

Your 'Easy Button' for CIS Compliance

Enhancing IBM i Security With Vanguard
Compliance Manager (VCMi)

Table of Contents

[1. Executive Summary](#)

[2. Introduction](#)

[3. The Compliance Challenge for IBM i](#)

[4. Introducing VCMi](#)

[5. Technical Overview of VCMi](#)

[6. Comparison to Competitors](#)

[7. Real-World Use Cases](#)

[8. Future Roadmap](#)

[9. Call to Action](#)



Executive Summary

For businesses relying on IBM i systems, ensuring both robust security and compliance with regulatory frameworks is essential. The intricacies involved in manual processes, combined with the evolving complexity of standards such as the Center for Internet Security (CIS) Benchmarks, can overwhelm IT teams. Vanguard Compliance Manager for IBM i (VCMi) is a state-of-the-art solution developed to address these challenges. With automated precision and adherence to CIS Guidelines, VCMi removes the inefficiencies and risks associated with manual checks while enabling organizations to stay fully audit ready.

What Is CIS?

The Center for Internet Security (CIS) provides globally recognized benchmarks for securing IT systems. For IBM i, adhering to the CIS Benchmarks enables organizations to safeguard IT systems against cyber threats. The CIS Benchmark for IBM i is “the product of a community consensus process and consists of secure configuration guidelines developed for IBM i,” according to CIS.

The CIS benchmark document was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from diverse backgrounds including consulting, software development, audit and compliance, security research, operations, government and legal.

Two configuration profiles are defined by the CIS Benchmark:

Level 1

Corporate/Enterprise Environment (general use) items with the intention to:

- Be practical and prudent
- Provide a clear security benefit
- Not negatively inhibit the utility of the technology beyond acceptable means

Level 2

High Security/Sensitive Data Environment (limited functionality) items with the intention to:

- Be applied in environments or use cases where security is paramount
- Act as defense in-depth measure
- Possibly negatively inhibit the utility or performance of the technology in the interest of security

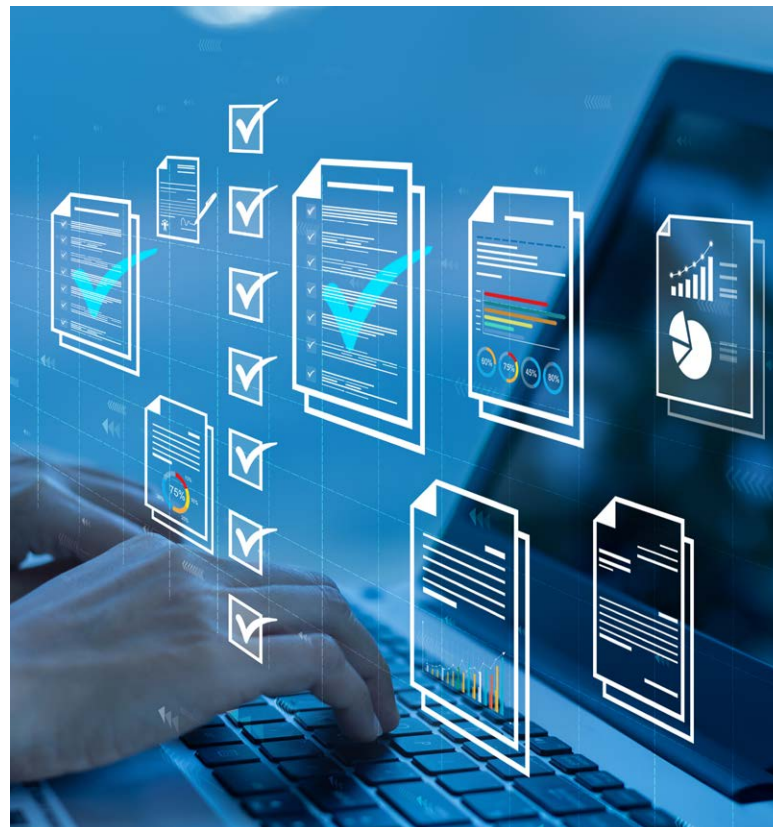
This e-book explains VCMi's functionality, its technical pillars and the strategic benefits it brings to organizations striving to run secure and audit-compliant IBM i operations.

