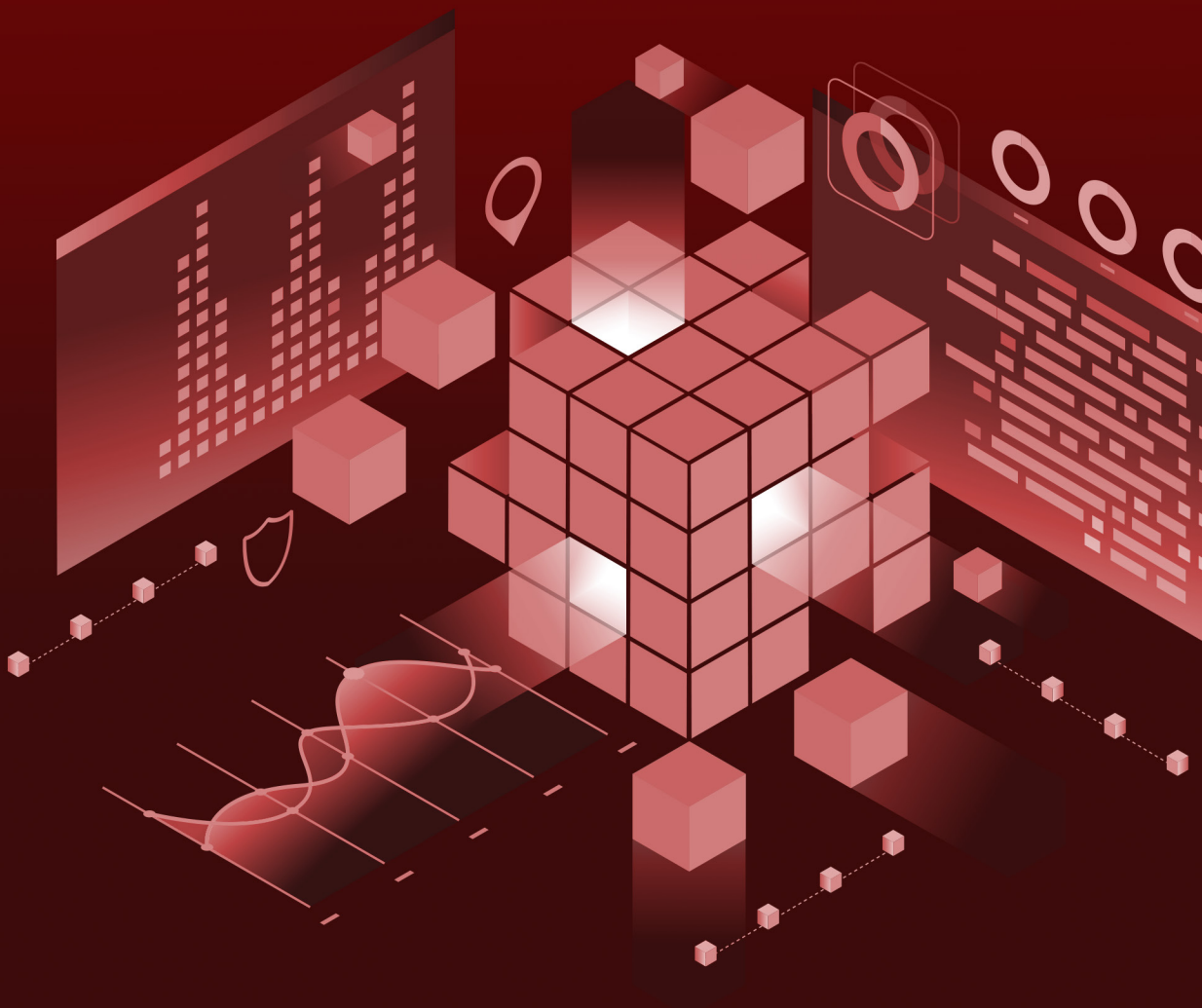
omnitza

Continuous Audit and Compliance Readiness & Enterprise Technology Management

From Scope to Evidence



ITOps, SecOps and Governance Risk and Compliance (GRC) staff use an array of tools and data to mitigate security posture exposures, ensure business resiliency, and protect sensitive data. However, audit readiness and compliance validation remain a top, impactful enterprise challenge.

