ManageEngine
AD360

Achieving continuous IT compliance:

A best practices handbook

www.manageengine.com/ad360

TABLE OF CONTENTS

Introduction

Reactive compliance management is a gamble organizations cannot take. As the global cyberattack surface and the cost of cybercrime continues to surge, it has become heavily incumbent for IT compliance standards to enforce requisites and best practices for organizations to follow. In an era where organizations are expected to comply with multiple regulations, it is completely unfeasible for organizations to perform compliance management on an ad-hoc basis. The practice of looking at compliance auditing as a one-time activity is known as **reactive or point-in-time compliance**, which amounts to siloed management that can result in:

Erroneous audit reports: Being a manual process, reactive compliance is vulnerable to the failings of human errors, time-based restrictions, and limitations. Such gaps can lead organizations into a downward spiral of inconsistent adherence to compliance mandates.

Lack of security preparedness: The absence of a perpetual compliance management strategy corresponds to a lack of security controls that can assess an organization's exposure to risk. To summarize, an organization that heavily relies on a reactive approach to data compliance is vulnerable to data breaches. Organizational networks are replete with actions performed by employees, third-party vendors, machine identities, and applications, and the optimal security practice for organizations to secure their network is for them to apply continuous monitoring tools that adapt well to rapid threat and incident response strategies.

Resource and workforce burden: Irrespective of an organization's size, reactive compliance requires IT professionals and auditors to work in strenuous conditions, as there are little or no provisions for them to automate data collection and parsing.

Business and reputational losses: Loss of business prospects and reputation are synonymous with non-compliance. With heavy financial penalties on one side, an organization must also bear the loss of trust from stakeholders, employees, and customers, which can manifest into a landslide of losses in terms of acquiring new customers, prospects, and revenue.

What is continuous IT compliance?

Continuous compliance, also known as proactive compliance, is the organizational discipline of treating compliance as a prolonged, perpetual journey. Continuous compliance ensures that the requisites of a privacy standard, such as evidence collection, auditing, and mitigation of security gaps, are met on a daily basis, as opposed to performing cumulative assessments and measures annually. By implementing continuous compliance, an organization can break siloes and irregularities by actively engaging their IT teams and employees with the requirements of these standards.

With the emergence of data privacy regulations and stringent fines that accompany their non-compliance, continuous compliance has been gaining a considerable amount of prominence across organizations. A recent study by Drata revealed that 91% of its respondents plan to implement continuous compliance in the next five years.

Best practices to achieve continuous compliance

Achieving continuous compliance is a step-by-step process that requires equal contribution from the three integral pillars of cybersecurity: people, process, and technology. Some of the most recommended and actionable steps include:

Identify your compliance standard

A preliminary step that must be taken by compliance managers is to map the standards required for their organization to follow. To start, they must understand what industry they belong to, their geographical presence, and the data standards they will be governed by in each country or area of their establishment.

How AD360 helps

AD360 has an expansive library of reports that are also cataloged based on their relevance to data privacy standards. Organizations can easily plan their compliance-based requirements without having to go through the hassle of manually mapping out which reports and information tailor to their standards' requisites.

Mitigate security gaps

Applying necessary security controls to safeguard your organization is not only tantamount to a hassle-free compliance audit, but it can also improve the overall robustness of operations and business outcomes.

How AD360 helps

As an enterprise-level identity and access management (IAM) platform that caters to on-premises and hybrid cloud environments, AD360 equips organizations with critical capabilities such as:

Unified MFA and SSO: AD360 makes user verification seamless and secure by enabling single sign-on (SSO) across hybrid Active Directory and other non-AD applications that support SAML, NTLM, OAuth, and OpenID Connect authentication standards. In addition to SSO, AD360 also provides multi-factor authentication (MFA) that supports 19 credential factors.

Automated user life cycle management: AD360 understands the power of automation in reducing the organizational attack surface. By applying template-based, supervised, and controlled automation of user creation, modification, and deletion, AD360 ensures that:

- Users get appropriate access to assets over a definite period of time.
- Inactive accounts are promptly deleted on a timely basis.
- Potentially bulk processes pertaining to a company's employee life cycle can be expedited.

Organizations can reduce human errors in employee life cycle management while also protecting against insider attacks that exploit obsolete accounts and undue elevated access.

Establish real-time, continuous controls

Continuous compliance requires dynamic data coverage. Organizations should develop a continuous monitoring strategy that enables them to record events happening across their IT environment on a daily basis and parse these insights into actionable information. With continuous monitoring, IT and security teams can also identify security gaps and vulnerabilities within a short span of time.

How AD360 helps

UBA-powered continuous monitoring: Driving the essence of continuous assessment to elevate evidence collection, AD360 applies user behavior analytics (UBA), an ML-based feature that records baseline identity behavior for every individual user. These baselines are further considered as a frame of reference to ensure that any anomalous activity carried out by the user is escalated via custom-configured alerts. AD360's cross-platform capabilities can be leveraged to:

- Centralize user monitoring.
- Configure alert-based escalation of threats.
- Correlate events with reduced manual effort.
- Detect anomalous activity.
- Gain end-to-end visibility of your composite IT environment.

Additionally, these reports can be made actionable for mitigation with AD360's integration with security information and event management solutions.

Maintain lucid documentation

A compliance management strategy is as good as its approach to documentation, as the latter is the sole palpable evidence to show an organization's compliance with its respective data standard(s). One of the salient facets of IT compliance documentation is reporting and access controls. An organization that maintains an audit trail of its environment to garner this information must ensure that:

- The results are accurate.
- The processes are hassle-free, and the information is readily available.
- The reports are easily accessible, i.e., they break down complex information into simplified terms.

How AD360 helps

AD360's audit reports provide granular insights into user activity by collecting and processing events across multiple applications and directory services. For instance, when it comes to presenting an audit trail about user logons, AD360's reporting capabilities retrieve information that presents:

- Logon failures based on users
- Logon failures caused due to bad passwords
- Logon failures categorized based on domain controllers and IP addresses
- Logon times that have extended beyond the stipulated period of duration

Conclusion

Compliance makes organizations accountable, and failing to comply leaves a lasting impact that cannot be easily reversed. AD360's IAM capabilities and audit-ready reports relieve compliance auditors of relying on manual, complex, and ineffective methods to retrieve comprehensive information about their organization's AD and Azure AD environments. AD360 helps organizations achieve:

- Identity security by leveraging its IAM, IGA, UBA, and backup and recovery capabilities
- Inherent compliance as a result of the above functions.

ManageEngine
AD360

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About ManageEngine AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console. For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote

Download