VCMi Makes Compliance Easy

Compliance management in IBM i environments typically involve complex frameworks, high-stakes audits and labor-intensive tasks. Even the most experienced IT teams can struggle with interpreting lengthy standards and consistently implementing them without error. Especially in industries like finance, insurance and healthcare, regulations place an immense burden on organizations to secure their systems and verify compliance through regular audits.

Built on Vanguard Integrity Professional's 39 years of expertise in safeguarding complex z/OS enterprise environments, Vanguard Compliance Manager for IBM i (VCMi) is designed specifically for IBM i systems. It empowers companies to automate compliance processes, substantially reduce the risk of human error and operate more efficiently.

With VCMi, compliance with the CIS standard is black and white. Either a system complies based on answers to actual questions within CIS (passes) or it doesn't (fails). There's no deviation. Think of VCMi as your CIS "Easy Button" for IBM i.



Why Manual Compliance Falls Short

1.

Cost of labor:

Reviews and audits require extensive hours from skilled IT staff.

2.

Risk of error:

Complex frameworks leave room for misinterpretation or oversight.

3.

Disruption:

Heavily manual efforts divert resources from other essential projects.

With VCMi, organizations can simplify these efforts, remaining compliant while saving time and resources.

The Compliance Challenge for IBM i

Compliance isn't just a technical requirement; it's a strategic priority for organizations operating under regulations such as HIPAA, PCI DSS and SOX. VCMi is audit friendly, in other words, it increases operational efficiency by automating internal & external audit reports. Unfortunately, for IBM i users without VCMi, achieving and maintaining compliance is easier said than done due to the following challenges:



Complexity of Standards

The CIS Benchmarks for IBM i form the foundation for secure system configurations. However, these benchmarks contain hundreds of detailed requirements across system configuration, operating system settings, role definitions and user-level permissions. Staying compliant demands not just expertise but also an immense investment in time and effort to monitor and enforce these guidelines.



Reliance on Manual Processes

Manual compliance management is both resource-intensive and error-prone. For example, IT teams must manually identify and review configuration anomalies against CIS standards. Over time, staff fatigue, changing team dynamics and miscommunication can lead to missed checks or incomplete reports.



Resource Constraints

IT departments often operate with lean teams, multitasking across multiple business-critical functions. Adding laborious compliance checks to their workload can strain team efficiency, leaving other critical initiatives underdeveloped.



Regulatory Penalties

Failure to follow compliance frameworks isn't just a legal exposure; it comes with reputational risks. Investigations and penalties can deter client trust and negatively impact business outcomes.

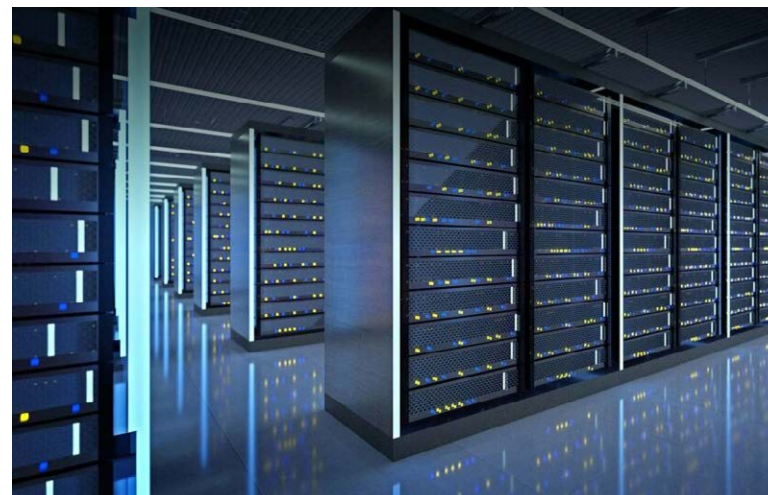
The VCMi Difference

VCMi was built to directly combat these pain points by automating large portions of the compliance process, offering speed, precision and reliability to IBM i users.

