If You Think Compliance is Expensive, Try Violations

Move Regulatory Compliance Activities to the Cloud to Help Simplify Remediation—and Avoid Fines

ORACLE WHITE PAPER | OCTOBER 2017

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.

Executive Summary

There's no turning back. Your sensitive data and critical applications are in the cloud. However, while many companies are enjoying a cloud-based honeymoon of improved efficiency, greater flexibility, and reduced costs, a hint of foul weather on the horizon threatens to spoil the bliss. Businesses that have embraced this new computing paradigm are seeing undeniable benefits, but they also face a greater risk of falling out of compliance with industry and government regulations, guidelines, and standards. As new requirements for data protection are ratified and a flood of established security regulations continue to be strictly enforced, you can't overlook the obvious question: Do the cloud services your organization uses put you in violation of regulations—and if they do, how would you know?

Many aspects of today's IT infrastructure must adhere to laws and regulations that safeguard sensitive data on behalf of organizations, industries, employees, partners, consumers, patients, and citizens. Most executives know that data breaches can occur when criminals gain illicit access to IT resources and data. But perhaps less understood is the fact that violations can arise from improper configuration and IT process errors as well. In other words, you don't need to be a victim of a cyber attack for your information systems to be on the wrong side of compliance regulations. It could just be your own oversight or error that puts you out of compliance.

Unfortunately, many companies delay investing in risk tools until after a compliance violation or data breach has occurred. Because of the new challenges and risks that come with the cloud model, it's more critical than ever to be proactive about cyber security. Being unaware of violations won't excuse you from penalties.

You don't need to be a victim of a cyber attack for your information systems to be on the wrong side of compliance regulations. It could just be your own internal oversight or error that leads to fines and penalties.

A Costly Struggle to Manage Security

Organizations that collect personal data must be able to prove that they comply with privacy and security principles. And with new European Union General Data Protection Regulations (GDPR), organizations must account for and be able to successfully protect EU citizens' personal data. Violations can incur fines up to millions of dollars and the potential for the closure of the business. Willful non-compliance can even lead to jail time.

It's no wonder that privacy and security have become top priorities for IT—with a significant impact on budgets. Management processes must be in place to assess the state of compliance and evaluate the risks and potential costs of non-compliance. Many business leaders find it difficult to weigh these costs against the projected expenses required to achieve and maintain compliance. It can be challenging to prioritize funding for the necessary actions.

Along with the need to obey an increasing number of regulatory mandates, organizations are also compelled to demonstrate operational transparency. As cloud services proliferate, IT organizations struggle to efficiently control the data security protocols needed to ensure compliance. Resources are often duplicated unnecessarily, impacting costs and undermining operational excellence. It is arduous and expensive to ensure that all necessary governance requirements are met.

A study by *Accounting Today* documents that annual Sarbanes-Oxley (SOX) compliance costs averaged $16 million in 2017, a jump of 77 percent from 2016.[1] Midmarket firms spend approximately $1.8 million, and Fortune 500 companies spend $35 million and require 15 full time resources to manage SOX compliance. A report from Berlin-

[1] https://www.accountingtoday.com/news/sox-compliance-costs-average-16m

based firm Research Gate indicates that firms that reported internal control deficiencies incurred significantly higher SOX compliance costs than firms that did not report internal control deficiencies.[2]

It’s tough to calculate the costs involved with compliance for directives such as Payment Card Industry Data Security Standard (PCI DSS). PCI compliance is a moving target as the technologies and tactics that attackers use to commit their crimes are always changing and becoming more sophisticated. Because of this, achieving and maintaining compliance is no simple task. New countermeasures must be constantly implemented to address emerging threats. This can discourage organizations from investing in the appropriate resources necessary to meet PCI DSS mandates, potentially exposing companies to substantial fines and other repercussions due to non-compliance and data security breaches.

Annual Sarbanes-Oxley (SOX) compliance costs averaged $16 million in 2017, a jump of 77 percent from 2016. Midmarket firms spend approximately $1.8 million, and Fortune 500 companies spend $35 million and require 15 full time resources to manage SOX compliance.

