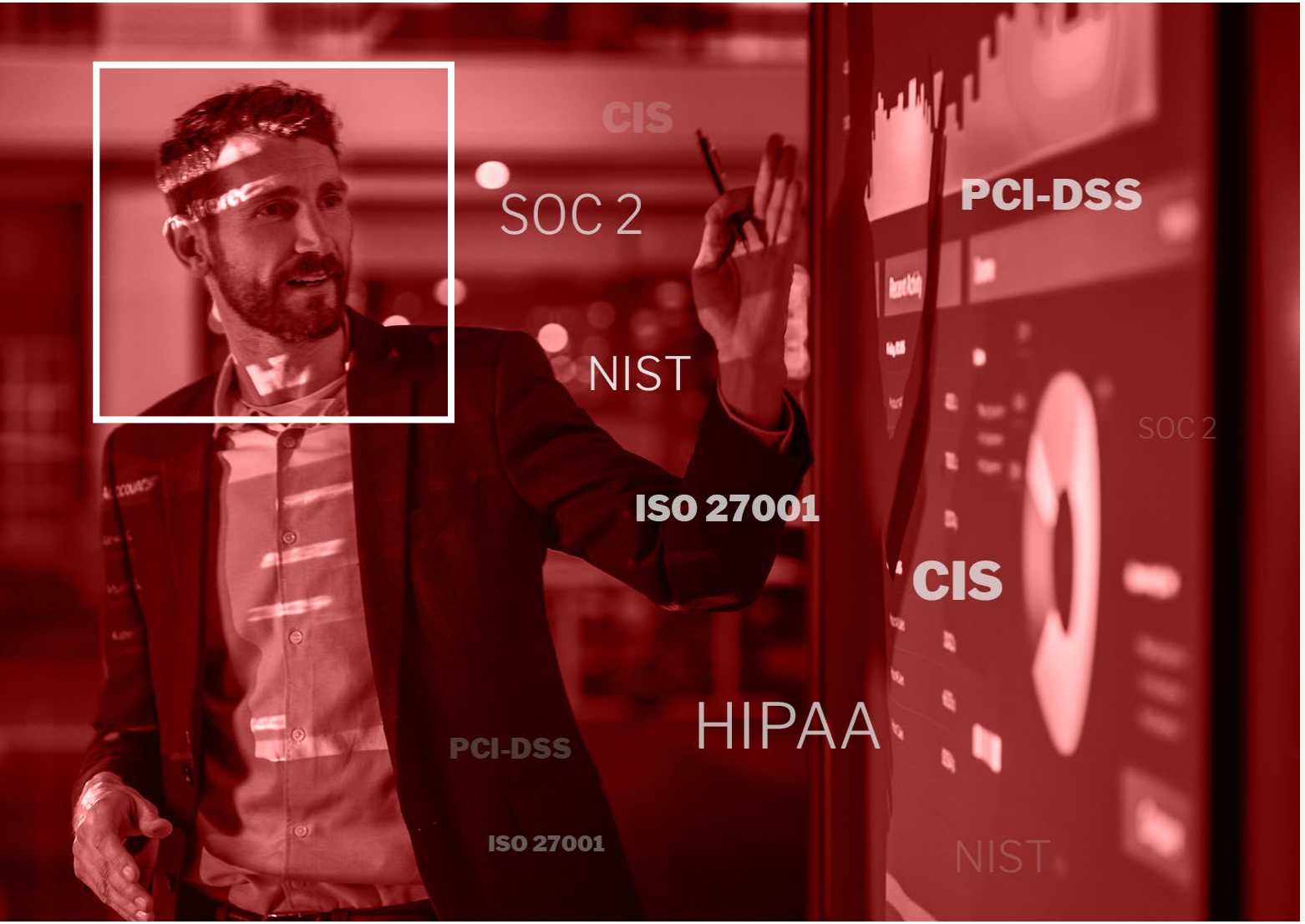


YouGov

SNAPSHOT SURVEY:

IT Compliance and Technology Audits

With the surge in hybrid-work, SaaS and cloud adoption, modern enterprises are facing resource and cost overruns to complete technology audits due to siloed inventories, poor data hygiene and inadequate process automation. This hinders adherence to security and compliance controls.

oomnitza

Summary

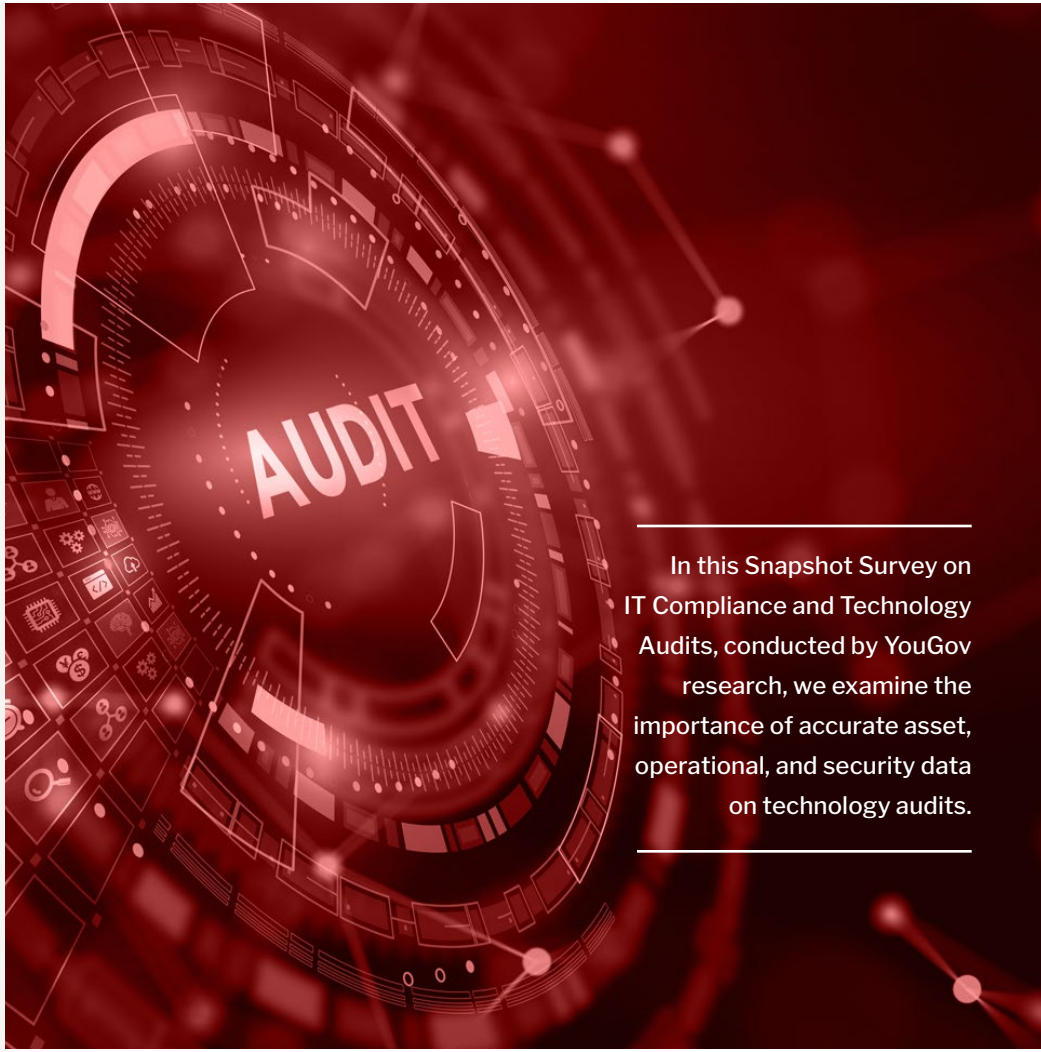
In today's dynamic business environment, the rapid adoption of technology has become paramount for driving efficiency and innovation. However, this creates additional challenges for IT organizations in the realm of technology audits and compliance, as it makes adherence to an ever growing list of compliance frameworks and mandates such as NIST, PCI-DSS, HIPAA, CIS, SOC 2 and ISO 27001 more onerous.

