ivanti

# Compliance for Today's Complex Audit

A modern, people-centric approach to removing the risk, cost and disruption from compliance efforts

## Introduction

Compliance audits make people nervous. IT staff, in particular, worry about whether they've actually complied with confusing and operationally challenging regulatory mandates. They worry about whether they can credibly prove compliance to potentially skeptical auditors. And they worry about how badly an audit "fire drill" will disrupt their team and consume productivity that's badly needed elsewhere.

This state of worry, however, isn't compulsory. With a people-centric, policy-automated approach to IT operations, you can reduce the risk of non-compliance dramatically. You can provide auditors with impressive, credible documentation of your compliance measures. And you can minimize compliance costs by ensuring that your IT operations are always inherently audit-ready.

Best of all, this exceptional level of compliance confidence can actually be a secondary benefit of your people-centric, policy-automated IT operations. The primary benefit is the ability to connect your people to the digital resources they need to do their jobs every day — faster, more securely, more accurately, and with less labor — even as your digital business keeps changing and expanding.

People-centric, policy-automated IT is thus a win for compliance leaders, IT teams, employees, the business and its customers.

## Why Compliance Hurts

Compliance demands that an organization's behaviors be governed rigorously by policies. These policies are typically defined in terms of generalized principles. Compliance also demands credible documentation that those policies were, in fact, operationalized and enforced universally across the organization.

IT compliance is worrisome, painful, expensive and disruptive because IT was never designed with such demands in mind. Instead, the evolution of IT has been driven by forces that include technology, expediency and organizational appetite for risk. When the business required PCs, IT had to deliver PCs. When it demanded CRM, IT delivered CRM. When it demanded analytics, IT delivered analytics. IT leaders and their supporting teams have done a remarkable job over the years of continually delivering game-changing technology to the business — despite limited budgets, conflicting vendor claims and an unprecedented requirement for non-stop learning.

But in the crush of relentless demands from the business to deliver the right technology at the right price with the least risk, compliance was never front-and-center. The result is an IT operations model that is fundamentally at odds with compliance in several ways, as outlined in the following chart:

| | IT Operations Model | Compliance Model |
|---|---|---|
| Operating Principle | Expediency: Get things done when the business needs them done, within budget/staffing constraints. Don't let the perfect be the enemy of the good. Make any necessary improvements next quarter. | Policy: Do everything in accordance with regulatory mandates. Errors and shortfalls are unacceptable failures that can result in fines, conduct penalties and other adverse consequences. |
| Organizing Unit | Technology: Operations are organized by infrastructure (servers, storage, networks); by application/resource type (ERP, CRM, email); and/or by function (developer, ops, security, support). | People and their behaviors: Determine the who, what, when and how. Did any employee see data they shouldn't have seen? Could a non-employee masquerade as a privileged user? How quickly can you revoke a terminated employee's access rights? |
| Risk Threshold | Corporate: Decide how much risk the business is willing to accept in its pursuit of competitive advantage, market share and other objectives. | Governmental/social: Decide how much risk regulators believe is acceptable for their constituents individually and for society as a whole. |
| Rationale for Automation | Primarily economic: Automate to cut labor costs significantly and/or prevent errors that also have significant costs attached. | Primarily governance: Automate to ensure that everything everywhere is always done according to policies currently in force. |
| Documentation | Secondary: First, get the job done. Good outcomes are their own documentation. Reports are only valuable insofar as they help us understand and solve problems. | Essential: Credible documentation of consistent, reliable operationalization of policies is indistinguishable from operationalization itself. If it's not auditable, it didn't happen. |

These disconnects explain why — as things stand today — IT compliance is almost invariably a costly, uncertain and disruptive after-the-fact burden that companies have to pile on top of their already considerable technology investments. Because compliance isn't built into IT, organizations struggle to impose policies on multiple, disparate access-control mechanisms. They waste hours they can't spare cobbling together audit-worthy reports from disparate log files — not to mention the constant back and forth to refine auditor requests with more and more data. And despite these efforts, organizations still approach compliance audits with fear. Worse yet, the outcomes of those audits often include penalties for the business and more problems for IT — problems that include even bigger to-do lists and a loss of credibility with upper management.

Clearly, there must be a better way.

## People-centric

IT operations remain organized around hardware, software, and data. This is a holdover from the beginnings of IT, when technology resided entirely within a data center and end users sat at static, fixed-location terminals. Even IT organizations that have responded to the digital enterprise with mobility management tools still typically focus on hardware and software — i.e. the end-user's device and its OS, MAC address, etc.

