Policy-Based Security, Compliance, and Risk Management

Automated approach boosts agility, reduces risks of security breaches and regulatory non-compliance, and improves operating efficiency
Table of Contents

Preface ................................................................. 3
Executive Summary .................................................. 4
Context ................................................................. 5
  Development Challenges .......................................... 5
  Production Challenges ............................................. 6
  The Cloud Capability Model ...................................... 6
Business Impact ....................................................... 8
  Efficiency ............................................................ 8
  Agility ............................................................... 8
  Reliability .......................................................... 9
Process Design and Implementation ................................ 10
  Step 1. Establish and Manage Security, Compliance, and Risk Policies ....... 10
  Step 2: Harden the Components and Create Gold Standards .................... 11
  Step 3: Remove Infrastructure Vulnerabilities ........................................ 11
  Step 4: Provide Network Segmentation and Defense in Depth ...................... 12
  Step 5: Implement Audit Logging ......................................... 13
  Step 6: Form Multifunctional Teams as Needed ..................................... 14
Organizational Considerations ........................................... 15
  Cloud Infrastructure Operations Center of Excellence ............................. 15
  Cloud Tenant Operations .............................................. 16
IT Business Management Considerations ............................... 17
  Percentage of External Audits Failed ........................................... 17
Technology / Tool Considerations ........................................ 18
  Technology Architecture ................................................ 18
  Centralized Management ................................................. 19
Key Success Factors .................................................... 20
  Obtain Executive Sponsorship .......................................... 20
  Acknowledge the Strategic Importance of Security and Compliance ........... 20
  Align Security and Compliance Initiatives to the Cloud Roadmap ............... 20
Next Steps .............................................................. 21
  Assess Operational Readiness Early ......................................... 21
  Determine Degree of Change Needed ......................................... 21
  Prepare the IT Organization for Change ....................................... 21
Why VMware for IT Transformation? ...................................... 22
Preface

Today’s IT organizations are under increasing pressure to deploy private or hybrid clouds and become a service provider to their business users. In many cases, this change is motivated by the increasing prevalence of business users going outside of corporate IT to procure IT services direct from external cloud vendors. In other cases, IT organizations view cloud as the answer for enabling greater innovation in the business. Whatever the catalyst, those organizations that have started making the move to cloud have already realized real gains in efficiency, agility, and reliability.

Based on its extensive experience working with customers on their implementations, VMware has identified five capabilities that are essential to unlocking the efficiency, agility, and reliability benefits of cloud:

- **On-demand services**: Service catalog with standardized offerings and tiered SLAs, actively managed and governed throughout its lifecycle, and with end-user access via a self-service portal
- **Automated provisioning and deployment**: Automated provisioning, release and deployment of infrastructure, platform, and end-user compute services
- **Proactive incident and problem management**: Monitoring and filtering of events, automatic incident resolution, and problem diagnosis
- **Policy-based security, compliance, and risk management**: Security, compliance, and risk management policies embedded into standard configurations enabling policy-aware applications and automation of security, audit, and risk management processes
- **IT financial management for cloud**: IT cost transparency and service-level usage-based ‘showbacks’ or ‘chargebacks’ using automated metering and billing tools

This white paper focuses on policy-based security, compliance, and risk management.
Executive Summary

The capabilities of the IT department have grown steadily over the past several decades. Unfortunately, so has the complexity of the underlying infrastructure. Today’s highly complex and often brittle platforms, the product of years of unplanned growth and mergers and acquisitions, have become increasingly unwieldy and difficult to manage effectively. These legacy infrastructures suffer from a range of problems that have substantial implications for the business:

• Operational inefficiencies such as high maintenance costs and poor resource utilization inflate IT budgets and erode bottom-line profitability.
• The inability to respond quickly to changing requirements and marketplace conditions creates competitive vulnerabilities, impair the ability to retain customers, and lead to missed opportunities.
• Service outages and poor application performance result in lost productivity and can damage the corporate brand.

Enterprises, government agencies, and other organizations are turning to cloud as a way to achieve the efficiency, agility, and reliability needed to drive innovation and compete more effectively. One common pitfall is that they do not adequately adapt the security, compliance, and risk management requirements of the business to the new technology. When security, compliance, and risk management processes are not aligned with the cloud architecture, it is difficult or impossible to achieve the desired benefits of cloud.

