eBook

4 Ways Identity Governance Helps Meet Compliance Measures

Omada

Do more with identity

Table of contents

Introduction

1.5 billion dollars. That's how much money has been levied in fines since GDPR's inception, three and a half short years ago[1]. And this is just one piece of legislation! GDPR is one of many high-profile pieces of regulation that put constraints on how organizations process personal data. Others include CCPA, HIPAA, SOX and PCI DSS, but there are many more that are specific to types of business, geographic location, company status, and more. It's an uphill climb for businesses to maintain compliance and as the increasing fines reveal, some organizations are struggling. However, achieving and meeting compliance mandates is possible; and a modern identity governance strategy can help tremendously.

[1] GDPR Fines List: Find all GDPR fines & detailed statistics (privacyaffairs.com)

> *"1.5 billion dollars. That's how much money has been levied in fines since GDPR's inception, three and a half short years ago."*

There are many pieces of legislation and standards of which organizations have to keep track. Here's a quick list of some of the most common:

Standards

NIST: National Institute of Standards and Technology
CIS Controls: Center for Internet Security Controls
ISO: International Organization for Standardization

Legislation

GDPR: General Data Protection Regulation
CCPA: California Consumer Privacy Act
SOX: Sarbanes-Oxley Act
HIPAA: Health Insurance Portability and Accountability Act
COPPA: Children's Online Privacy Protection Rule
PCI-DSS: Payment Card Industry Data Security Standard
NERC CIP Standards: NERC Critical Infrastructure Protection Standards

Compliance Challenges & Complicating Factors

Each new compliance mandate has created complex compliance issues, due to wide-ranging requirements with broad organizational reach and potential negative impact on corporate efficiency. Organizations face severe fines and reputational damage as a result. As an example, a GDPR fine can amount to 4% of annual global revenue, depending on the severity and circumstances of the violation. In addition, **a piecemeal approach to compliance (as opposed to a privacy-by-design approach) can make it incredibly time consuming and arduous for security and IT teams to keep up with the evolving legislative landscape.**

While fines steal headlines, they often pale in comparison to reputational damage, not to mention the operational effect of a breach. Implementing identity governance and administration (IGA) can help companies and public sector agencies efficiently meet regulatory requirements, avoid fines, and protect against breaches and data leaks.

4%

A GDPR fine can amount to 4% of global revenue

€169million

The GDPR enforcement agency issued more than €169 million in fines in 2020

Complicating Factors

Migration to the cloud and the rise of the hybrid and remote workforce have introduced new challenges to today's businesses as to how they maintain control, manage risk, and ensure compliance - all without restraining business efficiency and collaboration.

Addressing a complicated and continually expanding set of global regulations is only possible if businesses have the needed people strategy, partnered with reliable technology and security solutions. As digitalization accelerates and teams are forced to 'do more with less,' IT departments are facing greater and greater workloads – which makes it even harder to ensure compliance and stay on top of security requirements.

Fortunately, IGA solutions can help organizations determine who has access to what and enforce identity best practices. By doing so they can meet many key requirements of compliance mandates.

In this eBook, we'll explore the 4 ways that IGA helps businesses meet compliance measures:

1. **Identity Lifecycle Management**
2. **Entitlements Governance**
3. **Automated Audit**
4. **Business Workflows.**