But the center of both IT and compliance is the person, not their device. More specifically, for IT to become innately compliant, its management of every digital work session must be driven in real time by:

- **The Person's Identity Attributes**

It's not enough to merely authenticate a person's role. Access to digital resources must also be determined by a person's attributes and responsibilities. Job title/level, LOB or department, current project/team assignments and the like all determine whether any given person should access any given resource at any given time. Some information may reside in an HR system. Some may be determined by an LOB or departmental manager. But this information about any individual actively attempting to access digital resources is essential for compliance, security and alignment with the business.

- **The Context of the Person's Work Session**

Compliance requires more than just knowing that a legitimate employee is using a legitimate device. The context of any digital work session is critical as well. Are they logging in from a coffee shop with non-secure public Wi-Fi? From an anomalous location at an anomalous time? Have they signed specific attestations required by the compliance organization? Truly people-centric IT will factor the answers to these and other questions into its real-time management of the individual's digital workspace.

## Policy-Driven

Policies are simply rules that govern behaviors. In the case of IT compliance, policies are rules that govern IT processes and user access rights in accordance with mandates that come from multiple organizations outside the enterprise.

As noted above, this is in marked contrast to the typical IT organization's operating "rules" — which are driven by the demands of the business and tend to be somewhat limited in both their logic and parameters: respond to new privilege requests as soon as possible, don't allow network access from an unrecognized endpoint, flag excessive failed access attempts, etc.

For IT to become innately compliant, it must therefore gain the ability to define, store, enforce and modify rules with more parameters and greater complexity as required by external agencies. So, for example, IT may need to adopt a liberal geo-fencing policy for collaboration tools, a more constrained geo-fencing policy for the bulk of its enterprise applications and an even stricter geo-fencing policy for applications that include customer PII. Policy then needs to be enforced based on the context of the user to ensure they are enforced.

This policy enablement isn't just necessary for fulfilling the requirements of regulatory mandates operationally. A centralized, well-managed policy repository is also something every regulatory auditor will expect to see as evidence of an organization's due-diligence compliance program.

## Automated

Without effective automation, policies are almost impossible to enforce and are just words on a page. Policy-driven automation of user workspace controls is foundational to the compliance-enablement of IT operations for several reasons, including:

- **Compliance confidence.** Compliance that depends on manual processes, homegrown scripts and other sundry mechanisms is prone to error and omission. Compliance managers and auditors can't trust policy enforcement mechanisms that aren't fully automated.
- **Real-time context response.** Only with automation can IT operations respond immediately to policy-relevant conditions. So, if a context parameter such as location, time or network connection type violates an access policy, the system can respond appropriately in real time.
- **Audit-ready documentation**. Automated policy enforcement can also provide a credible source of self-documentation, since all access attempts and allows/denials can be captured in the same system that performs them. The result is a unified and highly credible audit report.
- **Reduced compliance workloads.** If compliance policies require IT staff to do more, then payroll budgets will always be a constraint on compliance execution. Automation removes this constraint — enabling IT to accommodate additional compliance requirements over time without additional funding.
- **Policy adaptability.** In a poorly automated environment, every change in regulatory requirements requires staff to re-learn rules and re-program scripts — if they can even find and/or understand them. A well-designed automation engine makes policy changes painless by allowing IT staff to simply re-define rules with a few keystrokes.
- **Self service and delegation.** Automation also enables LOB staff and managers to initiate actions directly without waiting for manual IT. This is invaluable in situations such as an employee firing — since it allows HR to revoke that user's privileges instantly and universally with a single mouse-click.

## The Bottom Line

For IT to fulfill ever-changing compliance mandates effectively, credibly and cost-efficiently, compliance must become an intrinsic aspect of IT operations. That means making IT more intrinsically people-centric — and providing IT with a unified mechanism for managing and automating compliance-related policies across the enterprise.

To ensure compliance, security and business alignment, IT needs an automated means of enforcing access policies based on user identities and roles, session context and a set of well-defined rules governing who is allowed to access what under which conditions.

## Audits Can Be Awesome

Regulatory mandates keep getting more technically demanding. The potential adverse consequences of audit failure keep growing, too. The benefits of audit-ready include:

- **Reduced compliance risk.** Reliably automated, rules-based governance of user access privileges reduces dramatically the risk of events and actions that violate mandates regarding the protection of customer data, transaction integrity and other requirements.
- **Highly credible audit documentation**. Compliance isn't just about being compliant. It's also about proving compliance. Audit documentation generated by the same system that enforces enterprise policy controls is far more likely to satisfy even the most demanding auditor than reports cobbled together from disparate logs.
- **Minimized compliance costs.** People-centric, policy-based IT eliminates compliance-related costs across the board — from the cost of writing new scripts for every new mandate to the cost of pre-audit fire drills.
- **Avoided/reduced non-compliance penalties.** Regulators often have wide discretion when it comes to penalties for compliance shortfalls, based on factors such as best efforts and executive commitment. Implementation of IT policy automation can thus itself be a primary factor in penalty avoidance — above and beyond

the positive outcomes that automation produces.