66% of organizations failed at least one audit over the last three years[1]

Organizations spend **$3.5M** each year on compliance activities[2]

Organizations consume an average of **58** working days each quarter on compliance audits[2]

Why? There are two significant contributors. First, asset / technology and operational intelligence, across the myriad of users, endpoints, applications and infrastructure, is siloed and fragmented. The higher order need to efficiently aggregate, correlate, and analyze the information is affected by the disjointed data that exists within different divisions, departments and management tools. Second, the broad array of tasks to assess control details, validate policy compliance, respond to violations and produce evidence is human resource intensive and error-prone. These data and workflow issues are exacerbated by the dynamics of today's hybrid workplace and the more fluid use of software/SaaS and cloud resources.

With increased audit frequency and range needed to meet expanding internal, industry and regulated specifications, how can organizations reduce complications, delays, and expenditures? More so, how can organizations progress towards continuous audit and compliance readiness by automating audit processes from Scope to Evidence.

Impactful Challenges

While small enterprises often pursue a cloud-first strategy, most enterprise organizations are on a cloud migration journey with growing private cloud and public cloud activity. The larger the company, the more distributed the environment — and the more siloed divisions and IT domains become. The global pandemic served as an accelerant to push more infrastructure and applications to the cloud, to propel digital transformation initiatives, to promulgate shadow IT/development, and to surge hybrid workplace adoption. The net effect of which has introduced audit readiness challenges:

- Audit data is siloed and fragmented, preventing timely and accurate analysis
- Compliance to often poorly maintained controls is less assured
- Less controlled use of cloud resources introducing new exposures
- Remote worker policy adherence deviation
- Audit processes have become more and more resource intensive
- Increases in audit delays, re-audits and unplanned expenditures
- Inefficient audit collaboration between business units
- Less confidence in an enterprise view of security posture

Beyond operating environment dynamics, it is not uncommon to have massive asset/technology datasets, many of which being incorrect, incomplete, duplicative or out of date – preventing effective analysis and control rationalization. It is equally common to not only find data discrepancies between business units, but also to discover that business units are tracking things differently against a common control framework. As most audit processes have many manual tasks, it becomes challenging for GRC teams to ask their peers to spend inordinate amounts of time and resources to support audits, and then to take corrective actions – often with unsubstantiated information. Inaccurate risk identification and slow problem resolution also affect how risk-based strategic and operational decisions are made.

Organizations reported audit non-compliance an annual average of **6 times** and **$460k** in fines[2]

30% of organizations reported between 10-20% increase in audit delay and costs[3]

94% of organizations report facing secure compliance and/or privacy issues in the cloud[2]

69% of cyberattacks started with an exploited mismanaged internet-facing asset[4]

The impact of these challenges manifests in broad operational control gaps, added time and cost, and poor decision making. Audits become more prolonged or delayed. Risk identification inaccuracies also result in delayed identification and mitigation of policy violations. In additional to frequent audit issues, there are added or unplanned audit expenditures, and in many cases, the cost of penalties and refactoring of enterprise procedures and controls. At minimum, the inability to identify, track and assess an enterprise's IT estate not only fails to satisfy mainstream security and IT management framework specifications, but introduces exposure to cyber-attack and data leakage. At worst, added delays, costs, fines, and resource consumption can deprecate the trust that GRC teams need to build with their business partners across the organization.