VCMi Is More Than a Compliance Tool

VCMi isn't just a compliance tool; it's designed to automate foundational security requirements on IBM i. Organizations can run various applications on VCMi, from custom-build software to industry-standard packages. The solution also incorporates security features to protect sensitive data and ensure compliance with industry regulations.

With VCMi, organizations can maintain compliance with regulations while shifting their resources back to higher-value tasks.



Key Benefits of VCMi

1

Security

Exceeds product standards
by meeting high security
demands

2

Compliance

Performs critical compliance
checks to adhere to industry-
specific regulations

3

Audit

Easy-to-use with
immediate results for
audit requirements

4

Single-pane View

Automatically
generated results

VCMi isn't Vanguard's first foray into IBM i solutions. IBM i products have been developed at the request of the company's existing clients, many of whom are among the Fortune 100.

These large organizations, which typically use both IBM Z and IBM i platforms, value Vanguard's long history of innovative enterprise security solutions on mainframe. But they need to consolidate contracts with vendors to streamline procurement operations. VCMi is the latest Vanguard solution for IBM i.

Top Features of VCMi

1. Codified CIS Benchmark checks tailored to IBM i.
2. Pass/fail reporting for quick, actionable insights.
3. Future-proof compatibility with IBM i v7.4 and v7.5.

Here's How VCMi Works Under the Hood:

Installation and Configuration

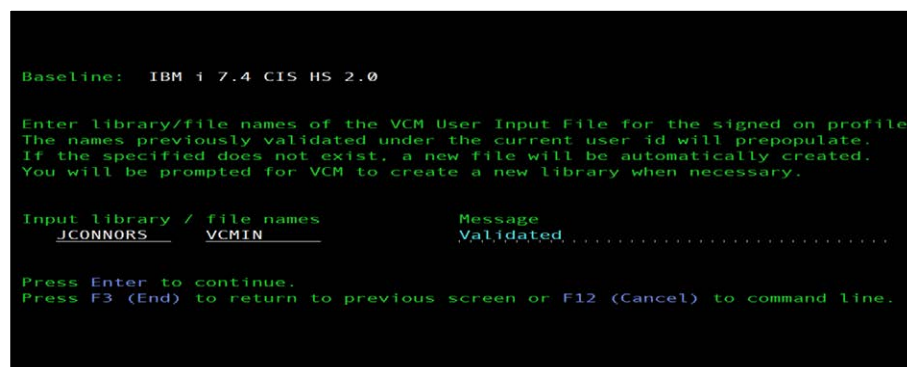
VCMi is installed from optical media (or .bin/.iso virtual media, using the LODRUN command. The product configuration is in the form of inquiry break messages with default answers. Pressing ENTER through the inquiry message will always take the default setting. The last step of the installation process starts the product in the Baseline Selection Screen.

The intuitive installation reduces onboarding time, accelerating an organization's path to operational use. Baseline configurations can be set to level 1 or level 2 of CIS security standards for IBM i.

After validation of your session user input file, VCMi enters its main product area. From there, CIS benchmark audits can be launched and managed and the results can be viewed and reported on.

An individual audit item is referenced throughout this and other Vanguard Compliance Manager documents as a "check." Like the way the CIS benchmark audits are grouped by chapter, section or security level within their documentation, VCMi checks are grouped by the version and release of the IBM i operating system, by VCMi baseline or by category. To make the product even more intuitive, the ID number assigned to a check (the Check ID) is comprised of the chapter, section and security level numbers under which the title was found in the CIS benchmark document. The chapter describes the command line options, available function and navigation of the VCMi category and check menus.

The VCMi library selection interface.