Within the context of these regulatory requirements, it is imperative to maintain an up-to-date and accurate inventory of all technology assets (hardware, software and cloud), who's using them, where they are, what vulnerabilities they have and the state of their security controls. This context forms the foundation for implementing effective security measures and demonstrating compliance.

The surge in hybrid and remote work, coupled with SaaS and cloud adoption, have added layers of complexity to maintaining accurate inventory controls. IT organizations have to look beyond traditional IT Asset Management (ITAM) and CMDB-based solutions, which often fall short in addressing the evolving technology landscape. Comprehensive asset lifecycle management and automated process workflows are essential for completing technology audits successfully and efficiently.

In this Snapshot Survey on IT Compliance and Technology Audits, conducted by YouGov research, we examine the importance of accurate asset, operational, and security data for technology audits.

The report sheds light on the impact of poor data hygiene, the challenges in maintaining technology inventories, resource and cost overruns in technology audits, and how well organizations are leveraging automated workflows to better orchestrate audit processes across multiple IT management and security tools. We underscore the need for strategic adjustments, increased automation and innovative solutions to manage the ever-evolving enterprise technology landscape.



Key Findings

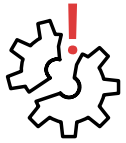
The research shows that data hygiene and accuracy issues are negatively impacting the timeliness, cost and quality of audits, especially in enterprises with 1000-5000 employees, and highly regulated industries such as utilities and infrastructure.

Inaccurate data is a significant issue, causing **46%** of respondents to experience considerable increases (10% or higher) in audit delays and costs.

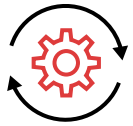
Enterprises with 1000-5000 employees were **27% more likely** to experience an increase in audit delays and costs (10% or higher).

47% of companies spent at least 10% more resources and money than their planned audit budget due to poor technology inventory data. This number rises to 55% in enterprises with 1000-5000 employees.

Improving data hygiene and incorporating more automated process workflows are essential for better adherence to security controls and faster completion of technology audits. The research shows that the majority of businesses acknowledge the need for improving data hygiene, establishing better processes and using more automation, and see these as areas they still need to address.



56% of companies reported the data accuracy of their CMDB was only 85% or lower with insufficient levels of process automation. This number rises to 67% in enterprises with 1000-5000 employees.



62% of organizations need to further automate their compliance assessment and technology audit preparation workflows to better adhere to security and compliance controls.

Almost 75% of utilities and infrastructure companies are exposed to undue security and compliance risks and need to better define and automate their compliance and audit processes.

The sections below show detailed breakdowns and analysis of the findings, including segmentation by business size.

The Importance of Technology Audits - Trends and Drivers

Technology audits are a necessary and important part of governance for all businesses. Failure to comply with regulatory mandates and security standards can lead to severe consequences, including security exposures, operational disruptions, financial penalties and reputational damage.

Several trends such as the increase in hybrid and remote work, the use of mobile technologies, and the surge in SaaS and cloud adoption, have added complexity to compliance initiatives and technology audits. However, these same trends increase the importance of governance and require enterprises to embrace improvements in processes, tools and automation to enhance the accuracy and efficiency of compliance audits. Examples include:

- The rise in remote work necessitates organizations to assess and ensure secure access to company systems, data handling outside the office environment, and compliance with labor laws in various jurisdictions.
- The proliferation of industry-specific regulations and cross-border data laws necessitates technology audits that comprehensively address compliance, data handling, and reporting, avoiding costly penalties and reputational damage.
- Technology audits now extend beyond internal systems to assess third-party vendors' security practices, emphasizing the need for rigorous due diligence and contractual agreements to safeguard sensitive data.
- As businesses migrate to cloud-based infrastructures, technology audits focus on ensuring data integrity during migration, cloud provider compliance, and the establishment of robust access controls.
- Traditional periodic audits are evolving into continuous monitoring processes, allowing businesses to identify issues in real-time, address them promptly, and stay agile in a rapidly changing environment.