Reducing Complexity

The universe of security and IT management frameworks can be daunting, but there are many policies, procedures and controls that are common across popular frameworks, standards and compliance requisites that most enterprise organizations will require. The key is to identify the key frameworks and mandates that must be adhered to satisfy internal and external audits. Whether it's NIST Cybersecurity Framework or NIST SP 800-53, ISO 27000 series, SOC2 and CIS controls, HIPAA and HITRUST CSF, CPPA and GDPR, PCI-DSS and SOX, FISMA and FedRAMP, or COBIT and COSO — organizations will choose a framework(s) and map common specifications, policies and controls. This task becomes more evident when supporting multi-national and cross-industry regulations.

Regardless of the framework, the three common control areas are that of asset intelligence, IT management, and protection mechanisms. Asset/Technology Intelligence incorporates endpoints (e.g. laptops and desktops), applications (e.g. software and SaaS), and network and cloud infrastructure (e.g. routers, switches, servers, storage and virtual resources). IT Management (inclusive of Identity Access Management) incorporates controls regarding ownership, access, entitlements, configuration, and lifecycle management. Protection mechanisms incorporates a wide variety of defenses such as endpoint protection, system encryption, vulnerability assessment and firewall/filter technology.

To streamline and scale auditing processes, organizations can deploy the respective set of policies with related controls that are used to verify adherence to compliance specifications, and then monitor, report, mitigate and refine. For example, a policy for compliant virtual systems that operate in a payment processing environment would include: running an approved configuration, having encrypted storage, having managed detection and response MDR) active, having an active owner within an authorized team, and consistent management (access) during a three-month interval. A compliance workflow would establish, monitor and remediate deviations related to these controls that support the policy.

Policy and control groupings, when used in conjunction with a process automation platform, can reduce audit and compliance complexity, as well as lower the cost of audit performance. GRC professionals, working with their IT operations and security peers, map each set of policies based on user, ownership, location, asset/technology security and operational state conditions. Effective policy mapping coordination among IT staff will also facilitate means for GRC teams and business units to identify business requirements and contractual obligations that have their own compliance requirements, as well as exceptions. However, this collaboration has reduced value if utilizing incomplete, out-of-date, omitted, or conflicting audit data. Data incongruity effects both evidence generation and exposure resolution efforts – and is the adversary of advancing process automation adoption and growth.

32% of organizations use 11 or more tools/databases for audits[4]

75% of organizations use spreadsheets as a key tool for security posture management[4]

40% of organizations cite accuracy issues due to conflicting data from different tools[4]

76% of organizations cite audit difficulties with data aggregation and interpretation[2]

To effectuate the reduction in audit and compliance complexity, GRC teams need to cut through the siloed departments, people, management tools and data to establish foundations for evidence and reporting preparation. While process automation maturity varies, the continued use and reliance on multiple tools and databases to fulfill internal and external audit requirements and workflows does not equate to operational efficiency or evidence accuracy. A recent survey[4] indicated that nearly a third of organizations use more than 11 tools for auditing, and that spreadsheets still represents a key aspect of audit analytics and reporting. Given the volume and fluidity of technology use at home, on-premises and in hybrid cloud, audit tool consolidation and IT estate coverage is crucial.

It is not only challenging to coordinate data requests across different teams, but often the data provided is not in a standard format or the data from different tools is conflicting. This issue does not negate the use of dedicated attestation-based compliance tools which have become a staple for auditing programs. This issue lies with the validation of technical controls used to enforce a policy. Aggregation of data from different IT management tools used by different teams and departments, at the API-level, can provide more efficient means to obtain and reconcile control data. But when it comes to audit accuracy, automated data aggregation, correlation and conflict resolution are inseparable. Improved data accuracy, as applied against a set of control rules, enables the identification of adherence or deviation from policies across asset/technology, IT management, and protection mechanisms.

Audit Readiness Automation Considerations and Enterprise Technology Management

How are organizations keeping pace with the technical controls given on-going business, user and technology dynamics? It begins by establishing an integrated system of record for asset technology. This requires access to the data within IT management tools that various teams use across IT domains – albeit each team and tool has varying operational context and controls. Some enterprises utilize multiple CMDBs and assemble various asset management tools, but there typically is no one central source of truth. Most enterprises have several sources that might conflict with each other or may not be regularly updated. This manifests in present-day auditing gaps.

