IT Compliance: How Technology Orchestration can keep you ahead of a complex regulatory environment

TABLE OF CONTENTS:

INTRODUCTION

Gartner Research defines IT Governance as "the processes that ensure the effective and efficient use of IT enabling an organization to achieve its goals."

Compliance is a critical component of IT governance. As the industry continues to evolve, more and more sensitive data and information enters the technology ecosystem, where the risk of errant exposure becomes more likely. The risks associated with being out of compliance are growing exponentially, and the potential liabilities in the forms of fines and increased regulatory oversight are quickly becoming onerous. The lack of self-regulation in most industries creates a framework that is ripe for error, and when an entire industry skids off the road (e.g. the banking crises of 2007-2008), or external events force a rapid shift in how the IT estate is managed (e.g. a sudden shift to working from home), the result is often increased oversight in the form of new regulations and compliance mandates.

The accelerated pace of technology innovation and its widespread availability has created a perfect storm of opportunity for business to be out of compliance. Most of the time these are not intentional acts, often it is the result of technology sprawl, poor internal procedures, or a lack of understanding of rules that are complex and dynamic. The problem is, none of those work as excuses, and regulatory agencies are quite happy to make an example of anyone who steps out of line. The other risk is the erosion of trust when a company does a very public face plant due to poor compliance oversight. Customers are hard to get, easy to lose, and regulators will take their pound of flesh when given the opportunity.

Compliance is not something you do once and you're done. It is an ongoing process that, if done correctly, can help your organization run more efficiently, and if not done correctly can potentially trigger millions in fines, bad PR, etc. In addition, this is not optional, so better to get it right anyway. Compliance management has two complementary facets; what is required for external regulatory agencies, government and industry entities and their auditors, and internal compliance mandates that are effectively best practices on company policies, which, if followed, can make the external audit run far more smoothly.

OBJECTIVES WITH IT COMPLIANCE

Compliance, when followed properly, is designed to deliver an operational framework to support both technical and procedural requirements that align to strategic objectives. This means achieving both legal and ethical objectives through policies and procedures that are legally defensible, with the intent of mitigating:

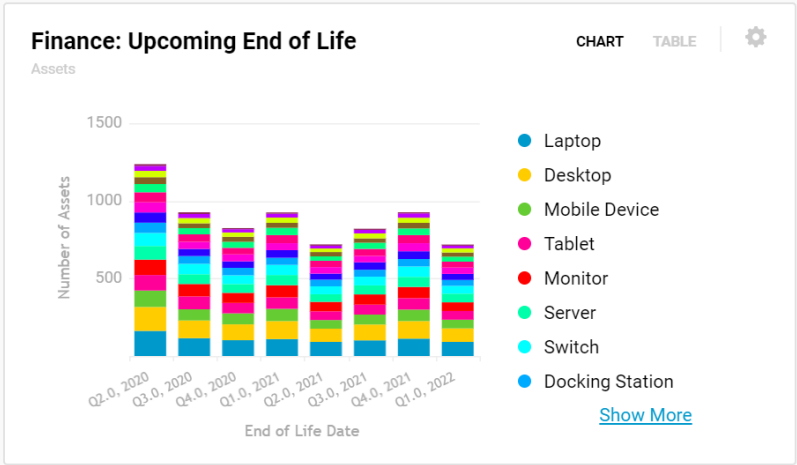
This sounds complicated, and it is. Since legal statues are drawn up by lawyers, most of them are subject to interpretation depending on context. There are guidelines specific to vertical industries (e.g. healthcare is regulated very differently than banking on some levels, and very similarly on others). There are best practices guidelines that can help navigate the process, but even if you're an expert, surrounded by experts, this will be a challenge, due to variables that may be outside the scope of control of compliance experts, such as:

- Your employees, who can easily violate governance rules and not even be aware of it
- IT's constant nemesis, Shadow IT - devices and applications that are outside the scope of what IT allows
- Your IT ecosystem, which can include multiple service providers for infrastructure (e.g. cloud) or process (supply chain enablers), who may not be paying as much attention as you
- The sudden and broad amplification of any issue via social media
- The seemingly endless cycle of iterations on new regulations, which can also vary significantly by region (e.g. laws passed in Europe can affect US-based companies very directly).

While the list of compliance frameworks grows and expands, for purposes of this discussion, we have focused on a few areas that our customers are telling us is driving their decisions on IT asset management, which we address in the next section.

GRC (GOVERNANCE, RISK, & COMPLIANCE) SCOPE AND REQUIREMENTS

Industry compliance is already a part of your daily routine. All of us are now used to getting mail from our service providers (banks, medical, insurance, etc.) that have excruciatingly detailed, legally dense documents regarding things like your privacy rights and how the service provider is following



The right system can alert you to assets approaching EoL, enabling legal hold when needed.