## Beyond Compliance

But the benefits of policy-based IT automation go far beyond compliance. Compliance-related policies, after all, are simply one set of rules. IT can automate all kinds of context-aware rules to better meet the ever-changing needs of today's increasingly digital business. Here are some broader benefits to the business:

- **Increased employee productivity.** The way IT is run at most organizations today, people invariably experience delays between the time they need a resource and the time IT gives them access to it. This is especially true when they're first hired or when they change positions. Role- and context-based automation eliminates these delays so people can be more productive sooner.
- **Superior security.** Role- and context-based automation enhances security by making it easier to operationalize whitelisting, to prevent questionable access events and to offboard terminated employees instantly.
- **Improved IT efficiency.** When IT staff doesn't have to spend its time on manual provisioning and de-provisioning, script writing and maintenance, log reviews, and other common tasks, they can focus their time and talents on higher-value business activities. That re-allocation of staff resources is especially important as the business keeps requiring IT to do more with less.
- **Enhanced organizational agility.** Automation of people-centric policies doesn't just help organizations respond more quickly to new regulatory mandates. It empowers IT to quickly re-configure people's digital workspaces in response to mergers, acquisitions and re-orgs. The resulting organization agility reduces the cost of these major events while also ensuring that they start paying off sooner.
- **A better, more consumer-like employee experience.** Tomorrow's workforce will have far less tolerance for IT-related delays than its predecessors. Well-automated IT that's based on an accurate understanding of who users are, what they need and where they are — and that can deliver self service as appropriate — is rapidly becoming a must for serving and engaging top "digital native" talent.
- **Better use of contractors.** Role-based rules make it easier to provide contractors with appropriately limited access rights quickly and safely — and then just as quickly cancel those rights when the engagement is over. This capability is especially important for seasonal businesses and HR organizations seeking to limit fixed payroll costs.

## Simplify Compliance with Ivanti

Ivanti provides organizations with the people-centric controls they need to maintain compliance with many of today's data security regulations and standards. The risk of a failed compliance audit is mitigated by focusing on the worker and ensuring that automation is in place: first managing data access based on policy to keep workers productive, then being able to prove that necessary processes are in place — not the other way around. This people-centric approach to compliance makes audits less of a headache, worker productivity and security is maintained and policies can be enforced.


**HIPAA:** The Health Insurance Portability and Accountability Act protects confidential healthcare information and ensures consistency across the healthcare industry. Ivanti automates and secures all digital workspaces for hospitals, clinics and other healthcare organization that must comply with HIPAA. Predicting the services clinicians need and delivering context-aware access keeps patient data secure and improves the quality of service that can be delivered to patients.

SOX

**SOX:** Complying with Sarbanes-Oxley is a requirement for all publicly traded companies to protect investors from the possibility of fraudulent accounting activities. Ivanti puts app-level controls in place to make sure workers only have the level of access they need to get their job done — nothing more and nothing less. Provision access based on identity attributes and context to enforce security policies.

PCI DSS COMPLIANT

**PCI DSS:** The Payment Card Industry Data Security Standard (PCI DSS) is a global standard for credit-card security. Ivanti helps any organization that accepts, processes, stores or transmits credit card information to maintain a secure environment for the credit-card holder. Ivanti ensures data is protected by enabling IT to provision attribute-based access that's based on policy, certify access levels and apply granular app-level security rules at the endpoint.

GDPR

**GDPR:** The General Data Protection Regulation (GDPR) is a EU-based regulation that protects the personal data of individuals within the EU. Any organization that deals with the personal data of individuals within the EU — data "controllers" or data "processors" — must be compliant with GDPR, and Ivanti can help. Securing data with audit-ready compliance measures keeps the workforce productive.

If you are required to comply with HIPAA, SOX, PCI, GDPR or other data-protection regulations, Ivanti could help you ease the process of meeting compliance audits through the enforcement of your governance and security policies. Organizations need not sacrifice productivity for compliance or vice-versa. Compliance and productivity can both be maintained.

ivanti

ivanti.com/contact
1 800 982 2130
epg@ivanti.com