oomnitza

USE CASE

Enterprise Technology Orchestration for Automated IT Audits

Introduction and Context

The annual, semi-annual, or quarterly IT audit remains one of the most resource-intensive and time-consuming activities of IT teams. As compliance has grown in both breadth and importance, the emphasis on running audits efficiently and with greater accuracy has become more mission critical. The primary goals of an IT audit are:

- Ensuring all IT assets and systems are properly secured
- Ensuring all IT assets and systems have the proper levels of availability and redundancy
- Conducting a regular census of IT assets to identify aging assets and assist with procurement planning
- Identifying unused or stranded assets to improve usage rates and optimization

Over the past decade, a confluence of trends in IT, device management, and migration to cloud infrastructure has made the process of completing IT audits far more complicated. These trends include:

This growing diversity of assets makes it harder for IT audit professionals to assess the two key audit parameters - security and availability - of infrastructure, devices, and services, as well as the increase of systems that are not located on premise Different asset types live in different asset silos, each managed by a different type of software. Asset information required for an audit may reside in the CMDB, MDM. SAM, CSB, UEM and/or Cloud infrastructure management platforms. SSOs and employee directories may also contain key information about security and software usage, SaaS, and Cloud infrastructure.

In many cases, these systems are challenging to connect to and acquire data from; IT audit projects often (surprisingly) still live in large, complicated spreadsheets. Data collection, cleansing, and reconciliation involves multiple manual steps, which injects human error into audit processes. Enterprise Technology Orchestration (ETO) enables automated asset discovery and reconciliation across all these silos and generates a regularly updated “single pane of glass” view of IT assets that can dramatically reduce costs and completion times of IT audits. ETO also creates automated audit-centric workflows to simplify the spin-up and operational aspects of audits. Lastly, ETO can automate the crucial security auditing aspects to make an accurate census of which security controls are in place where and what systems are properly patched. By being agentless and flexible, ETO can easily integrate new data sources or asset classes and evolve with an IT estate over time.

USE CASE 1: AUTOMATED IT ASSET DISCOVERY AND INVENTORY

The first and most time-consuming part of any IT audit is figuring out who has what where. Autodiscovery within an ETO system allows audit teams to quickly survey and visualize the entire IT estate across all silos of assets. This discovery includes laptops, mobile, on-prem software, Cloud infrastructure, and SaaS. Oomnitza leverages existing agents in sub-systems (ITAM, CMDB, MDM, SAM, UEM) to discover and bidirectionally update all assets attached to corporate networks. By tapping into existing ITAM capabilities and aggregating the information, Oomnitza lets audit teams continuously calculate:

Total number of

physical assets in use by type (laptops, mobile), geography, and department

Detailed breakdowns

and trend data about assets in use by type, geography, and department

Location, type, & geography

of "stranded" (not in use) assets

Total number of SaaS

and cloud infrastructure licenses in use

Equally important, Oomnitza reconciles asset counts and identification across silos to ensure accurate accounting and reduce uncertainty resulting from duplicates, aged records, and inaccurate data due to human error.

USE CASE 2: AUTOMATED SECURITY STATUS COMPLIANCE ASSESSMENT

A key part of the IT audit is to assess the security status of the IT estate. This means identifying gaps in coverage where assets are not properly patched or protected by relevant security controls. Oomnitza collects and aggregates patch and security control information. saving audit teams the hassle of reconciling patch and control status across multiple asset systems. It also transforms the exercise into a living relational database, managing what has mostly been an exercise conducted in spreadsheets to a programmatic routine requiring minimal human counting and movement of data. Audit teams can quickly create workflows that collect all updated asset security information and export it via APIs into any auditing tool or into other platforms used to track security compliance and coverage. By acquiring and aggregating all asset data enterprise-wide, Oomnitza helps IT audit teams identify asset security coverage gaps. Oomnitza can detect and instantly report on the following:

#1. ACCESS CONTROL
status on all systems and assets

#2. ASSETS THAT ARE CORRECTLY
updated and patched

#3. ENDPOINT ASSETS
covered by EDRs, AV, Malware Protection, and other end-point protections

#4. ENCRYPTION STATUS
of assets (hard drives, data-at-rest)

#5. SECURITY RISKS
from unprotected network connections (outside the VPN)

#6. AVAILABILITY RISKS
to the IT state from security gaps

Building a business case for Oomnitza for IT audits

The average cost of an IT audit is high, ranging from the tens of thousands of dollars for smaller businesses to the hundreds of thousands or even millions of dollars for large multinationals. These estimates generally factor in staff time for data collection, aggregation, reconciliation, price of audit software and other audit tools, oversight by an outside entity to validate or manage the audit, and work disruptions caused by the audit. Compounding the issue is the growing shortage of trained and competent IT audit specialists. All of this assumes you're in compliance post-audit. If you're not, you can comfortably add a six or seven figure fine to that total, and those are just the direct costs, there's indicentals like loss of customer trust, reputations that can take years to build and seconds to destroy, etc.

Factoring in all of the above, you can build a business case for Oomnitza by first estimating the total costs of running an IT audit with your status quo. Next, tabulate the benefits of using Oomnitza, applying a back-of-the-envelope cost reduction or efficiency improvement to each benefit. Some of the concrete benefits might include:

- Reduced staff time on audits (general)
- Reduced time spent reconciling asset data across silos
- Reduced time spent correcting errors in asset audits injected by human error
- Reduced duration of audits enabled by automating key workflows
- Reduced reliance on outside oversight to run and adjudicate audits

- Reduced interruption to the general workforce due to IT audit processes
- Reduced costs of ongoing compliance efforts that piggyback on more efficient and automated IT audits
- Reduced costs of repeating key asset processes in case of unclear results
- Improved enterprise IT availability

Secondary benefits of running cleaner, faster audits are also considerable and should be emphasized. Secondary benefits for CIOs, CFOs, COOs, and CISOs may include:

Compare your tabulated status quo costs versus calculated estimated cost reductions delivered by an ETO such as Oomnitza. In our experience, Oomnitza can slice 25% or more from IT audit costs. Teams that adopt ETO gain considerable trust in their audit process and make it easier to conduct an audit, either with internal or external resources.

This exercise should paint a definitive picture of the value of Oomnitza for IT security. Beyond these calculations, make sure to value the improved trust in systems and peace of mind resulting from creating a single, accurate, reconciled system of record as a foundation underpinning the most critical IT security tasks.

About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By consolidating technology asset data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks, and ensure great employee experience and productivity. Oomnitza is headquartered in San Francisco.

www.oomnitza.com