55% of organizations have less than 75% asset intelligence coverage[5]

39% of organizations cite issues to complete hybrid IT inventory due to frequent asset change[4]

53% of organization report remote workers deviating from security policies and controls[5]

Over a **third** of organizations cite compliance, visibility, and policy enforcement challenges[5]

Automation relies on accurate data, and "you can't manage what you can't measure." Which endpoints have vulnerabilities, inactive defenses, or have defenses that have not been maintained. What portfolio of applications are installed or being accessed in the cloud. What software or SaaS use is unauthorized. With the pervasive use of cloud computing, when and where are new instances of cloud workloads being spun up. Who owns them? What changes were made — are they correctly configured or exposed. The same is true for private cloud and network resources.

It is this matrix of data that organizations use to apply a policy (guidelines to be met) that drive the processes (actions to be taken) and procedures (detailed steps that comprise the action) — these three elements serve as the basis for automation. Audit and compliance process automation needs to establish and periodically refine compliance policies and their controls to ensure successful execution.

Key Compliance and Audit Readiness Process Automation Considerations

1. Ensure GRC, security and IT teams have standardized on a framework(s) and specifications in order to enable a mapping of common policies, and monitoring and tuning of their controls
2. Increase the appropriation and accuracy of technology/asset lifecycle data and security state
3. Automate manual intensive audit processes across the IT organization
4. Build flexibility in monitoring and reporting to adjust for new requirements and different auditors
5. Move to persistent audit readiness to address the ephemeral nature of user, endpoint, application, and network and cloud infrastructure

Enterprise Technology Management (ETM) provides a platform that enables key business process automation for technology and IT, and delivers the necessary system of record and workflow flexibility to facilitate continuous audit and compliance readiness.