This paper describes an automated, policy-based system for security, compliance, and risk management. It describes specific challenges for the organization’s development and production environments and presents the business benefits that can be expected. The key steps in the process design are outlined along with the considerations for the organization, technology, and IT business management. Finally, it outlines some of the key factors that drive a successful implementation and suggests next steps for IT managers who are ready to move forward with their policy-based security, compliance, and risk management initiatives.
Context

As the IT infrastructure has grown in complexity, IT architects are finding it harder and harder to integrate security, compliance, and risk management into designs from the beginning. Instead, these components are procured piecemeal in response to a specific need and bolted onto the existing infrastructure. This approach creates silos, drives up operating costs, and compromises the ability to ensure high levels of security and compliance.

The good news is that architects now have access to new tools and technology that allow IT organizations to set policies that govern data mobility, user access rights, data management, and other factors. Policy-based security, compliance, and risk management describes the capability to design these mechanisms into the environment from the start and govern those controls via an integrated and centralized policy.

Security, compliance, and risk management challenges can be examined in the context of two major domains within the organization, development, and production.

Development Challenges

Developers often develop new applications on systems that lack the compliance and security standards of production machines. Reasons include:

• The overhead associated with manually implementing security and compliance is high.
• Developers lack expertise in security and compliance procedures.
• Changes in regulations typically are not communicated outside of the security and compliance functions, making it difficult for developers to remain current on requirements.

When developers are not conscious of security and compliance regulations, they create applications that meet the business requirements but fail to pass security and compliance tests. Applications cannot be deployed into the production environment without costly rework and delays in service deployment (Figure 1).

![Figure 1. Application development in a non-compliant environment](image-url)
Production Challenges

An important capability of cloud operations is automated provisioning, which typically reduces the time required to provision a service dramatically. However, the security and compliance activities often add a significant amount of time to the overall process, negating the benefits of streamlined provisioning. Therefore, the impact of automated provisioning on total cycle time is relatively minor—unless the security and compliance activities are also streamlined (Figure 2).

![Figure 2. Typical time to deploy services with manual and automated provisioning](image)

The Cloud Capability Model

In working with global enterprises and service providers, VMware has found distinct patterns of IT organizations and their capabilities as they move to embrace cloud computing. VMware has used this insight to establish a Cloud Capability Model, helping IT identify opportunities for growth and evolution of technologies and architectures, organizational models, operational processes and financial measures. This Cloud Capability Model provides a path for IT to take greater advantage of existing systems, teams and resources, embrace third party cloud assets and providers, and extend IT standards for security, governance and performance into this new model for IT. Across the Cloud Capability Model, customers are able to break free from a situation where resources are exhausted by simply maintaining existing systems to an environment where IT is a clear strategic business partner, delivering new services and capabilities aligned to and in support of business goals.

Policy-based security, compliance, and risk management should be understood in the context of the Cloud Capability Model, which provides a roadmap to help organizations assess their current state in regard to people, processes, technology, and business management, and plan cloud initiatives (Figure 3).
Reactive: Most IT organizations exhaust significant resources maintaining siloed legacy systems and are therefore challenged to make the desired contribution to future business results. A common response is to standardize the infrastructure, which reduces complexity and reclaims some IT resources for strategic work. The need for rapid innovation has driven business stakeholders outside of traditional IT channels, creating a tension between IT and business stakeholders. As a result, cloud has entered the business opportunistically, threatening to create silos of activities that cannot satisfy the mandates for security, risk management and compliance.

Proactive: IT has moved to embrace cloud as a model for achieving the innovation requirements of the business through increased efficiency, agility, and reliability. Shifts in processes and organizational responsibilities attempt to bring structure to cloud decisions and directions. More importantly, IT has embraced a new role, that of a service broker. IT is now able to leverage external providers to deliver rapid innovation within the governance structure of IT, balancing costs, quality of service, and risks. This shifts cloud from being an opportunistic technology purchase to a strategic environment with broader business impact.

Innovative: IT has fully implemented cloud computing as their model for producing and consuming computing, shifting legacy systems to a more flexible infrastructure, investing in automation and policy-based management for greater efficiency and reliability and enabling a broad range of stakeholders to consume IT services via self-service. Detailed measurement capabilities enable IT to quantify the financial impact of sourcing decisions, redirecting saved resources to drive new services and capabilities that advance business goals. IT continues to successfully manage multiple resources from internal and external pools of infrastructure, balancing cost, quality of service, and risk metrics across heterogeneous environments.
Business Impact

Automated policy-based security, compliance, and risk management delivers substantial business value in the areas of efficiency, agility, and reliability.