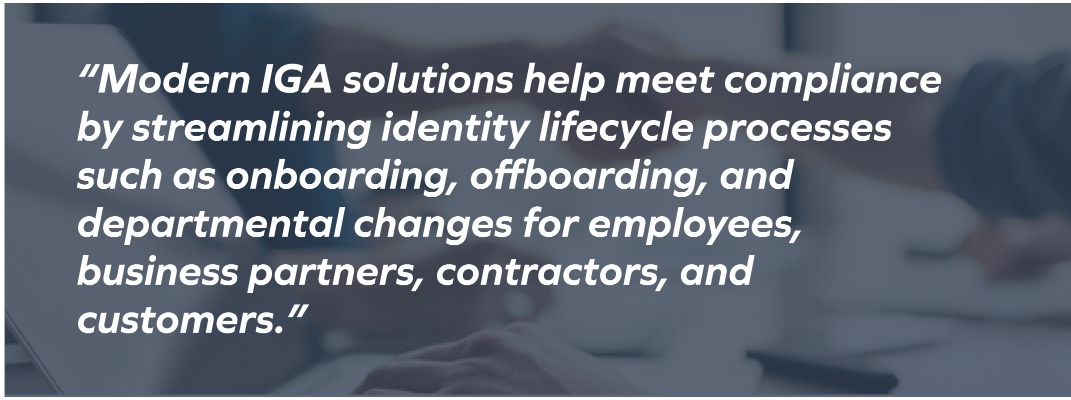
1. Identity Lifecycle Management

One of the biggest compliance headaches for organizations is making sure that the right people have access to the right resources for the right reasons. This becomes increasingly complex and challenging as people get hired, promoted, and/or leave the organization. A critical capability of an Identity Governance solution is to enable and grant access rights according to defined roles and policies. This means ensuring that each identity has the right level of access at any given point in time, based on their job role, employment status or otherwise. This is often a critical component of meeting compliance measures as it helps to ensure that different identities only have the specific access rights required to do their jobs, with access defined in a Role Based Access Control (RBAC) model.

65% Of people were looking for a new job as of August 2021[2]

25% In 2021, one in four people quit their jobs[3]

Governing identities and access is critical when complying with legislative and regulatory requirements. For instance, GDPR states that organizations should have processes in place to manage, monitor and document identities' access, complying to need-to-know/need-to-have principles - which can also be referred to as 'least privilege'.



> ***"Modern IGA solutions help meet compliance by streamlining identity lifecycle processes such as onboarding, offboarding, and departmental changes for employees, business partners, contractors, and customers."***

For example, when a new employee joins, an IGA solution creates a new record in the master HR system. This employee is assigned predefined user accounts and access rights that give access to resources common to all employees, such as Active Directory, email, shared drives, and company benefits. However, this record also allows for specialist applications to be used, based on that user's new role.

[2] Four Things We Learned About the Resignation Wave–and What to Do Next | Visier Inc.

[3] PwC US Pulse Survey: Next in Work

54% Of organizations don’t have a full inventory of all third parties with access to their network

65% Of organizations haven’t identified third-parties with access to their most sensitive data[4]

2. Entitlements Governance & Risk

Once each identity has been given access to the right resources, maintaining order is critical to meet future rounds of compliance and audit checks, as well as maintain security. **At organizations with large numbers of employees, third-party vendors, auditors, and more, it can be complex to document who has access to what, and why they were granted that access.** Additionally, as users require access to applications that may not be automatically permitted, managers may just end up rubber-stamping approvals because they feel overwhelmed with the number of requests. This can cause problems for meeting compliance down the line, as well as providing access that is not necessarily needed, with obvious security implications.

Take as an example an IT contractor who has just had their 3-month contract extended, but is now going to be working on a different application within the organizational stack. As such, their entitlements should change to include only the things required in their new role, and their access will need to be extended. This typically will mean that the identity will lose some access to systems no longer needed for the new role and gain access to systems they previously didn’t have. However, it can be difficult to ensure that the user only has access to the resources needed for their new job, while automatically removing the privileges from the old; something that can cause an organization to be in non-compliance. This is also referred to as ‘entitlements creep’.

[4] Omada and SecZetta Collaborate to Reduce Threat of Third-Party Breaches (prnewswire.com)

3. Automated Audit

A modern Identity Governance solution should be able to ensure that users are not granted more access rights than they need, as well as giving business system owners the opportunity to ensure the correct level of access. **A modern IGA solution should allow administrators and security teams to focus on areas of high risk and also allow them to double click into those which are most critical.**

Identity Governance processes allow data administrators to create classification tag categories. Furthermore, they should be able to enforce policies involving data protection regulations and Segregation of Duties (SoD) to prevent toxic combinations based on previous and future roles. IGA solutions help meet compliance by regularly verifying that information such as access rights, policies, role definitions and master/identity data are still valid and up to date and provide an aggregated overview of system compliance.

Many IT departments keep track of access rights in spreadsheets to document their process to auditors, a method that is time-consuming, prone to errors, and may even violate external regulations. In addition, documentation used for audits may be fragmented; reasons for granting access might not be properly logged or employees may accumulate access over time, with rights not being revoked when they move department or otherwise.