The Impact of Inaccurate Data

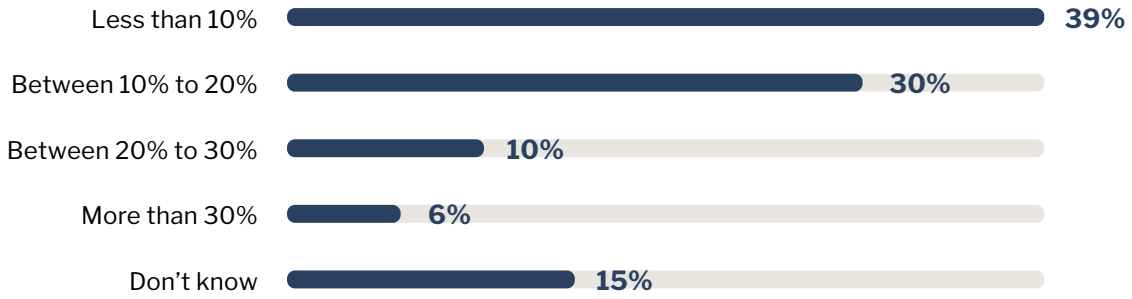
Comprehensive and accurate asset information is vital to complete technology audits successfully and efficiently.

Our survey unveils the impact of inaccurate technology, deployment, operational, and security data on technology audits.

Notably, 46% of respondents faced a considerable increase (10% or higher) in audit delays and costs, with 1000-5000 employee enterprises 27% more prone to such disruptions.

While most organizations use multiple tools and databases to prepare for audits, they face accuracy issues due to conflicting data from different tools. More tools do not necessarily equate to accurate technology data.

What is the negative impact that internal, regulatory and compliance audits have on your organization's resources due to inaccurate asset, technology, deployment, operational, and security data? Estimate the increase in audit delays and costs you have experienced.



of companies have experienced a considerable increase in audit delays and costs due to inaccurate asset data

KEY FINDINGS

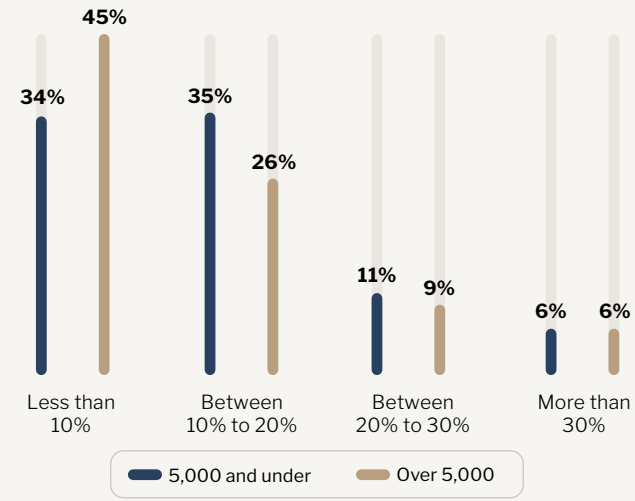
46% of respondents experienced a considerable increase (10% or higher) in audit delays and costs due to inaccurate asset data.

16% of organizations experienced a significant increase (20% or higher) in audit delays and costs due to inaccurate asset data.

Enterprises with 1000-5000 employees were **27% more likely** to experience an increase in audit delays and costs (10% or higher).

Utilities and infrastructure companies lagged the rest with **54%** experiencing considerable increases in audit delays and costs.