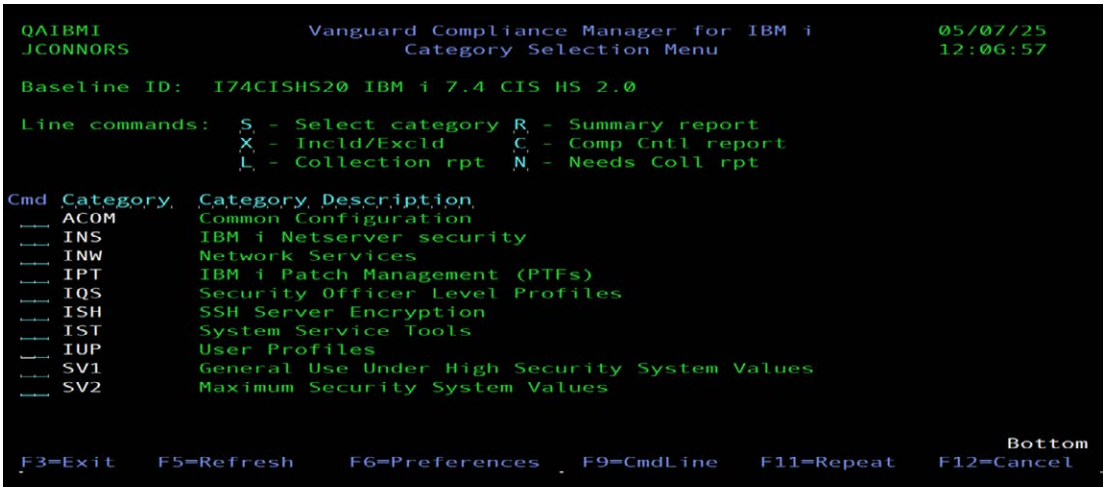
```
Baseline:  IBM i 7.4 CIS HS 2.0

Enter library/file names of the VCM User Input File for the signed on profile
The names previously validated under the current user id will prepopulate.
If the specified does not exist, a new file will be automatically created.
You will be prompted for VCM to create a new library when necessary.

Input library / file names      Message
  JCONNORS      VCMIN      Validated.....

Press Enter to continue.
Press F3 (End) to return to previous screen or F12 (Cancel) to command line.
```


The VCMi category selection interface.



The User Interface

The VCMi user interface is composed of menus navigated through an emulated 5250 terminal session. Line commands specify actions performed on the menu item collective selected with the letter indicated in each menu header.

Menu item collectives include:

Baselines

The collections of all categories of checks corresponding to the published version of the CIS Benchmarks documents.

Categories

A group of checks under an indicated commonality referenced by a three-character abbreviation (i.e., the first three letters of the Check ID).

Checks

Performs validation of a system setting as referenced by the Check ID.

Quick Setup

Installing VCMi takes just minutes with intuitive menus guiding you through selecting the appropriate CIS baseline.

Automated Assessment & Reporting

Once configured, VCMi automates several critical tasks across:

- **Baseline Adherence:** Align systems with your selected CIS Benchmark level (e.g., High Security).
- **Audit Execution:** Conduct hundreds of configuration checks in minutes.
- **Report Output:** Generate regulator-ready summaries suitable for auditors or executives.

Key Innovation

By automating compliance assessments, VCMi eliminates two key pain points:

1. **Human Errors:** Automated CIS checklist enforcement ensures flawless execution.
2. **Time Inefficiencies:** Manual audits that traditionally span weeks are reduced to hours.



Comparison to Competitors

While numerous compliance and security solutions target generic IT environments, their limitations become apparent when applied to IBM i systems.

