifier:
Delivers alerts to Windows desktops via a pop-up message box or a slider in the lower right corner of the screen.

Dial-Up Connection:
Connects or disconnects a Windows Dial-up Connection. Typically this is for servers that are not on the Internet, but need to connect to send alerts.

eMail Alert:
Sends SMTP eMail messages to mail boxes, cell phones, mobile devices, etc. The eMail action has Alert Digests which are a powerful/friendly feature that combines multiple alerts that happen within a short time into a single eMail notification. This can be very helpful when something goes really wrong. You can easily specify when messages should be sent or suppressed.

Execute Script:
Similar to the Execute Script monitor, this Action lets you extend the list of available actions via your own script written in VBScript. Many variables from the source monitor are also available for creating rich, situation-specific responses.

Message Box:
A simple message box that displays monitor findings. These message boxes are smart: if there are many pending alerts you can easily dismiss them all at once.

Monitor-Directed eMail:
The monitor which detects a problem specifies the eMail address to use for each alert. This is very useful when sending reminders and alerts to end users such as with the User Quota Monitor and the Directory Quota Monitor.

Network Message (Net Send):
Sends a message box containing the critical monitor details to every place that you are logged in.

Pager Alert via SNPP:
Send monitor results to pagers via standard Simple Network Paging Protocol (SNPP). You can easily specify when messages should be sent or suppressed, and the content of the message.

PagerDuty Integration:
Send alerts directly to your PagerDuty account and track them using the full power of the PagerDuty platform.

Phone Dialer (DTMF/SMS):
Dials a modem/phone and optionally sends DTMF commands or other commands (to send SMS messages for example). This is typically used by a disconnected server to send an alert over a normal phone line (where the CallerID identifies the server).

Play Sound:
Audible alert when monitors detect a problem with the server.

Reboot Server:
Reboots the server if a monitor has detected a critical system failure.

Run Report:
When this action is triggered, it will run the specified Scheduled Report including sending any eMails or saving PDF or CSV files that report requires.

SMS Text Message:
Send SMS text messages to your mobile device via your service providers SMS Internet gateway (SMPP server). You can control which information gets sent, as well as when messages are allowed.

Server Maintenance:
Set or remove the Immediate Maintenance period for a server or servers.

SNMP Trap:
Sends an SNMP Trap with details from the monitor firing the action.

Start Application:
Starts a specified application when the monitor triggers actions.

Start Service:
Sends control messages to the Windows Service Control Manager to start, stop or restart a specified service.

Syslog:
Sends monitor alerts to a Syslog server on the network.

Write to Event Log:
Writes monitor details to the Windows Event Log.

Write to Log File:
Log the findings of any triggered monitor to a file. Separate files can be created for each day, week, month, etc.

**Reporting**

Ad Hoc Reports:
Generate reports on the fly to quickly see graphical trends.

Branding Reports:
Easily brand reports with your company logo at the top.

Group Settings:
Group summary reports can be specified and controlled in a per-group way. In addition, group reports can be automatically eMailed to anyone that needs to keep track of the servers.

HTTP accessible reports:
Reports are generated in HTML and accessible from within the Compliance to Code Console application, or from a web browser.

Inventory:
Collect and report on hardware and system inventory of the monitored servers and devices.

Multi-Port Chart:
Combines and shows multiple bandwidth charts on an efficient set of one or more graphs.

Password Protection:
Password protect web reports in Compliance to Code.

Satellite Status:
Quickly see the current status of an individual Satellite Monitoring Service.

Satellite Summaries:
Two reports that let you see the status of all of the Satellites at once.

Scheduled Reports:
You can create scheduled reports which will get created when you want them, and optionally eMail the report to a list of recipients. Scheduled report URLs are stable so you can add them to your Favorites list to quickly and easily see the latest results.

Server Status:
Easily see at a glance the state of your server along with system statistics.

System Activity Log:
Quickly see which monitors are running, how long they are taking, which actions are being fired and more.

Standard Report Tabs:
View the tabs and information that is common among most report types.

Uptime Reports:
Uptime Reports can be run on many different types of data, with summarization at the raw, hourly, daily, weekly and monthly level.

Group - All Errors Report:
The All Errors report show all recent errors on all monitors on all servers/devices within a group. This is a good place to quickly get a detailed view of any problems happening on the network.

Group - All Servers Report:
This report shows all of your servers in a group in a single page. Each server is a small box that is color coded according to the status of the monitors on that server.

Group - Custom Group:
Create custom reports at a group level to show custom HTML, charts, and other status values for the contained servers.