INCREASED AUDIT DELAYS
(BY COMPANY SIZE)



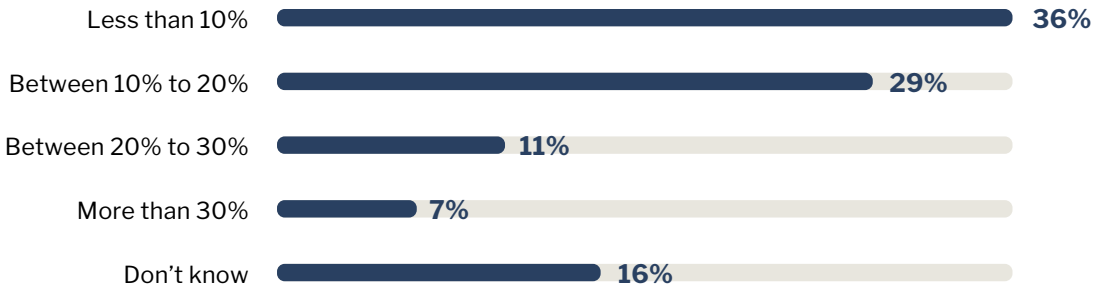
Throwing Resources and Money at the Problem

There are two resources that every IT organization is short of: time and money. Budgeting for technology audits is a necessity, however cost overruns are not only the audit overage itself, but also the impact to resources and investments in other primary value chain activities.

The survey exposes a significant financial strain, as 47% of companies exceeded their planned audit budget and resources due to challenges in obtaining and analyzing technology inventory data.

Navigating the complexities of siloed technology data is proving to be costly for enterprises, including the opportunity cost of resources pulled off other strategic projects.

As a follow on to the previous question, estimate the increase in audit resources and fee expenditures that your organization has experienced to complete its internal, regulatory and compliance audits due to challenges in obtaining and analyzing distributed asset, technology, deployment, operational, and security data?



of companies went over budget (10% or more) on audit resources and expenditures due to poor technology inventory data

KEY FINDINGS

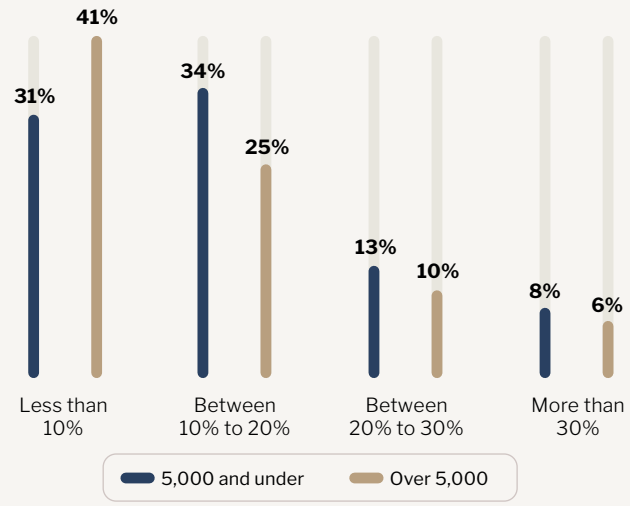
47% of companies spent more resources and money than their planned audit budget due to poor technology inventory data.

For **18%** of enterprises, audit resource and budget increases soared (20% or higher) due to poor technology inventory data.

Over half (55%) of enterprises with 1000-5000 employees faced audit resource and cost increases due to poor technology inventory data.

Enterprises with 1000-5000 employees were **32% more likely** to experience audit resource and cost overruns.

INCREASE IN AUDIT RESOURCES AND EXPENDITURES
(BY COMPANY SIZE)



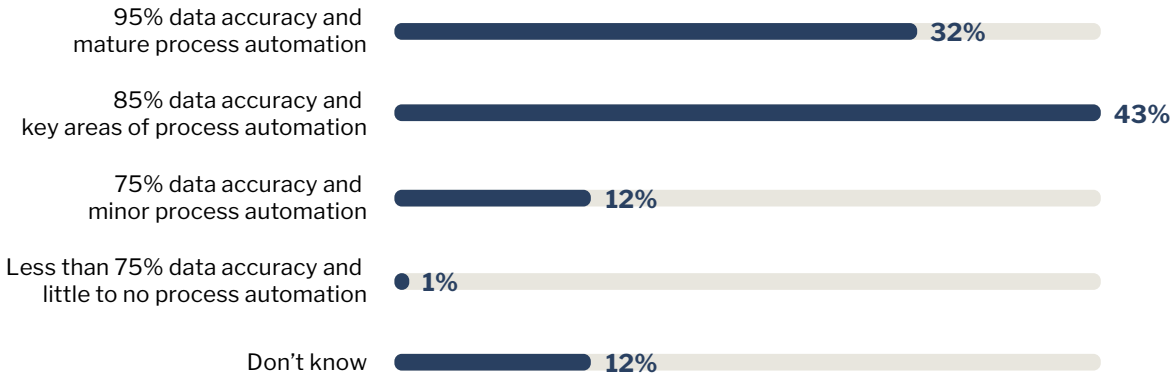
Data Accuracy: CMDB's are Not the Answer