58%

Of organizations failed to address GDPR compliance for data requests within a one-month timeframe[5]

22days

Is spent on average by major retailers to respond to pending access requests[6]

[5] https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/

[6] https://www.gtlaw-dataprivacydish.com/2021/09/how-long-do-retailers-take-to-respond-to-access-requests/#edn2

Companies that use identity governance are establishing a solid foundation for maintaining compliance by making it a strategic tool. **A modern IGA solution will have in-depth governance dashboards that can quickly show access across systems and highlight compliance violations.**

Additionally, governance reporting provides full point-in-time overview of all access for all identities plus trend reporting over time. It has an even more dramatic effect on IT teams, who no longer have to sift through large volumes of data to prove compliance to auditors.

[5] https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/

[6] https://www.gtlaw-dataprivacydish.com/2021/09/how-long-do-retailers-take-to-respond-to-access-requests/#edn2

Common items to keep track of in audit logs, including historical data:

- Permission changes
- Active (and inactive) accounts
- Master Data, Identity Data
- Access Requests and Approvals
- Certifications and Surveys
- Assignments Granted

4. Business Workflows

A topic that does not get enough mention in the compliance conversation is that of efficient workflows, both for business users and for IT administrators. It is extremely common for business users to require access to additional applications or data to which they are not given access out-of-the-box. Without automated workflows, it can be a long time before business users get the access they need, leading to lost productivity. In addition, an overabundance of access requests can also lead to downsides for IT administrators. When overworked, administrators, help desks, and managers may end up rubber-stamping approvals and granting unnecessary and unsafe access, leading to failed audits down the road - and can lead to the organization being over-exposed to security vulnerabilities.

$15.56	**The average ticket cost for support teams**[7]
$140B	**The amount that info/data security breaches as a result of IT-related problems will cost**[8]
$60B	**The amount that IT-related software problems are estimated to impact the US economy**

"Modern IGA solutions solve essential GDPR challenges related to access control and transparency, helping organizations improve security and compliance, while also managing users' access rights purposefully and efficiently. "

An modern IGA solution should allow users to seamlessly request additional access to business applications, while setting conditional policies where access can be granted based on business context. This also provides managers and systems owners with the ability to approve or deny access, and ensures existing access can be transferred to another user if needed, for example if someone goes on vacation.

Modern IGA solutions should also provide automated implementation of business workflows and processes that enable efficiency, such as automated provisioning, self-service access requests and approvals. At the same time they need to be adaptable enough to embrace organizational uniqueness, such as employees fulfilling multiple job roles. When it comes to identities and access management, implementing an IGA solution makes it possible to ensure continuous compliance with GDPR.

By making users and administrators follow the same access request and approval process each time and centralizing the management of access to all (onboarded) systems in one place, one single point of truth can be created - and compliance measures can more easily be met.

[7] https://www.thinkhdi.com/library/supportworld/2017/metric-of-month-service-desk-cost-per-ticket.aspx

[8] Mark Hall, Apollo RCA instructor and investigator

A Compliance Asset

GDPR opened the floodgates for similar regulations in other regions of the world. Already-burdened IT teams are struggling with the demands borne of digital transformation and remote work; compliance often falls by the wayside as a result. But GDPR and similar compliance mandates aren't optional for those to whom they apply, and fines, breaches and reputational damage can have long-term effects.

One support asset for IT security and regulatory compliance is a cloud-based, next-generation IGA solution. This gives organizations the ability to offer automated access to an increasing number of technology assets. At the same time, it takes the burden off IT staff and manages potential security and compliance risks. Modern IGA solutions can be a real compliance asset for organizations dealing with today's many regulations, especially with user-friendly compliance dashboards that provide a fast and focused overview of the actual state of identities and their access across the business. These dashboards can also highlight access risk as well as serve as the foundation for reports for audits. Modern IGA solutions help with Identity Lifecycle Management, Entitlements Governance, Automating Audit and enabling efficient Business Workflows. They are a vital tool to meet the growing demands of compliance mandates facing organizations of all shapes and sizes.

Modern IGA solutions help with Identity Lifecycle Management, Entitlements Governance, Automating Audit and enabling efficient Business Workflows.

Omada is a global market leader in Identity Governance and Administration that offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach. Omada has operations in North America and Europe, delivering solutions directly and via a network of skilled partners and system integrators.

Omada

www.omadaidentity.com | info@omadaidentity.com