Group - Group Overview:
A compact report that shows high-level server health with detailed monitor types in a column layout.

Group - Group Summary:
See a one line status indicator per server to see at a glance how the servers in your data center are doing. Per-group status reports are also supported.

Group - Network Map:
View all of the servers/devices within a group in a single report, grouping all computers and showing their status.

Group - Status Map:
See a graphical map that contains status indicators that show you at a glance how servers in different geographic regions are doing.

System - Config Audit:
This report shows you what your current configuration is with your Groups, Servers, Monitors, and Actions.

System - Connected Sessions:
See all sessions (Console, Satellite, mobile apps) currently connected to the Central Service.

System - Error Audit:
Powerful report to look at current and past alert conditions that have been detected by the system.

System - Monitor Scope:
Displays a summary of what is being monitored on a per-group basis. This would be appropriate to show stake holders to indicate the level of monitoring work being done.

System - Monitor Status:
A quick table-based overview of current monitor statuses. You can specify a specific monitor type, only monitors in error, etc.

System - Statistics:
View system statistics such as HTTPS connections and data transferred, numbers of monitors and connected Satellites, etc.

System - System Audit:
Find out about activities within the monitoring system, such as alert eMails sent, user logins, Satellite disconnects, etc.

System - User Permissions:
This report will display all users defined in the system, what they have access to, and their permissions.

**Product Features**

Automated Maintenance Schedule:
While a computer is in maintenance mode, the system won't run monitors. It will turn itself back on automatically after the maintenance window expires if you manually entered maintenance mode, or it can automatically enter and leave maintenance mode on a schedule.

Automatic Fail Over:
Setup a second instance of C2C to monitor the primary monitoring service, and take over if it fails.

Bulk Configuration:
Perform changes of settings in actions, monitors, reports and scheduling for several servers at one time, or copy configuration settings to other servers.

Configuration Security:
Password protect the C2C Management Console, and alert on changes that could affect monitoring.

Database Options:
Easily point C2C Management monitor at the embedded SQLite database or use an external Microsoft SQL Server.

Easy to Use and Configure:
Due to the agent-less integration in a network segment and the easy roll-out of only one satellite per sub-network, the system is one of the simplest, clearest and most effective monitoring tools.

Embedded HTTP Server:
Control the HTTP port that C2C Management Monitor uses, and optionally enable HTTPS (SSL).

Error Auditing:
Keep track of which errors have been reviewed and acknowledged. Also a great way for administrators to have an overview of any errors within their area of responsibility.

Event Escalation:
Many monitors are capable of sending escalating events. For example, low disk space alerts could first go to a first-tier Ops team. If the aren't handled in a specified time frame, they could be forwarded to a second-tier Ops team.

External API:
Send basic configuration requests to the product via an HTTPS URL.

Inventory:
Collect and report on hardware and system inventory of the monitored servers and devices.

Mobile - iPhone:
C2C Management Monitor for iPhone lets you stay up to date even if you're away.

Mobile - Android:
C2C Management Monitor for Android lets you stay up to date even if you're away.

Mobile - Windows:
C2C Management Monitor for Windows lets you stay up to date even if you're away.

Runs as a service:
C2C Management Monitor is composed of a console that you interact with, and a system service that is started when the computer boots up and is always running in the background.

Server Grouping:
Group servers together in visual groups to help keep track of them. Group-based status reports are also available.

Simple Branding:
Easily brand C2C Management system to have your name and graphics by simply dropping a couple of files into the installation directory. Rebranding will be provided with the C2C Toolbox.

Simple Installation:
Takes less than 3 minutes to install and get a default installation customized for your system.

Smart Configuration:
Paste a list of servers or IP address into a list and let C2C Management Monitor inspect and self-configure for each server/device. Or easily copy the configuration from one configured server to one or more other servers.