Deploying and utilizing a Configuration Management Database (CMDB) effectively proves to be a persistent challenge, particularly in the areas of data accuracy and hygiene.

Managing the complexities of asset discovery, data synchronization and integration with multiple systems can be a daunting task, especially when many of these processes are manual and labor intensive. This results in discrepancies between CMDBs and actual infrastructure, impacting the overall effectiveness of IT operations.

Survey findings reveal that 56% of companies struggle with 85% or lower data accuracy and inadequate process automation, indicating that CMDBs alone aren't sufficient to manage today's diverse asset portfolios.

With regard to your organization's IT asset portfolio data accuracy and process automation, what best describes the current state of your organizations IT Service Management (ITSM) and Configuration Management Database (CMDB) investments? [Asset portfolio includes endpoints, applications, SaaS, network infrastructure, and multi-cloud infrastructure]



of companies reported 85% or lower data accuracy in their CMDB with inadequate process automation

KEY FINDINGS

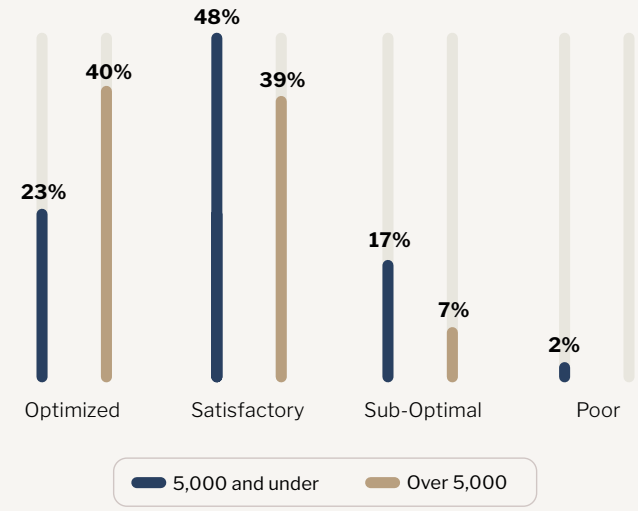
56% of companies reported the data accuracy of their CMDB was **only 85% or lower** with inadequate levels of process automation

32% of companies reported **95%** data accuracy and mature process automation. This is somewhat at odds with the increased audit delays, resources and costs associated with poor technology data hygiene reported in previous questions - indicating either over-confidence and/or the need for even higher data hygiene for audit purposes.

Two-thirds of enterprises with 1000-5000 employees indicated they had **only 85% or lower** data accuracy in their CMDB.

Larger enterprises (more than 5,000 employees) seem to have higher confidence in their technology data hygiene, although in their case, smaller percentages of inaccurate data can represent a significantly larger number of assets, thereby leading to higher audit preparation effort, costs and delays.

DATA HYGIENE AND ACCURACY
(BY COMPANY SIZE)



Compliance and Audit Process Automation

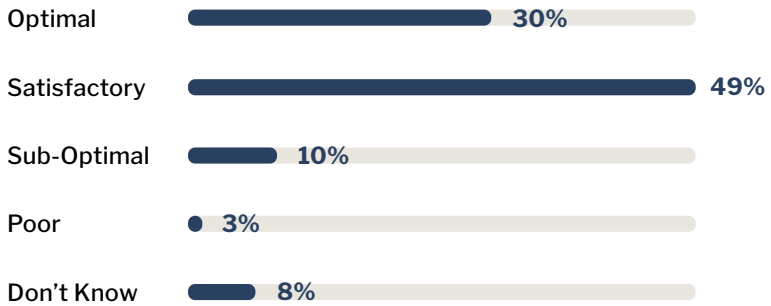
Compliance with multiple security frameworks and regulatory mandates requires an emphasis on automation.

