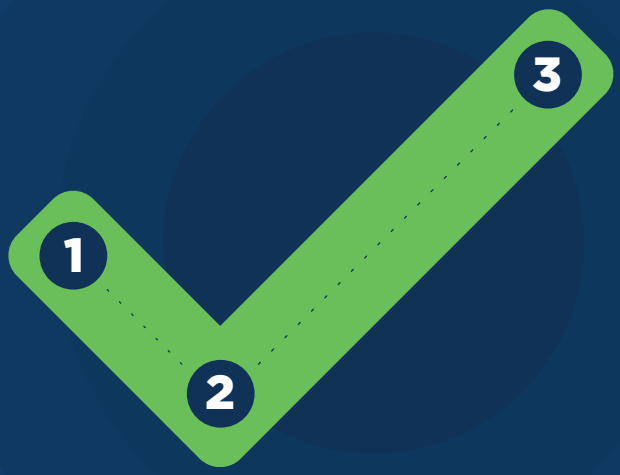
WHITE PAPER

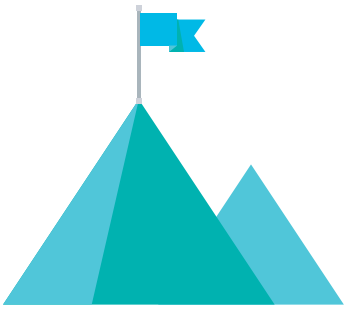



# Three Key Best Practices for DevOps Teams to Ensure Compliance

## Driving Compliance with Greater Visibility, Monitoring and Audits

suse.com

SUSE



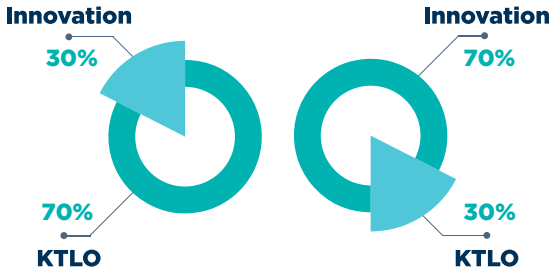
## Ensuring Compliance in DevOps

DevOps has fundamentally changed the way software developers, QA, and IT operations professionals work. Businesses are increasingly adopting a DevOps approach and culture because of its power to virtually eliminate organizational silos by improving collaboration and communication. The DevOps approach establishes an environment where there is continuous integration and continuous deployment of the latest software with integrated application lifecycle management, leading to more frequent and reliable service delivery. Ultimately, adopting a DevOps model increases agility and enables the business to rapidly respond to changing customer demands and competitive pressures.

While many companies aspire to adopt DevOps, it requires an open and flexible infrastructure. However, many organizations are finding that their IT infrastructure is becoming more complex. Not only are they trying to manage their internal systems, but are now trying to get a handle on the use of public cloud infrastructure, creating additional layers of complexity. This complexity potentially limits the agility that organizations are attempting to achieve when adopting DevOps and significantly complicates compliance efforts.

Ensuring compliance with a complex infrastructure is a difficult endeavor. Furthermore, in today's digital enterprise, IT innovation is a growing priority. However, many IT organizations still spend great time and money on merely maintaining the existing IT infrastructure. To ensure compliance and enable innovation, this trend must shift.

**CIOs across the industry agree. "If an organization still views the role of IT as 70% keep-the-lights-on (KTLO) and 30% innovation, it's on a trajectory of certain obsolescence," said Jonathan Reichental, CIO for the City of Palo Alto, Calif. "With technology now at the center of all activities, leaders must demand the inverse: 70% innovation and 30% KTLO."**




With a future that requires innovation and an immediate need for compliance today, the question remains: How can IT streamline infrastructure management and reduce complexity to better allocate resources and allow more time for innovation while ensuring strict compliance?

Infrastructure management tools play a vital role in priming the IT organization's infrastructure for innovation and compliance. By automating management, streamlining operations, and improving visibility, these tools help IT reduce infrastructure complexity and ensure compliance across multiple dimensions—ultimately mitigating risk throughout the enterprise.

## Adopting a Three-Dimensional Approach to Compliance

For most IT organizations, the need for compliance goes without saying. Internal corporate policies and external regulations like HIPAA and Sarbanes Oxley require compliance. Businesses in heavily regulated industries like healthcare, financial services, and public service are among those with the greatest need for strong compliance programs.

However, businesses in every industry need to consider compliance, whether maintaining compliance to the latest OS patch levels to avoid the impacts of the latest security virus or compliance for software licensing agreements to avoid contract breaches. Without compliance, the business puts itself at risk for a loss of customer trust, financial penalties, and even jail time for those involved.

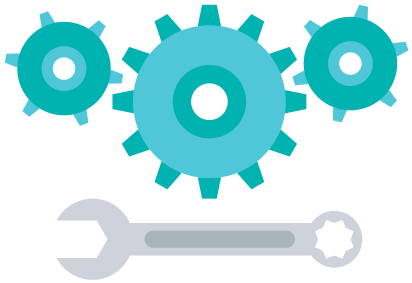
When examining potential vulnerabilities in IT, there are three dimensions that guide an effective compliance program: security compliance, system standards, and licensing or subscription management.

Security compliance typically involves a dedicated department that performs audits to monitor and detect security vulnerabilities. Whether a threat is noted in the press or identified through network monitoring software, it must be quickly remediated. With new threats cropping up daily, protecting the business and its sensitive data is critical.

For system standards compliance, most IT departments define an optimal standard for how systems should operate (e.g., operating system level, patch level, network settings, etc.). In the normal course of business, systems often move away from this standard due to systems updates, software patches, and other changes. The IT organization must identify which systems no longer meet the defined standards and bring them back into compliance.