Efficiency

Reduced CapEx
An infrastructure outfitted to enable automated policy-based security, compliance, and risk management eliminates the need for multiple special-purpose appliances in favor of centrally managed security. It lowers capital investment and provides greater visibility and control over the security infrastructure.

Lower security and compliance operating expenses
When security, compliance, and risk management are automated, internal stakeholders can “do the right thing” and contribute to the organization’s overall risk mitigation strategy. For example, consider the application development scenario described earlier, in which development systems lack compliance and security standards. An automated, policy-driven approach implements these standards in a cost-effective way without burdening the developers with security and compliance tasks. The development environment can have the same level of security as the production environment, which in turn reduces the expense of reworking non-compliant applications (Figure 4).

Agility

More rapid provisioning and access to resources
Automating the entire provisioning process—including security, compliance, and risk management—creates a more agile platform that can respond faster and more flexibly to changing requirements. Business agility becomes an organizational attribute that executives can rely upon to help them respond to an unpredictable and volatile marketplace.

![Figure 4. Production environment with automated security and compliance](image-url)
Reliability

Increased security across the environment
Policy-based security, compliance, and risk management addresses a number of vulnerabilities within the cloud environment. It defends the perimeter of the virtual data center against a full range of attacks and also protects applications from network-based threats. The system ensures that guest machines—common vectors for threats—are secure and compliant before they are granted access.

Support for proliferation of endpoint device types (e.g. BYOD)
Policy-based security can address a growing issue in the enterprise: employees who provide their own endpoint devices, a practice widely known as Bring Your Own Device (BYOD). The system gathers information in real time from users and devices and makes proactive policy decisions consistently across the entire organization automatically. For example, it could control access to applications and content based on the user’s location and device type. Such a policy would be automatically and consistently implemented across the entire environment, strengthening the organization’s security posture. An automated system also allows security managers to make rapid adjustments to security policies in response to new threats and attack vectors.
Process Design and Implementation

The key steps to implement a policy-based security, compliance, and risk management system are outlined in this section. This process represents general guidelines that should be tailored to the individual needs of each organization.

Step 1. Establish and Manage Security, Compliance, and Risk Policies

In an automated, policy-based security, compliance, and risk management system, policies are used to instantiate the underlying security, compliance, and risk requirements and their controls. These policies can be used then to both create and audit the affected components. Finally they are continually reviewed for modification if the underlying requirements change or if the original business objectives or other reasons for the policy’s existence no longer apply. As such, the policy should have a process for controlling its overall lifecycle (Figure 5).

![Figure 5. Policy lifecycle process](image-url)
Step 2: Harden the Components and Create Gold Standards

The first step is to harden the components of the cloud infrastructure and services running on that infrastructure, that is, setting the configurations to match the requirements of the appropriate regulations. This process is greatly facilitated by the out-of-the-box templates that provide rich starting points for commonly used regulations such as SOX, HIPAA, FISMA, and PCI DSS. These standard configurations are complemented by custom templates that implement more specialized industry-specific standard and internal governance regulations. Typical tasks include:

- Harden the hypervisor configurations for cloud infrastructure, network and storage
- Harden the hypervisor guest virtual machine settings
- Harden the guest operating system (virtual and physical)

As each new virtual machine is deployed, policies are used to harden it. Gold standards are then created which guide the subsequent deployment of similar VMs (Figure 6).

Step 3: Remove Infrastructure Vulnerabilities

Keeping current with patches and updates forms an important part of effective security, compliance, and risk management. Pushing patches out to employees, partners, and vendors mitigates known vulnerabilities. Access control systems assess the compliance state of anyone accessing the network from outside the firewall and remediate vulnerabilities with patches and other measures before granting access.

Software provisioning can be made more secure by creating predefined packages with all configuration settings and then pushing them out to employees and others as needed. Another recommended technique is to implement malware defenses at the hypervisor level.
Step 4: Provide Network Segmentation and Defense in Depth

The traditional approach to cloud infrastructure security involves a complex mixture of components such as firewalls, access control devices, and load balancers. In the automated, policy-based architecture, these components are virtualized and centrally managed—an approach often called defense in depth. Virtual firewalls are application-aware, offering protection against network-based threats. Virtual machines can be moved to enforce security groups. This approach eliminates the need for multipurpose hardware and security air-gaps (Figure 7).