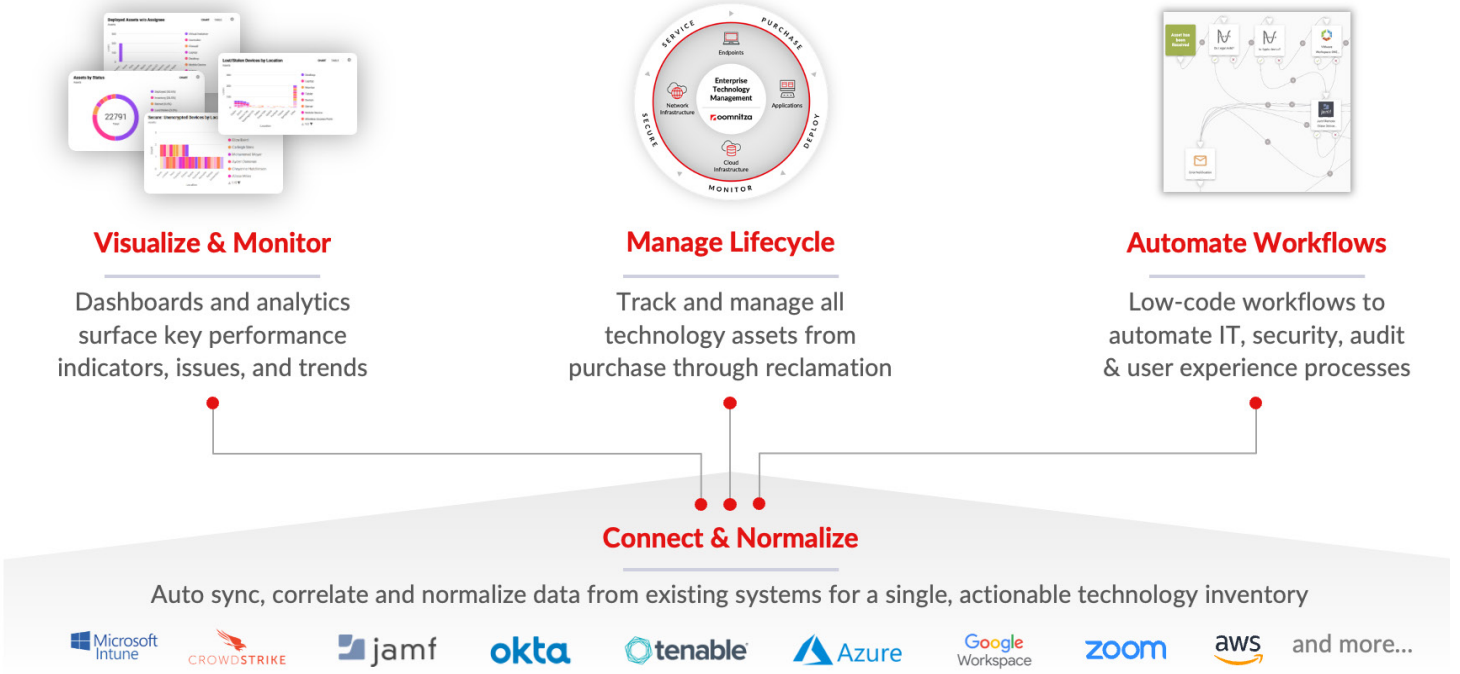


Figure 1: Enterprise Technology Management Framework

ETM platforms apply multi-source data normalization and advanced correlation that allow security and GRC staff to be better equipped to analyze and interpret policy compliance information. As such, lifecycle management, from purchase to end-of-life, becomes crucial in the audit process. This allows security and GRC staff to consolidate compliance information, have more standardized analytics, gain greater insight, and improve exposure remediation - across an enterprise's entire IT estate. While audits are an assessment of adherence over a given time period, it is imperative to rectify identified deviations and remediate issues going forward since each completed audit. Ultimately, organizations need to move from periodic inspection and reporting to persistent audit readiness and compliance exposure mitigation.

With an ETM platform, audit reporting preparation is always available, incident management is more proactive, exceptions are reduced, audit completion becomes more predictable (and less costly), and audit workflows are more easily tuned.

End to End Audit and Compliance Readiness Process Automation

The objectives for an automated audit and compliance readiness process is to increase risk mitigation efficacy and reduce audit delays, gaps, costs and penalties. This process encompasses steps to aggregate and cross-correlate audit data, create workflows with related policy controls, report and monitor adherence, and facilitate problem resolution. As depicted below, the process, from Scope to Evidence, is comprised of four parts: scoping, assessment, mitigation and evidence generation.

Figure 2: Audit Readiness and Compliance Validation Process Automation

Scope. Identify the breadth of requirements needed to satisfy internal and external audit specifications. Determine the roles, asset technologies and technical controls in scope. Oomnitza directly integrates with an organization's existing IAM, IT and security management tools allowing operators to easily define rules to track adherence to a wide array of configuration, access, ownership, management, and security requirements. Robust analytics allows for easy building of interactive security and compliance dashboards and reports for stakeholders and auditors.

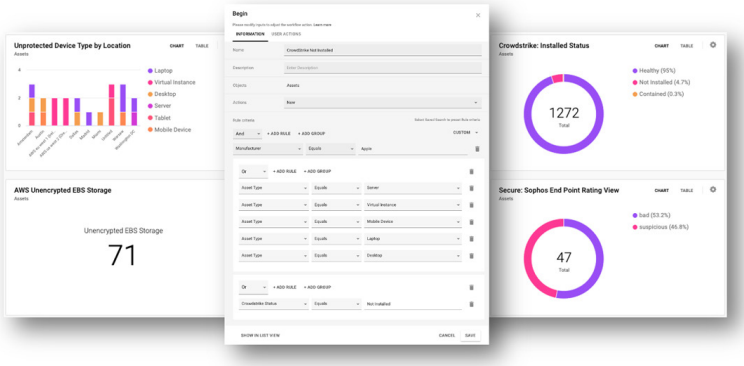


Figure 3: Audit Readiness and Compliance Validation Process Automation: Scope

Assess. Oomnitza makes defining, monitoring and responding to policy violations easy through its low code, WYSIWYG workflow editor. IT professionals can easily create simple to complex workflows to identify security and management policy issues and gaps across endpoints, applications, network infrastructure and cloud infrastructure. Workflows are easy to understand, maintain and standardize — offering simplified rule editing with available attributes and operators.