The third dimension of compliance involves licensing or subscription management which reduces software license compliance concerns and unexpected licensing costs. Compliance in this area involves gaining better visibility into licensing agreements to manage all subscriptions and ensure control across the enterprise.

To mitigate risk across the business in all three dimensions of compliance, the IT organization needs infrastructure management tools that offer greater visibility, automation, and monitoring. According to Gartner's Neil MacDonald, vice president and distinguished analyst, "Information security teams and infrastructure must adapt to support emerging digital business requirements, and simultaneously deal with the increasingly advanced threat environment. Security and risk leaders need to fully engage with the latest technology trends if they are to define, achieve, and maintain effective security and risk management programs that simultaneously enable digital business opportunities and manage risk."



# Best Practice #1:

## Optimize Operations and Infrastructure to Limit Shadow IT

With so many facets to an effective compliance program, the complexity of the IT infrastructure makes compliance a difficult endeavor. One of the most significant implications of a complex infrastructure is the delay and lack of agility from IT in meeting the needs of business users, ultimately driving an increase in risky shadow IT activities.

As business users feel pressure to quickly exceed customer expectations and respond to competitive pressures, they will circumvent the internal IT organization altogether to access services they need. They see that they can quickly provision an instance in the public cloud with the simple swipe of a credit card.

These activities pose a threat to the organization's security protections, wreaks havoc on subscription management, and takes system standard compliance out of the purview of IT.

Optimizing IT operations and reducing infrastructure complexity go a long way toward reducing this shadow IT. With an efficient server, VM, and container infrastructure, the IT organization can improve speed and agility in service delivery for its business users. An infrastructure management solution offers the tools IT needs to drive greater infrastructure simplicity. It enables IT to optimize operations with a single tool that automates and manages container images across development, test, and production environments, ensuring streamlined management across all DevOps activities. Automated server provisioning, patching, and configuration enables faster, consistent, and repeatable server deployments. In addition, an infrastructure management solution enables IT to quickly build and deliver container images based on repositories and improve configuration management with parameter-driven updates. Altogether, these activities support a continuous integration/continuous deployment model that is a hallmark of DevOps environments.

When DevOps runs like a well-oiled machine in this way, IT provisions and delivers cloud resources and services to business users with speed and agility, making business users less likely to engage in shadow IT behaviors that pose risks to the business. As a result, compliance in all three dimensions—security, licensing, and system standards—is naturally improved.

### Ensuring Compliance in DevOps with SUSE Manager

**SUSE Manager is a best-in-class open source infrastructure management solution for a software-defined infrastructure. The solution is designed to help enterprise DevOps and IT operations teams reduce complexity, regain control of IT assets, increase efficiency while meeting security policies, and optimize operations with automation to reduce costs.**

**www.suse.com**

# Best Practice #2:

## Closely Monitor Deployments for Internal Compliance

In addition to optimizing operations, improving compliance requires the ability to easily monitor deployments and ensure internal requirements are met. With a single infrastructure management tool, IT can easily track compliance to ensure the infrastructure complies with defined subscription and system standards.

License tracking capabilities enable IT to simplify, organize, and automate software licenses to maintain long-term compliance and enforce software usage policies that guarantee security. With global monitoring, licensing can be based on actual data usage which creates opportunities for cost improvements.

Monitoring compliance with defined system standards is also important to meeting internal requirements and mitigating risk across the business. By automating infrastructure management and improving monitoring, the IT organization can ensure system compliance through automated patch management and daily notifications of systems that are not compliant with the current patch level.

Easy and efficient monitoring enables oversight into container and cloud VM compliance across DevOps environments. With greater visibility into workloads in hybrid cloud and container infrastructures, IT can ensure compliance with expanded management capabilities and internal system standards. By managing configuration changes with a single tool, the IT organization can increase control and validate compliance across the infrastructure and DevOps environments.

# Best Practice #3:

## Improve Visibility of Systems and Deployments for Greater Security

The fundamental goal of any IT compliance effort is to remedy any security vulnerabilities that pose a risk to the business. Before that can be done, however, IT must audit deployments and gain visibility into those vulnerabilities.

> **"The effectiveness of ransomware and the increased need for a structured process around security and device management continue to drive the SVM [security and vulnerability management] market," said Rob Ayoub, research director for IDC. "Organizations are demanding better tools to allow for the prevention, discovery, and remediation of attacks.... These tools are becoming an invaluable component in prioritization of threats and discovery of attacks."**

An infrastructure management tool offers graphical visualization of systems and their relationship to each other. This enables quick identification of systems deployed in hybrid cloud and container infrastructures that are out of compliance.

This visibility also offers detailed compliance auditing and reporting with the ability to track all hardware and software changes made to the infrastructure. In this way, IT can gain an additional understanding of infrastructure dependencies and reduce any complexities associated with those dependencies. Ultimately, IT regains control of assets by drilling down into system details to quickly identify and resolve any health or patch issues.

## Conclusion

TheDevOps has the potential to fundamentally change the way the business develops and delivers services. Despite the agility and flexibility DevOps can offer, complex IT infrastructures limit innovation and complicate compliance activities. To achieve three-dimensional compliance for optimal subscription usage, system standards, and security, the IT organization can improve simplicity and limit complexity with infrastructure management tools.

By automating management, streamlining operations, and improving visibility, these tools help IT optimize the environment for innovation, increase monitoring for internal compliance, and gain great visibility into the security of systems and deployments. Ultimately, the business achieves the flexibility and agility offered by DevOps and builds a future defined by innovation while ensuring compliance across the enterprise.

**For more information, contact your local SUSE Solutions Provider, visit us online or call SUSE at:**

1-800-796-3700 (U.S. and Canada)
1-801-861-4500 (Worldwide)

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

**www.suse.com**