Figure 7. Defense in depth
Step 5: Implement Audit Logging

Audit logging of network traffic, compliance alerts, firewall activity, operating system changes, and provisioning activities is considered a best practice for maintaining the security of any IT environment. In addition, logging is a specific requirement of many regulations and standards. Automated logging that is cloud-aware and easy to manage fulfills these requirements effectively without adding complexity or increasing operating expenses. Ideally, the audit logging function interfaces with security information and event management (SIEM) tools to provide visibility to security managers and their supervisors (Figure 8).

Figure 8. Audit logging
Step 6: Form Multifunctional Teams as Needed

Traditional IT groups are organized into functional specialties that correspond to physical components such as servers, storage, and networking. In a cloud environment, the need is for multifunctional teams that bring together all the technical specialties required to effectively manage a particular cloud operation such as security, compliance, and risk management (Figure 9). When it is not possible to break up functional groups, the formation of virtual teams can be a workable solution.

Figure 9. Multifunctional teams
Organizational Considerations

Impactful cloud initiatives require not only the right technology but also organizational changes to people and processes. The most significant changes are to establish two new cross-functional departments, the Cloud Infrastructure Operations Center of Excellence (CoE) and Cloud Tenant Operations.

Cloud Infrastructure Operations Center of Excellence

The Cloud Infrastructure Operations CoE coordinates the activities of all the organizational resources that are required to drive a successful cloud initiative. It brings together business analysts and technical experts to consistently measure, account for, and improve the effectiveness of cloud infrastructure operations management (Figure 10).

Figure 10. Cloud Infrastructure Operations Center of Excellence

These functional specialties within the Cloud Infrastructure Operations CoE have particular responsibilities for policy-based security, compliance, and risk management¹:

**Architect**
- Works with the IT Security team to make sure any architecture or design decisions address security and compliance

**Analyst**
- Works with the IT Security team to make sure that the cloud infrastructure aligns with IT security and compliance policies; assists in developing automated compliance policies
- Maintains awareness of software patches and their impact on the environment
- Maintains the cloud infrastructure Asset Management data

---

¹ A complete description of the functional responsibilities of the members of the Cloud Infrastructure Operations Center of Excellence is contained in “Organizing for Cloud Operations,” 2012, VMware white paper.
**Administrator**
- Audits cloud infrastructure component configuration consistency
- Tests and installs cloud infrastructure patches
- Develops and maintains cloud infrastructure user access roles
- Works with the IT Security team to implement cloud-related security and compliance policies

**Cloud Tenant Operations**
Cloud Tenant Operations is central to governing, developing and providing cloud service offerings. It manages service governance, service design and development, service operations, and provisioning (Figure 11).

![Cloud Tenant Operations Diagram](image)

*Figure 11. Cloud Tenant Operations*

These functional specialties within Cloud Tenant Operations have particular responsibilities for policy-based security, compliance, and risk management:

**Service Developer**
- Works with Cloud Service Analyst and Application Development to make sure security, operations, and chargeback metering capabilities are built into cloud service offerings

**Service Analyst**
- Works with the IT Security team to make sure that services align with IT security and compliance policies
- Assists in developing automated compliance policies
IT Business Management Considerations

Organizations need a mechanism for measuring the business benefits of cloud operations. The IT Transformation Dashboard presents a set of key performance indicators (KPIs) in an easy-to-understand dashboard format. The dashboard should be distributed on a regular schedule to encourage cloud stakeholders to compare relevant KPIs over time and use these metrics as a common language for interactions within the organization.

KPIs such as the one described below provide visibility into the value of policy-based security, compliance, and risk management to the organization. (Figure 12)

**Percentage of External Audits Failed**

This KPI indicates the organization’s ability to meet the requirements of external auditors, expressed as a percentage of the total audits performed.

![IT Transformation Dashboard](image)

*Figure 12. IT Transformation Dashboard*
Technology / Tool Considerations

Effective security, compliance, and risk management requires automated tools to implement the policies and provide visibility and control to security, compliance, and risk managers and a well-defined policy lifecycle process.

Technology Architecture

While the technology for a security and compliance architecture must be adapted to each organization’s unique requirements, the key tools include (Figure 13):

- **Edge**: Secure the perimeter of the virtual data center with gateway services such as firewall/NAT, load balancer, and VPN.
- **Application**: Isolate and protect applications and databases against network threats and implement audit and compliance controls with application-aware firewall solution.
- **Endpoints**: Offload key antivirus and anti-malware functions to a virtual appliance and satisfy compliance and audit requirements through logging of antivirus and anti-malware activities.
- **Access control**: Ensure guest security and enforce compliance through effective administrative access control.