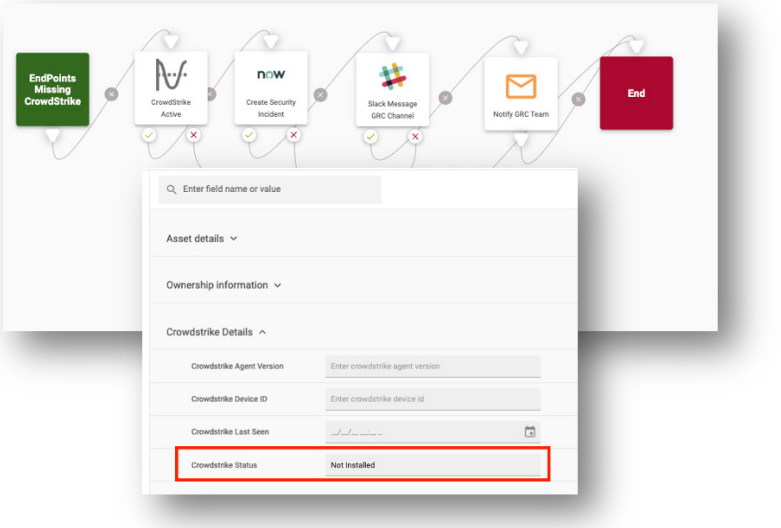


Figure 4: Audit Readiness and Compliance Validation Process Automation: Assess

Mitigate. Oomnitza not only monitors and reports policy adherence and issues, but allows IT staff to automatically initiate remediation or proactively invoke compensating controls. Workflows can trigger notifications, approval requests, control installation or reactivation, owner reassignment, isolation and deprovisioning actions and more — leveraging an organization's existing IT tools and ticketing.

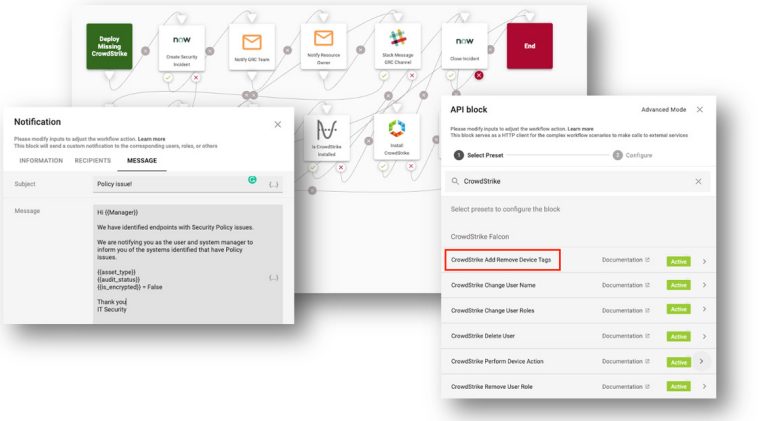


Figure 5: Audit Readiness and Compliance Validation Process Automation: Mitigate

Evidence. Oomnitza automates evidence gathering and report generation tasks to enable GRC managers and auditors to substantiate adherence. Audit, compliance and corrective action details are always available at the operator's fingertips to produce reports or export data. Compliance information can be readily sent to executives and LOB operators or incorporated into external BI systems. Technology security and lifecycle state context can be shared via API to other IT management, security and logging tools.