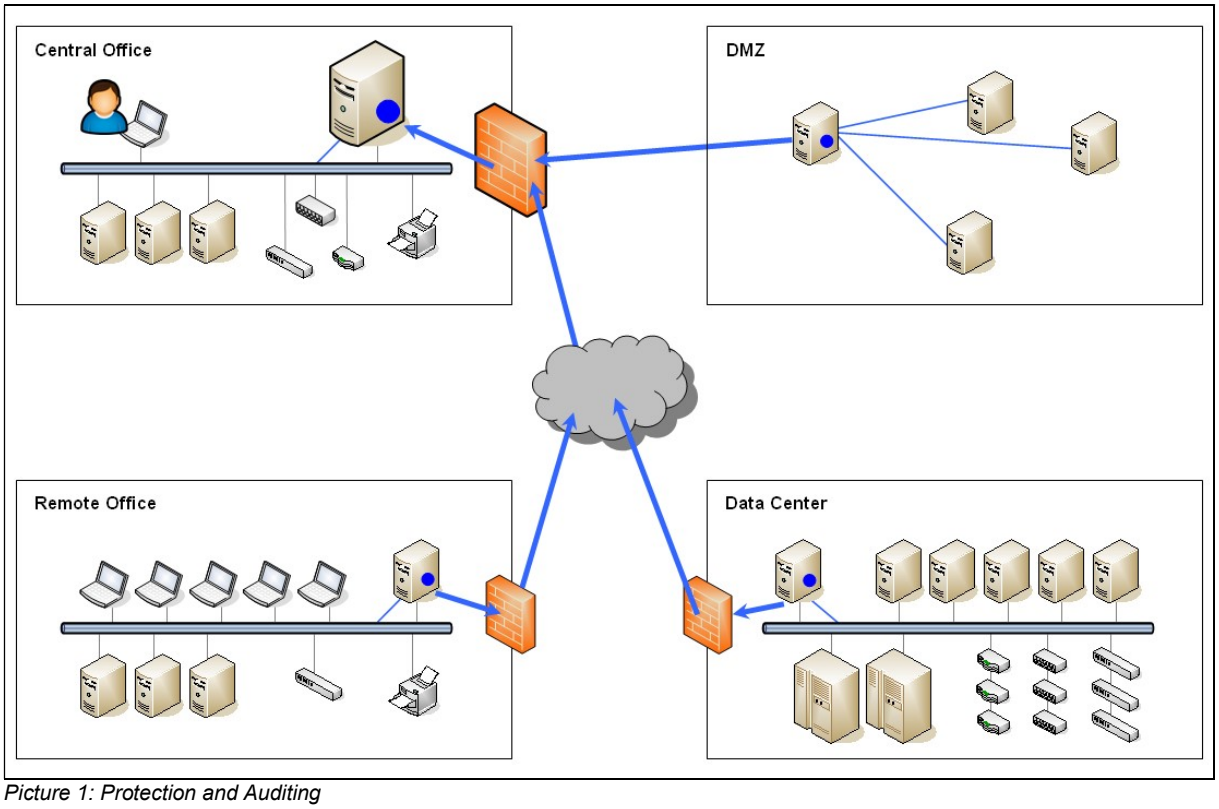
VMWare ESX:
Monitor aspects of a VMWare ESX host server.

**Fulfillment of Compliance Requirements:**

An important cornerstone of information security covered by our solution is availability. Many compliance mandates require ongoing monitoring of the infrastructure and require continiuty management to ensure the availability of the services provided. Our solution can help meet these requirements, including those listed below:

- PCI (Payment Card Industry) DSS 10.5.5, 11.5, 12.9.5
- SOX (Sarbanes-Oxley) DS5.5
- GLBA (Gramm-Leach-Bliley Act) 16 CFR Part 314.4(b) and (3)
- HIPAA (Health Insurance Portability and Accountability Act) 164.312(b)
- FISMA (Federal Information Security Management Act) AC-19, CP-9, SI-1, SI-7
- ISO 27001/27002 12.3, 12.5.1, 12.5.3, 15.3
- ISO 27001:2013 - Annex A.5-A.18
- European Law on protection of Business Secrets (GeschGehG)
- BSI KRITIS
- §203 StGB
- BaFin (BAIT, KAIT & VAIT)

**Protection and Auditing:**




*Picture 1: Protection and Auditing*

Our C2C - Compliance to Code system can monitor the operating parameters of hundreds of remote networks and/or local network only. It allows monitoring for Windows, Linux, Unix and network devices. Ping, CPU, memory, disk, SNMP + traps, event logs, services, etc.

No scripts or configuration files are required. The system monitors on-premises as well as IoT devices.

C2C - Compliance to Code highly scalable and enterprise-ready. In minutes, define simple rules to monitor essential operational parameters or set up monitoring satellites that protect remote servers and report back to the central server. Cover all your availability requirements from a central console.

Please contact your sales and consulting representative to work out you best integration type and pricing.

© 2023 HKM Consulting GmbH

© 2023 Janus Event und Entertainment GmbH

Alle Rechte vorbehalten. Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen Zustimmung des Verlags. Dies gilt auch auf die fotomechanische Vervielfältigung (Fotokopie, analoge oder digitale Ablichtung, Mikrokopie) und die Einspeisung und Verbreitung in elektronischen Systemen.

HKM Consulting GmbH
Klaus Martin Hecht
redaktion@hkm-consulting.de