Our survey examines the current use of automated process workflows in enterprise IT organizations.

While 30% of respondents indicated good adoption of automated and auditable processes, a significant 62% acknowledge the need for more automation to improve adherence to security and compliance controls.

As we have seen throughout this survey, the use of automated process workflows has a direct impact on the quality of technology inventory data, better adherence to security controls, and faster completion of technology audits.

Which of the following best describes the current state of your organization's use of automated process workflows across IT management tools and operational data to accurately validate and track adherence to security and compliance controls?



Optimal. Well-coordinated automated processes and tools with actions that are fully tracked, auditable and improved upon.

Satisfactory. Majority of defined processes and tool integrations automated. There is room for improvement, as compliance and security issues are experienced periodically.

of organizations need to further automate their compliance and audit preparation workflows to improve adherence

Suboptimal. Some processes that are automated with ad hoc use of tools. The organization frequently experiences compliance and security issues.

Poor. Majority of processes are manual and nominally tracked with ad hoc use of tools. The organization frequently experiences compliance and security issues.

KEY FINDINGS

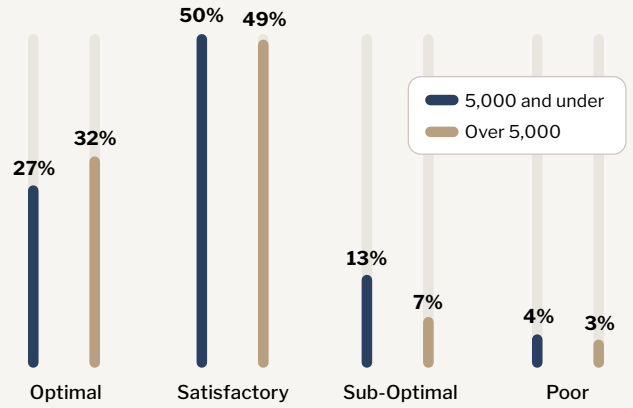
62% of organizations need to further automate their compliance assessment and audit preparation workflows to better adhere to security and compliance controls.

13% of enterprises frequently experience compliance and security issues and are exposed to unnecessary risk. These organizations would benefit from a fresh look at their end-to-end compliance needs and should invest in appropriate tools to automate their technology audit preparation processes to reduce audit delays, failures and fines.

Enterprises with 1000-5000 employees lag, with **two-thirds** needing to invest more in automated process workflows to adhere to security and compliance controls..

Almost **75%** of utilities and infrastructure companies are exposed to undue security and compliance risks and need to better automate their audit processes.

COMPLIANCE AND AUDIT PROCESS AUTOMATION
(BY COMPANY SIZE)



Research Methodology

The survey was conducted and data compiled by YouGov plc, an international research data and analytics group. The independent research surveyed 213 senior level information technology professionals from companies of more than 1,000 employees across a diverse set of industries within the United States.

YouGov

YouGov is an international online research data and analytics technology group with a mission to offer unparalleled insight into what the world thinks. As the pioneer of online market research, we have a strong record for data accuracy, a wide range of quantitative and qualitative research, and innovation. With a proprietary panel of over 22 million registered members globally, YouGov has one of the world's largest research networks.

oomnitza

Oomnitza provides an Enterprise Technology Management (ETM) solution for asset lifecycle management and IT process automation that empowers enterprise IT organizations to scale by orchestrating and automating processes across siloed technologies.

Our agentless, SaaS platform integrates with your existing IT, security and business systems to aggregate and correlate multi-source data into a comprehensive, accurate and actionable asset inventory for better technology data hygiene and audit readiness.

We enable organizations to confidently automate their technology workflows using standardized applications and low-code/no-code workflows to reduce manual tasks, service tickets, security risks and redundant technology spend.

Learn more at Oomnitza.com

oomnitza

GET STARTED TODAY

Request a Demo →

Take a Product Tour →