The U.S. Department of Health and Human Services fines organizations that fail to implement the appropriate controls to protect healthcare data and the privacy of patients. Fines of up to $1.5 million can be issued for HIPAA violations; with that number multiplied by the number of years each violation has been allowed to persist. The cost of non-compliance can be up to $500 per user/record. Willful neglect can incur fines of $50,000 per violation and possible jail time.

The bigger your company, the steeper the consequences can become. Fines for GDPR violations may be 20 million Euros or up to four percent of global revenue. These examples of the potential penalties for non-compliance across various directives underscore what’s at stake. The ever-increasing number of regulations and the unmistakably high price of violations compel companies to stay vigilant about maintaining a full understanding of their regulatory compliance requirements.

All of this may seem overwhelming, and perhaps even a little draconian. But remember, these strictly enforced regulations are in place to help companies, and entire industries, operate effectively and protect against unauthorized access. Over the long run, businesses that have sensitive data stored in the cloud will benefit from the safeguards outlined in these laws, regulations, and guidelines. Data breaches and security violations can damage an organization’s trust, brand, market value, and reputation. Predictably, most consumers would prefer to conduct business with a company that has never experienced a data breach. As such, it is critical that enterprises have a clear strategy in place to address the requirements for data management in the cloud.

Are You In Control of Your Data?

Regulatory compliance is complicated because there are many laws, regulations and guidelines. Some regulations are focused on outcomes and best practices—and not necessarily on how to achieve them—while others are open to interpretation. This can create a complex and oftentimes subjective strategy that must be continuously examined. Additionally, regulations are dynamic and updated regularly to ensure new findings are incorporated.

Compliance regulations demand that you collect, analyze, and store your data securely. You need to show compliance during audits and through reporting. You also need the data for eDiscovery, forensic investigation, and other compliance use cases. To do this effectively, you need to collect comprehensive, timely, accurate and

[2] https://www.researchgate.net/publication/228240104_Costs_of_Complying_with_SOX_-Measurement_Variation_and_Investors'_Anticipation

actionable compliance data across all your IT environments. Ideally, you should be able to leverage similarities among the compliance policies to build a strong secure IT environment.

Overview of Major Regulations

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) is designed to protect patient confidentiality and data privacy. It mandates the standardization of electronic health records systems and secure personal health information (PHI).
- Sarbanes-Oxley Act (SOX) was enacted in 2002 to protect people from fraudulent practices and accounting errors. It sets rules about how business records are stored and retained in IT systems for seven years.
- Federal Information Security Management Act (FISMA) was signed into U.S. law in 2002. FISMA strives to minimize risks to data by requiring federal agencies to conduct annual reviews of information security programs.
- Payment Card Industry Data Security Standard (PCI DSS) was created in 2004. It safeguards the security of credit, debit, and cash card transactions. Businesses need to tag and store all transaction logs for one year and ensure that card numbers, social security numbers, and other personal information is properly secured.
- The European Union General Data Protection Regulation (GDPR) was adopted in April 2016 and becomes enforceable May 25, 2018. GDPR intends to strengthen and unify data protection for all European Union (EU) citizens. It also addresses the export of personal data outside the EU.
- There are also numerous local and international standards and regulation codes that apply to various industries, fields, and specialized trades.

Maintaining compliance with these regulations not only requires significant knowledge and understanding, it’s also expensive and resource-intensive. Organizations must identify compliance requirements that are defined by local regulatory entities and international laws and regulations as well as internal compliance requirements outlined in contracts, business strategies, and company policies. Internal requirements and service level agreements may not follow the same regulations as legislated mandates, but businesses can’t overlook the overall governance required for internal audits and compliance.

Inadvertent technology misconfigurations and lack of security controls can lead to security vulnerabilities that result in compliance violations, and potential data breaches. Staying proactive and vigilant about these misconfigurations and vulnerabilities is critical, but it has become progressively more difficult to setup security and compliance controls as organizations move their workloads to the cloud and expose sensitive data to mobile devices. Many customers don’t fully understand the shared responsibility of security and compliance with cloud service providers. And because cloud services are adopted and deployed quickly, new attack vectors may be exposed with simple configuration errors.

