Cybersecurity Management Suite™ (CSMS)

Supports the successful deployment of a NIST CSF 2.0 cybersecurity process by coordinating tools, people, and tasks.

In today's fast-evolving digital landscape, enterprises require robust and scalable cybersecurity solutions to safeguard their infrastructure. Most organizations deploy a wide range of cybersecurity software to avoid hacks and breaches. However, they rarely implement unifying processes and controls that are required for these tools to be effective.

Common roadblocks to success include:

- Siloed Cyber GRC (Governance, Risk and Compliance) tools and processes working in isolation
- A lack of proactive management platforms
- Loosely defined or undefined networks and users.

As a result, hacks and breaches keep happening. Current cybersecurity solutions aren't working!

Introducing Cybersecurity Management Suite™ (CSMS)

How can an organization improve its cybersecurity posture? With Eracent's innovative Cybersecurity Management Suite (CSMS), a comprehensive cybersecurity management solution.

CyberSuite, for short, is an innovative Cybersecurity Continuous Compliance Automation (CCCA) management system. Acting as a central management hub, CyberSuite empowers organizations to control all aspects of their cybersecurity operations effectively to help ensure compliance with regulatory requirements and industry standards.

The Foundation of the Cybersecurity Management Suite

Eracent's CyberSuite is built on a trio of powerful services:

CyberDiscovery™

CyberDiscovery is a highly sophisticated scanning engine that provides in-depth insights into an organization's IT environment. CyberDiscovery supports both agent-based and agentless scanning across on-premises and cloud environments. With the proven ability to scale to hundreds of thousands of machines and endpoints, CyberDiscovery extracts detailed information from any computing device, ensuring full visibility and security assessment of IT assets.

Network Probe™

The Eracent Network Probe extends the power of CyberDiscovery with real-time, agentless scanning of all IoT and Cyber-Physical Systems (CPS) devices, networking hardware, and connected endpoints. It can scale to millions of devices, providing organizations with a complete, real-time picture of their network landscape, ensuring that no device goes undetected.

IT-Pedia®

IT-Pedia is a comprehensive, curated knowledge base that contains detailed information about millions of hardware and software products, as well as open-source components found in IT environments and applications. IT-Pedia includes details that cannot be found by discovery tools. This information typically requires extensive manual searching to locate, verify and populate into the databases of other tools. IT-Pedia provides enrichment data and normalization to enhance the value of business systems, and it gets them all speaking the same language. IT-Pedia also provides details about physical attributes, product use rights, and crucial insights such as end-of-life data and vulnerability assessments.

Advanced Capabilities for Total Cybersecurity Management

CyberDiscovery

As mentioned above, the CyberDiscovery module serves as a bridge between real-world IT environments and security frameworks. It enhances visibility, security, and risk management for IT assets, including all endpoints, devices, and installed software. CyberDiscovery integrates with data sources such as Eracent's IT Management Center (ITMC), ServiceNow, SCCM, and OpenVAS to collect high-quality asset data and provide comprehensive vulnerability assessments.

Software Bill of Materials (SBOM) Analysis

To provide deep visibility into application components, CyberSuite includes SBOM analysis through the Eracent SBOM Manager™. The SBOM Manager facilitates an automated approach for managing and analyzing Software Bills of Materials (SBOMs), focusing on cybersecurity and vulnerability assessment, open source license risk reduction, and obsolescence management. This module supports concurrent real-time analysis of thousands of application components, and it offers a centralized repository for storing all an organization's SBOMs.

By providing this integrated view, the CyberDiscovery Module and SBOM Manager support proactive cybersecurity management, helping organizations better understand and mitigate risks across their IT landscapes. SBOM Manager integrates with existing cybersecurity and discovery tools to ensure compliance and risk mitigation.

The Eracent SBOM Manager stands apart as a powerful solution for both software creators and software consumers who must meet the requirements of cyber mandates like Executive Order 14028, The Digital Operations Resiliency Act (DORA), The New York State Department of Financial Services 500 (DFS 500) and other legislation.

Risk Scoring & Management

Managing vast amounts of cybersecurity data can be overwhelming. Eracent simplifies this process with its proprietary Risk Score™ methodology, which condenses multiple risk factors into a single, quantifiable metric. Risk Score integrates data from:

- Real-time infrastructure scans
- Enterprise ticketing systems
- Asset management platforms
- Financial and HR systems
- LMS and contractual data,
- and many other sources.

This capability is powered by CyberDiscovery interfaces to third party tools and the Eracent ITMC Lifecycle™ suite, which includes specialized modules for Asset, Contract, and Software License Management.

Risk & Framework Management

With real-time risk scoring in place, organizations can build a holistic cybersecurity program, evaluating policy effectiveness and implementing industry-standard security frameworks such as CIS or the NIST Cybersecurity Framework (CSF 2.0). The Risk Manager and Framework Manager modules facilitate compliance and continuous security improvement.

Framework Manager

The primary function of the Framework Manager is to link formal requirements established in industry standards to the company's internal regulations, established in policies and procedures, and mapping responsibilities and technologies. The resulting benefit is that any implementation of a standard becomes organized and easily controllable, leading to significant cost reduction.

The Framework Manager module of CSMS offers the following functionalities:

- Defines implementation of popular industry security frameworks
- Defines Policies implemented in the enterprise together with corresponding Efforts and Practices
- Maps Policies, Practices, and Efforts to all applicable Frameworks
- Creates and executes audit schedules
- Maps the technologies applied in the enterprise to Frameworks
- Provides real-time measurements of Framework and Policy compliance, and
- Offers Frameworks and Policies governance capabilities.

Framework profiles and their branches define a way to measure the performance of the company at each level by defining the metrics and weights. The system's performance can be overseen using audit functionality, enabling businesses to review audit progress and take corrective actions as needed.

Risk Manager

The Risk Manager module allows customers to handle risks from identification to creating a response plan. Any identified risk goes through the following steps:

- Defining a Risk Event - a threat or event that can impact the company
- Categorizing the event and evaluating the probability of occurrence and the impact
- Assigning an owner to accepted risks and defining a risk-handling strategy
- Defining Risk Triggers—circumstances that can initiate the risk
- Implementing measures to reduce the probability of triggers, and
- Developing Risk Response Plans to mitigate the impact of potential risk events.

The Risk Manager contributes towards updating policies and procedures, reducing the probability and impact of emerging threats.

Business Data Manager

The Business Data Manager module focuses on comprehensive data management, helping enterprises track details about all processed data sets, including category, source, legal aspects, involved systems, third parties, ownership, storage, processing methods, and critical content. The following data parameters are tracked:

- Category and type
- Data Source
- Legal considerations
- Systems involved in processing
- Third parties involved
- Governance aspects (who owns the data)
- Technical aspects (how the data is stored and processed), and
- Information content (what critical information is processed).

How Can You Benefit From Using the Cybersecurity Management Suite (CSMS)?

Executive-Level Security Oversight

CyberSuite's unified approach enables executives to manage enterprise-wide cybersecurity from a single point of control. With real-time visibility, automated risk assessment, and powerful security governance tools, Eracent empowers organizations to establish and maintain an integrated, effective, and scalable cybersecurity program.

Stay ahead of cyber threats with Eracent CyberSuite – an all-in-one cybersecurity management solution!

To learn more about Eracent's other Foundational Data, IT Asset Management and Cybersecurity solutions, contact Eracent today!

Eracent, Inc.
519 Easton Road, P.O. Box 647
Riegelsville, PA 18077 USA

info@eracent.com
+1- 908-537-6520

eracent.com

 04-07-2025 rev.