Here’s how VCMi stacks up:

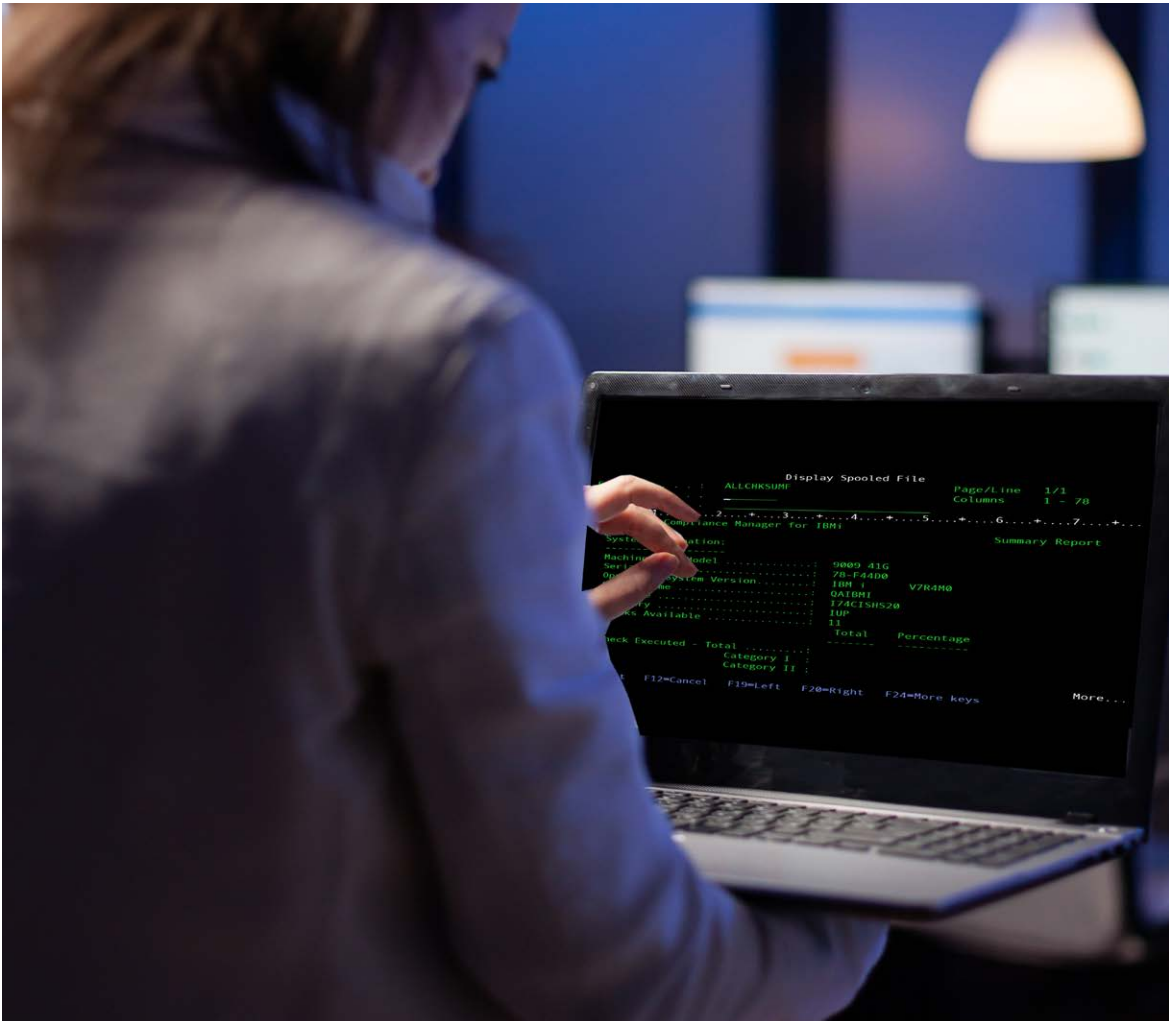
Dedicated IBM i Support

Unlike alternative competitors, whom approach compliance as part of broader monitoring, VCMi specializes in IBM i compliance exclusively. It’s aligned with IBM i’s unique architecture and directly integrates CIS Baseline adherence.