Organizations must identify compliance requirements that are defined by local regulatory entities and international laws and regulations as well as internal compliance requirements outlined in contracts, business strategies, and company policies.

It’s not easy to verify compliance with pertinent regulations in light of these rapidly changing cloud configurations. Cloud services can be configured and provisioned quickly—often with little or no effort required from IT managers or service providers. However, while the effort is not trivial, keep in mind that good compliance practices are an enabler for best practices. For example, PCI ensures safe transactions, HIPAA ensures safe access to medical records, GDPR ensures safe usage of personal data—all examples of exemplary business practices.

Does Your Risk Assessment Strategy Work in the Cloud?

Where is the edge of your network? How much are you responsible for, and how much are your cloud service providers responsible for? Cloud-based business models blur the concept of a network *perimeter*. While cloud service providers are responsible for the security of their global infrastructure, it's your job to implement security measures to protect your content, applications, systems, platforms, and data. The more a cloud service vendor provides, the more it is responsible for—and the less control clients have.

That's why you need to acquire comprehensive, timely, accurate and actionable compliance data across production, development, and test environments. These requirements have never been more important than in today's highly virtualized IT environments, where systems lifecycles can last anywhere from months to years.

Compliance requirements have never been more important than in today's highly virtualized IT environments, where systems lifecycles can last anywhere from months to years.

There are a number of core technical frameworks that businesses should focus on in order to simplify the compliance effort. By leveraging the similarities among regulations and policies, companies can achieve an integrated approach to enterprise-wide governance, risk management, and compliance. Core compliance technologies include the following:

Securing users with identity and access management – Identity management systems associate specific rights and restrictions with each user's established identity. They govern how employees, contractors, vendors, partners, customers, and other stakeholders use IT resources. To comply with strict regulations, you need to implement access and identity management technology for both application users and IT personnel, including system administrators.

Securing apps with application security – Applications are at the core of business operations, and you need to ensure that the use and administration of these applications complies with pertinent regulations governing the privacy of consumers, patients, and citizens. For many companies, that means evaluating a heterogeneous collection of operating systems, application servers, and databases within a narrow time window to establish a compliance score, and then associating that score with relevant benchmarks, rules, and resource evaluations. These evaluations allow you to determine if your compliance posture is improving or deteriorating, and subsequently violating a particular regulation or service level agreement.

Securing data with data security – Deploying encryption and key management for data, both at rest and in motion, is one of the most common steps to securing sensitive data. This practice ensures that even if sensitive data is lost, it is useless to cybercriminals. Data masking is a great way to ensure that sensitive data is protected. It eases the pressure on compliance officers because you are not storing actual sensitive data. However, these controls represent only a portion of what is required for complete security and data protection. You should also consider implementing technology for data loss prevention, application layer redaction, and nonproduction data masking.

Streamlining Compliance Activities with Oracle's Security Cloud Services

As the network edge moves into the cloud, your IT resources are vulnerable to new threats. You need consistent security controls that span cloud and on-premises environments. These controls must apply identity *context* to better predict, prevent, detect, and respond to threats—and to keep your sensitive information secure.

Oracle's Identity-based Security Operations Center (SOC) framework provides comprehensive monitoring, correlation, threat detection, analytics, and remediation tools across hybrid environments. It is designed to be deployed in total or in phases. For example, you might start with log analytics and configurations and then add security analytics, data security, identity, and so forth, as you gradually build a modern, intelligent security operations center.

For many customers, the starting point is Oracle Configuration and Compliance Cloud Service, a PaaS solution that automates the process of enforcing security configurations and industry best practices. This technology is useful for evaluating key policies for compliance readiness for both on-premises and cloud resources—as well as for hybrid topologies with highly virtualized environments. Oracle Configuration and Compliance Cloud Service automates the configuration, scanning, assessment, scoring, and reporting of your compliance posture, so you can focus on *remediation at scale*. Compliance officers receive enterprise-wide assessment snapshots, while IT administrators receive compliance violation work lists, so they can prioritize the remediation of severe violations that impact the compliance score.