> "
> **Compliance management is not just saying you're compliant, but actually being able to prove you are.**
> "

compliance protocols, etc. This is endemic to everything we do, and compliance for IT infrastructure and asset management is no exception; being able to prove that internal best practices and adherence to external regulatory requirements are in place are a core part of an IT managers responsibility, and in bigger companies there are entire divisions dedicated to this.

One of the critical elements of compliance management is not just saying you're compliant, but actually being able to prove you are through carefully documented procedures. The procedures themselves can be conditional on the specifics of the company, process, and industry, but it needs to be defensible to someone who is good at looking for discrepancies. The role of IT in the compliance framework is becoming more pervasive as more and more information is stored and shared online, while at the same time essentially every business process is supported by IT infrastructure. Orchestrating this highly varied technology is essentially managing the infrastructure that supports business processes, which can also be subject to its own compliance and regulatory requirements and oversight. This includes privacy compliance (which has become more complex with companies shifting their infrastructure to the cloud), financial compliance (which are completely tied to the systems that enable them), and legal/HR (where are contracts stored physically and logically, how did the information enter the system, etc.). Keeping track of these details requires a sophisticated yet easy to use system that can scale and adjust to changing requirements, but most critically, ties to the internal workflow associated with how your business creates products and services. Assets connected to people and processes are assets that are tracked to profitability, both in terms of contribution to top line revenue, as well as to bottom line impact via line items such as reduced audit and compliance costs. As mentioned earlier, it is also important that this become integral to how your business operates on an ongoing basis. Orchestration of enterprise technology not an event or a product, it's a business-critical process.

The role of IT compliance is becoming far more mission critical as the dependency on IT for nearly any business process becomes deeply embedded in how companies operate. This applies to both how the specific technologies are managed, and the procedures that are associated with their use, which is effectively where IT Governance becomes relevant. For larger companies this is a significant (C-level) function, where governance can include legal, finance, purchasing, HR, and myriad other functions that are subject to regulatory oversight.

As an enveloping framework, risk management is closely associated with IT compliance and governance, since so much of the risk for business today is driven by the dynamics of IT infrastructure (e.g. consumer privacy in the cloud, data breaches, etc.). Tying Governance, Risk, and Compliance together into a cohesive framework is not only a best practices requirement, it's consistent with how most companies operate, since all functions are interdependent, and when properly executed, reduces redundancies.

COMPLIANCE FRAMEWORKS

There are a significant number of compliance requirements that affect the IT estate, some of which are industry specific, with some industries (healthcare, financial services) being more heavily regulated than others. Specific frameworks that we have found are relevant to our customers include:

GDPR

General Data Protection Regulation is particularly relevant for ITAM practitioners as it affects consumer data security across the entire asset lifecycle, and particularly during disposition at the end of life stage. Any asset with data needs to be re-imaged prior to either donation or disposal; the penalties for improper disposal and exposure of personal information are steep (the larger of $22 million dollars, or 4% of global revenues). GDPR treats assets that are being disposed of no differently than assets in use, so compliance is a constant in any IT asset orchestration process. To avoid this, maintaining chain of custody of the asset as it progress-es through its lifecycle is incredibly important, and is one of Oomnitza's strongest value-adds.

CCPA

California Consumer Privacy Act which has recently been enacted adds another layer of complexity to compliance related to risk mitigation. The associated requirements can trigger a shift in internal processes and/or policies related to CCPA oversight, such as new integrations between customer databases and data processing infrastructure (including off-site data), dealing with consumer rights across a broad array of IT-enabled channels, and staying ahead of the complexities and repriorizations associated with a data breach. This requires keeping track of all assets as they transition through their lifecycle, tying together asset data from siloed systems to gain a more holistic perspective, and creating a logical connection between the device and its associated user (to manage risk profiles) in order to accelerate investigations and remediation. Connecting users to assets across the lifecycle is another of Oomnitza's core differentiators; we are one of the few companies that offers this capability.

SOX

Sarbanes - Oxley focuses on financial transparency and internal operational control and reporting as a means of mitigating fraud risk. In terms of IT Asset Management (section 404 - Management Assessment of Internal Controls), the focus is on proper accounting of fixed and mobile IT assets. Compliance with SOX requires knowing (with high confidence) where specific assets are at any time, knowing whether there are ghost assets (on your books but no longer physically there), the levels of write-offs required due to lost or misplaced assets, and (most annoying) are you paying taxes on assets that you no longer have? Oomnitza's focus is tracking all IT assets as they move through their lifecycle, supporting an automated, integrated and holistic view, specifically to deal with associated financial compliance requirements.