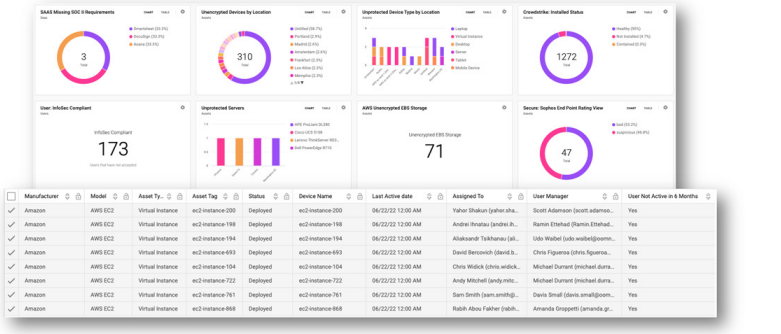


Figure 6: Audit Readiness and Compliance Validation Process Automation: Evidence

Calibration. To enable continuous improvement, Oomnitza facilitates ITOps, security and GRC teams to collaborate to refine workflows, policies and reports based on new requirements, exceptions, gaps, controls and IT management tools. With a centralized process automation platform, these teams can periodically extend workflows and data sharing, update rules and reports, and invoke more stringent remediation actions to support a wider array of operational audit and compliance conditions.

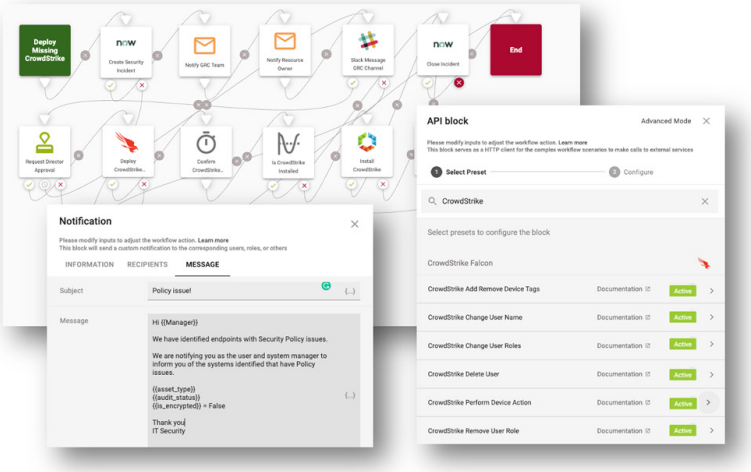


Figure 7: Audit Readiness and Compliance Validation Process Automation: Calibration

Continuous Audit and Compliance Readiness

Enterprise Technology Management solutions provide a platform for business process automation that delivers accurate asset technology intelligence, integrated workflows, and reporting analytics that enable GRC, security and IT teams to achieve continuous audit and compliance readiness. An approach that not only advances audit efficiency, but one that keeps pace with today's modern enterprise IT estate, new business initiatives, and evolving internal and external compliance requirements.

49% of organizations expressed room for improvement in their workflows due to periodic security and compliance issues[3]

51% of organizations anticipate automation would reduce time spent being audited[2]

50% of organizations anticipate automation would increases responsiveness to audit evidence requests[2]

1 ESG Research: 2021: State of Data Privacy and Compliance
2 Vanson Bourne/Telos: 2020 Survey, A Wake Up Call: The Harsh Reality of Audit Fatigue
3 You-Gov/Oomnitza: 2022 State of Audit Readiness report
4 ESG Research: 2022 Security Hygiene and Posture Management
5 CyberSecurity Insiders: 2022 Attack Surface Management Maturity report

About Oomnitza

Oomnitza offers the industry's most versatile Enterprise Technology Management platform that delivers key business process automation for IT. Our SaaS solution, featuring agentless integrations, best practices and low-code workflows, enables enterprises to quickly achieve operational, security and financial efficiency leveraging their existing endpoint, application, network infrastructure and cloud infrastructure systems. We help some of the most well-known and innovative companies to optimize resources, mitigate cyber risk, expedite audits and fortify digital experience. Learn more at Oomnitza.com.

oomnitza

Schedule a solution demo to see what powerful Enterprise Technology Management can do for you.
oomnitza.com /request-a-demo