Tight integration of all the tools reduces risk by providing a unified approach to security and compliance.

![Security and compliance architecture for cloud](image-url)
Centralized Management

A defining characteristic of a policy-based security, compliance, and risk management system is the deployment of a single, integrated solution for centralized management of both public and private cloud resources. A centralized management system accelerates the adoption of cloud computing by addressing the security and compliance concerns of business users. This unified approach to configuration management reduces potential security threats and minimizes the effort and cost of compliance (Figure 14).

Figure 14. Architecture of centralized management system
Key Success Factors

While every cloud deployment has unique characteristics, VMware has identified a number of success factors that are common across a broad spectrum of industries, organization sizes, and operational goals.

**Obtain Executive Sponsorship**

Implementing an automated policy-based approach for security, compliance, and risk management inevitably requires changes—sometimes substantial in nature—to the organizational structure and job responsibilities. For example, there may be a need to establish multifunctional teams in the form of a cross-functional Cloud Infrastructure Operations Center of Excellence and surrounding ecosystem. Therefore, alignment between the organization’s IT management and business executives is crucial. Executive sponsors who clearly support the strategic objectives of cloud initiatives can help ensure continued funding.

**Acknowledge the Strategic Importance of Security and Compliance**

Security and compliance activities have traditionally been regarded as tactical in nature, tasks that enable the more strategic IT functions that are directly related to the business. A successful migration to the cloud requires changing this attitude. As cloud computing plays an increasingly prominent role in driving business innovation, security and compliance managers become front-office strategists: in effect, they take a seat in the boardroom.

This level of strategic importance is reflected in the proliferation of executive job titles such as Chief Security Officer (CSO), Chief Information Security Office (CISO), Chief Security and Compliance Officer (CSCO), Chief Compliance Officer (CCO), Chief Risk Officer (CRO) and Chief Risk Management Officer (CRMO). Lines of reporting are also affected, as CSOs increasingly report to the CEO, CFO, COO, or even the board of directors.

**Align Security and Compliance Initiatives to the Cloud Roadmap**

The traditional view of security and compliance as tactical necessities often led to a “bolt-on” approach: design the architecture around the “important” capabilities such as computing, storage, and networking and then add security and compliance appliances in an ad-hoc fashion. When security and compliance move to the strategic side of the equation, they must be planned and architected into the cloud roadmap alongside the other functional components. Otherwise, the resulting cloud platform will lack a sufficiently robust and effective security and compliance posture to achieve the desired benefits.
Next Steps

Once an organization has decided to implement a policy-based security, compliance, and risk management system, a number of steps are necessary.

Assess Operational Readiness Early

One potential pitfall on the road to implementing a policy-based approach is readiness. Many organizations discover that they have underestimated—sometimes dramatically—the investment needed in people, processes, and technology to move from their current infrastructure to a strategic implementation of security, compliance, and risk management in the cloud environment. Early readiness assessment is essential to crafting a transition plan that minimizes risk and provides cross-organizational visibility and coordination for security and compliance initiatives.

Determine Degree of Change Needed

Once the operational readiness assessment is complete, IT leaders should understand the degree of change required across the processes, organization, and tools and technology. They should understand the impact of policy-based security, compliance, and risk management on IT staffers currently responsible for these functions and establish their roles in the transformation to a policy-based system.

Prepare the IT Organization for Change

IT leaders should test the waters to see how ready their own organization is for the change to a policy-based system. IT managers must communicate clearly to staff the rationale for the change and provide visibility into the impact on individual job responsibilities. It is particularly important that managers discuss any planned reallocation of staff based on reductions in troubleshooting time to alleviate fears of staff reductions.
Why VMware for IT Transformation?

The move to the cloud is a foregone conclusion for many organizations today, but the path forward is often unclear. What is the current state of my infrastructure? How do we begin to move forward? What are the right technology choices for implementing our cloud? Most importantly, who can help us achieve our goals?

VMware has built some of the largest and most successful public and private clouds in the world. Now VMware is using that experience to bring to market a complete solution that includes a full suite of software products as well as the services you need to gain the maximum benefit from cloud computing. This combination of software and expertise, delivered via services and education to customers of all sizes across all industries, is unique to VMware and its global ecosystem of partners.

To learn more about the VMware cloud solution, visit www.vmware.com/cloud