

How to Optimize SAP SuccessFactors Incentive Management (SFIM) With Technical Health Checks



This guide outlines what a technical health check is, the problems it can solve, and how Canidium performs them.

How Technical Health Checks Optimize SFIM



Technical health checks are vital for maintaining the reliability, security, and performance of technology systems, ultimately supporting the overall success of an organization.



What is a technical health check?

A technical health check, also referred to as a system or infrastructure audit, is a process where an organization evaluates the general health, performance, and security of its IT systems, software, and hardware components.

The objective of a technical health check is to detect any current problems, weaknesses, or opportunities for enhancement. This process guarantees the system's dependability, stability, and effectiveness.

What are the benefits of a technical health check?

- ✓ Identifying Issues Early
- ✓ Improved Performance
- ✓ Enhanced Security
- ✓ Compliance and Risk Management
- ✓ Cost Optimization
- ✓ Future Planning



Are you experiencing?

Low rep adoption

User confusion

Shadow accounting

Lack of trust in SFIM software

Slow processing time

Lack of reporting

Lack of training

Challenging organizational changes

The Typical Elements of A Technical Health Check



System Performance Analysis

Evaluate the performance metrics of servers, networks, and applications to identify any bottlenecks or areas of suboptimal performance.

Security Assessment

Thoroughly examine security measures, including firewall configurations, access controls, encryption protocols, and vulnerability scanning, to identify potential weaknesses or areas of concern.

Data Backup and Disaster Recovery Evaluation

Review the organization's data backup strategies and disaster recovery plans to ensure that critical data is adequately protected and can be restored in an emergency.

Software and Hardware Updates

Check if the software and firmware versions are up-to-date and identify any required patches or updates to improve system stability and security.

Network Infrastructure Review

Assess the network architecture, bandwidth utilization, and network security to ensure efficient data flow and protection against threats.

Application and Database Analysis

Evaluate the performance and security of applications and databases, looking for any vulnerabilities that might expose the system to potential risks.

Compliance and Governance Check

Verify whether the system adheres to relevant industry standards, regulations, and internal policies.



What does a Canidium technical health check look like?



At Canidium, we focus on three main areas:

- ✓ Configuration
- ✓ Automation
- ✓ Reporting and Analytics

We provide a clear and concise blueprint for operational success with SFIM. We also offer go-to-market sessions to improve adoption rates and offer impartial guidance on your next steps.

Our process involves:

1. Interviewing key stakeholders and users
2. Conducting a System Assessment Impact Analysis
3. Taking an unbiased customer-focused strategic approach



By working with us, you will learn about any inefficiencies in your environment, and we will debug any unexpected behavior, optimize processes, and improve your workflows.

Ready to plan your technical health check?

[Reach out to our expert technical health check team to learn more.](#)