Oracle Configuration and Compliance Cloud Service is a key component of Oracle Identity SOC. This unified management platform can be extended to deliver operational excellence for IT Ops, DevOps, and SecOps functions, helping organizations unify their monitoring activities across all critical infrastructure. Oracle Identity SOC supports a broad set of use cases including Security Incident and Event Management (SIEM), User Behavior Analytics (UBA) for security operations, Configuration and Compliance Management for compliance and risk management, Identity Management (IDM) for user security, Cloud Access Security Broker (CASB) for application security, and database technologies such as encryption, key management, masking, and access control for data security.

Automating Cloud Security with a Cloud Access Security Broker

Protecting access to IT resources is especially challenging as sanctioned and rogue cloud services proliferate. Because these services have become so easy to deploy, business units often implement them independently of the IT department—and often without regard for security. In addition, individual users typically access numerous unauthorized cloud services that IT has no idea about, a practice known as *shadow IT*.

CASBs have emerged as the go-to solution for cloud security. These software tools reside between your on-premises infrastructure and your cloud infrastructure, sort of like a gatekeeper that extends your security policies into the cloud. However, a modern CASB must go beyond simple shadow IT discovery; it must also secure sanctioned IT services. The ideal solution will protect your entire cloud footprint—including infrastructure (IaaS), applications (SaaS), and platform services (PaaS.)

CASBs have emerged as the go-to solution for cloud security. These software tools reside between your on-premises infrastructure and your cloud infrastructure, sort of like a gatekeeper that extends your security policies into the cloud.

Oracle CASB meets these cloud security requirements by allowing you to configure standard security settings that are inherited by each cloud application. It includes out-of-the-box rules for Oracle Cloud and Amazon Web Services (AWS). Once these fundamental values are established, Oracle CASB monitors your cloud service settings and alerts you to any changes. It prevents “configuration drift” by allowing you to restore these approved settings at any time, eliminating tedious investigations and making it easier to prepare for compliance audits.

Comprehensive Access and Identity Management

Most of today’s organizations depend on a mix of cloud applications and on-premises applications, each with their own methods of identifying users and provisioning access to IT resources. Oracle Identity Cloud Service helps to rationalize and synchronize these identity management activities. As new cloud applications come online they are replicated and synchronized with on-premises apps, and vice versa, enabling “single pane of glass” management of the entire infrastructure. With Oracle Identity Cloud Service you can expand user identities to include multichannel experiences on phones, tablets, and computers via integrated API security hooks.

Centralized identity-as-a-service simplifies access to enterprise information resources and enables administrators to easily audit which users can access which resources at which times. They can maintain constant control and conduct complete entitlement reviews to catch situations where people no longer need access, with outbound credentials for hosted applications in the cloud and inbound credentials from third parties. This mature cloud service streamlines the process of accepting trusted identities and granting access to all types of applications. It’s a proven, centralized approach that dramatically expands your ability to leverage the identity platform for all of your user authorization needs.

Oracle CASB allows you to configure standard security settings that are inherited by each cloud application, and includes out-of-the-box rules for Oracle Cloud and Amazon Web Services (AWS).

Secure Your Journey to Cloud Today

Oracle has all the technologies you need to formulate a complete compliance framework and strategy. Its identity-based Security Operations Center framework provides comprehensive monitoring, threat detection, analytics, and remediation tools across hybrid environments that include on-premises and cloud resources. In addition, Oracle Security Cloud is designed to unify threat, user, and operational data from multiple sources. It incorporates preventive, detective, and predictive controls, along with artificial intelligence and machine learning to enable actionable intelligence.

Click here to learn more about how your organization can improve its security and compliance posture by implementing identity-centric, context-aware security practices:

- Improve visibility into Oracle and third-party SaaS/PaaS/IaaS security practices
- Enhance efforts to discover shadow IT processes throughout the enterprise and enforce rigorous cloud security protocols
- Better address strict regulatory and compliance mandates such as the requirements under the forthcoming EU GDPR
- Enforce access controls by authenticating and authorizing cloud applications and IT resources

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. *1017*

If You Think Compliance is Expensive, Try Violations
October 2017

Oracle is committed to developing practices and products that help protect the environment