In contrast, the competitor hardens systems and modifies settings to change standards, rather than report on whether a system meets (or doesn’t meet) the CIS standard.

Competitive Strengths

- CIS Benchmarks fully codified for precise checks.
- Pass/fail assessments eliminate ambiguity.
- Streamlined reporting tailored specifically to IBM i’s architecture.



Key Differences at a Glance

Feature	VCMi	Generic Tools
CIS Integration	Strict	Partial
Compliance Automation	Full	Limited
IBM i Optimization	Yes	No

NIST and CIS Differences

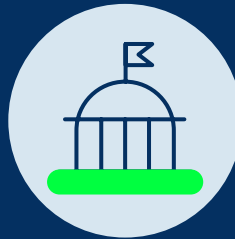
NIST and CIS are both cybersecurity frameworks, but they differ in their approach and focus. NIST (National Institute of Standards and Technology) offers a broad, risk-based approach to managing cybersecurity risks, while CIS (Center for Internet Security) provides more specific, control-based recommendations for hardening systems and improving security posture.

Real-World Use Cases



Financial Services

Banks looking to optimize their audit preparation can significantly reduce time investment and minimize staff hours by leveraging VCMi. This powerful tool streamlines the process of ensuring PCI DSS compliance, freeing up valuable resources for other critical tasks.



Government

For government entities navigating the complexities of NIST compliance, VCMi offers a powerful advantage. The automated checks not only facilitate smooth and successful audits but also significantly reduce the manual effort and time traditionally involved, leading to more accurate and efficient compliance management.



Healthcare

Hospitals entrusted with safeguarding patient data utilize VCMi's automated CIS compliance checks for continuous monitoring and proactive identification of potential vulnerabilities, significantly reducing the risk of data breaches and ensuring ongoing adherence to stringent regulatory requirements.



Manufacturing

Global manufacturers are increasingly turning to VCMi to facilitate their operational workflows according to the stringent CIS benchmark guidelines. This proactive approach ensures reliable security for their critical intellectual property and accelerates the acquisition of necessary regulatory approvals, facilitating quicker access to global markets and enhancing overall efficiency.

Future Roadmap

Because Vanguard builds its own technology in house and doesn't rely on mergers and acquisitions, the company has complete control over the current and future development of its products.

As a result, VCMi's development roadmap positions it as a future-ready compliance platform. The VCMi roadmap includes:

CIS Compatibility

The CIS standards change approximately every 18 months. VCMi will maintain compatibility with those standards.

Customization

While the main product will follow the CIS Benchmark to the letter, Vanguard will create custom baseline checks for any customers that want to deviate slightly from the CIS Benchmark.

Enterprise API Integration

Vanguard regularly develops custom APIs based on client requirements to improve efficiencies and accuracy. Eventually some of these APIs will be part of VCMi.

Custom Compliance Frameworks

Organizations with unique regulatory frameworks will gain tools to codify their specific requirements into VCMi.

Enterprise Dashboards

Because each enterprise has its own dashboard tool, the goal is to integrate VCMi into each dashboard to enable organizations to know at a glance if they are complying with the CIS Benchmark.



See VCMi in Action

Compliance doesn't have to be overwhelming. With VCMi, IBM i users gain a partner that automates effort-intensive tasks while boosting accuracy. Whether you're aiming to simplify reporting or solidify your position in audits, VCMi is the tool you need.

Contact Vanguard Integrity Professionals today to schedule a demo or consultation to see how VCMi can revolutionize your compliance management process:



702-794-0014



biz.dev@go2vanguard.com

Your compliance challenges end here.





About Vanguard Integrity Professionals

Founded in 1986 to help customers safeguard mission critical applications and data, Vanguard Integrity Professionals is the largest independent provider of enterprise security software for addressing complex security and regulatory compliance challenges. Vanguard continuously drives innovation in security software and technology to stay ahead of evolving regulatory requirements in an ever-changing threatscape. Led by some of the most knowledgeable minds in the cybersecurity industry our security solutions take the lead.