HIPPA

Health Insurance Portability and Accountability Act

HIPAA focuses on tracking and maintaining information on any device that stores or can access electronic protected health information (ePHI). The HIPAA Security Rule requires that organizations keep precise track of assets (hardware and/or electronic media), as well as the person associated with that asset. This implies running internal audits on the device and associated user, specific to access of ePHI, and in addition, organizations are expected to keep track of where data is stored, maintained, received, transmitted, as well as the actual physical location. When a HIPAA audit occurs, the Office of Civil Rights will focus on the data, associated assets, and any movement or exact location information related to both. This is another instance of tracking devices or assets through their entire lifecycle, and ensuring the asset is clearly associated with a user, which is Oomnitza's core value-add.

ISO 27001

Information security management system (ISMS)

Defines an information security management system (ISMS) that covers policies and procedures for legal, physical, and technical controls with respect to risk management. It covers IT asset orchestration, but also extends well beyond. The specification includes defining your security policies, the scope of the ISMS, the need to conduct a risk assessment and then manage the identified risks, set controls and objectives and deliver a state-ment of applicability. Given that most IT-based risk surfaces when technology enters or exits the process ecosystem, having an orchestration solution that covers the entirety of the digital estate with a strong emphasis on security during the on and off-boarding process is critical to accelerating time to value.

SOC-2

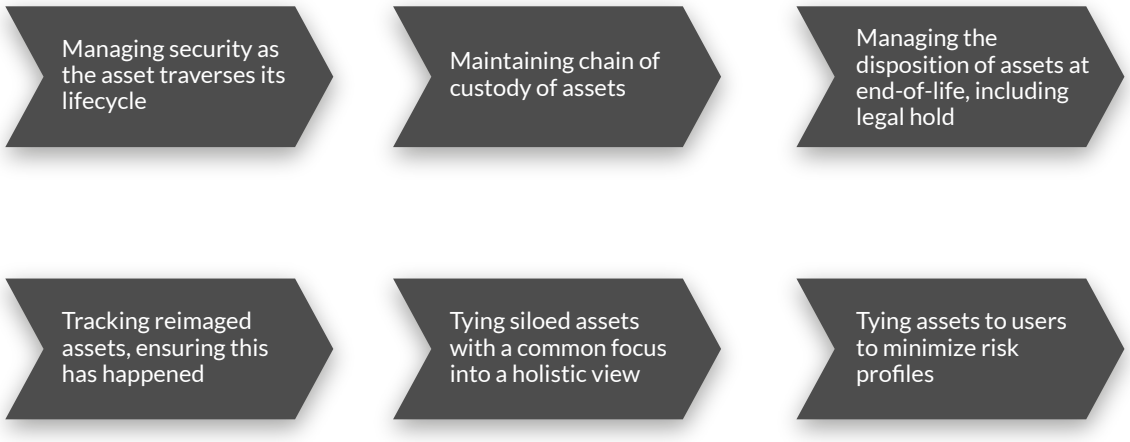
System and Organization Controls

There are multiple versions of SOC (SOC 1, 2, 3 and Cybersecurity) compliance that focus on different facets of business operations. For IT purposes, the relevant version is SOC-2, which covers Security, Availability, Processing Integrity, Confidentiality and Privacy. This pertains primarily to the data being processed, and how it is handled, either by the entity being regulated, or by any entity they choose to outsource to, such as a cloud services provider. As in most instances, security is the first filter (get this right and everything else flows smoothly), so ensuring a strong security posture for orchestration technology is critical. By correlating devices to specific users, Oomnitza is able to create a timely and actionable security profile that addresses compliance and audit requirements.

SUMMARY

There are multiple compliance requirements that need to be met regardless of the company's focus, and with the sudden shift of the IT ecosystem due to remote work requirements the potential attack surface has increased substantially, which in turn complicates compliance management. Also keep in mind your obligations under privacy law can vary, depending on, for example, if your company is considered as a data controller under the General Data Protection Regulation (GDPR), or as a business under the California Consumer Privacy Act (CCPA). In Oomnitza's case, we are considered a third-party data processor under the GDPR, and a service provider under the CCPA, because we handle the personal data or personal information of our customers' end users on behalf of its customers (or subscribers). Data controllers and businesses bear the primary responsibility for ensuring that their processing of personal data is compliant with relevant data protection law. So it's not just the applicable law, but how you are seen in the context of your IT infrastructure and the data that runs across it.

Key requirements for a solution that can address multiple compliance frameworks includes:



While the regulatory framework can vary significantly by industry and governing entity, as far as orchestrating the technology in your enterprise, it comes down to knowing with precision what is where, and to whom the assets are connected. It sounds simple, but as anyone in IT can tell you, it becomes enormously complex very quickly, which is where a solution that addresses information needs across the entire digital estate becomes mission critical.

About Oomnitza

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