Moving towards compliance with identity governance for files

Protecting an organization's most sensitive information—intellectual property, financial documents, personal information on both employees and customers, etc.—is an important responsibility for information technology (IT) and security departments. Amid the growing presence of cyber crimes and theft, industry and government regulations, including the Health Insurance Portability and Accountability Act, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and the European General Data Protection Regulation, were put into place to help protect this data.

While these regulations were intended to force good behaviors in order to improve the overall risk posture of global organizations, these compliance mandates created parallel projects for many organizations focused on proving compliance and protecting themselves. Fortunately, by implementing a governance-based approach to identity governance, you can help secure your organization's sensitive data while simultaneously supporting compliance with these laws, saving time and resources that can then focus on moving your business forward.

You can't protect what you can't see

Many regulations require protection of your sensitive data, but with much of all data in enterprises being unstructured—and therefore residing outside applications and databases—effectively managing access to all your sensitive data is a challenge. Unstructured data—text documents, spreadsheets, presentations, emails, etc.—does not follow the same rules that structured data does, and it is growing at an alarming rate.

In order to protect your data, you must first find where all your files reside, determine what sensitive information it contains, and who has access. Some organizations have policies in place that instruct employees where to place sensitive information. Unfortunately, even if policies are in place, it doesn't mean that they are followed. You must employ a solution that can both identify sensitive information and also validate and enforce the rules you put into place. And for compliance requirements, you need the ability to attest to these policies and controls.

Managing access to sensitive data

A common problem with unstructured data is that access can be granted from multiple authoritative sources and through multiple permission tracks. Once you've identified the sensitive data files, you then need to know not only who has access to those files, but also what they're doing with that access. Having this information will also help when compliance auditors arrive and want to know how you are ensuring the right people have the right access to the right data at the right time.

Another piece of this puzzle is to elect the correct owners for your data. Structured data has traditionally been assigned business owners to help manage access to it and the same should be true for your unstructured data. But just as it can be difficult to identify what data is sensitive and what isn't, it can be challenging to designate the right owners for your data.

Rather than assign data owners based on usage, your process should include the option for business users to provide direct feedback, or elect an owner. The issue many organizations face is that the correct data owner cannot be found by traditional means; more often than not, this information only resides in the minds of the users who actively utilize the data. The solution? Instead of attempting to create rules to automatically assign owners, ask those who work with the data on a regular basis to be your eyes and ears. Those who work most closely with the information can collectively identify who would be best to own and govern access to the data in question.

Nearly 80 percent of medical data is unstructured and siloed after it is created[1]

Automation is key

Because of the sheer volume of unstructured data an enterprise can possess, it is nearly impossible for the governance of this data to occur manually. Automation must be implemented so that responses can occur in real-time and with high efficiency from both the IT and business sides of house.

Tools such as automated provisioning and deprovisioning of access, self-service access requests, and automated certifications of access are all needed in order effectively govern data stored in files.

SailPoint can help

Healthcare organizations have the highest costs associated with data breaches—per year cost of roughly $7.413 million annually.[2] To fully address today's modern data security needs, organizations are moving beyond traditional data access governance solutions, and incorporating sensitive data stored in files and folders as part of their comprehensive identity governance program.

Visibility

In order to protect access to sensitive data, you must have a holistic view across your entire infrastructure. If your IT team or business owners are unaware of where sensitive data resides, cannot see all the permissions a user has, or how this access is being used, then they simply cannot make the right access decisions to mitigate security and compliance risks.

IdentityIQ File Access Manager helps answer these essential questions:

— Where is your sensitive information?

— Who has access to it and is that access too broad?

— What are those users doing with their access, and do these actions violate your security policy?

— Can you prove all this to an auditor?

Control

Accurately identifying data owners is a key step towards effectively controlling and securing your organization's data. While structured data stores have generally been assigned business owners, unstructured data usually do not have a complementary owner. Without proper data owners, unstructured data in files can be easily overlooked, incorrectly classified, and improperly managed in terms of who has access.

Organizations that fail to actively assign accountability to those who are most knowledgeable about who should and shouldn't have access are leaving themselves open to data breaches and regulatory penalties.

Once the owners have been elected from those who actually use the data on a regular basis, you must then enable them to manage their data via user-friendly tools that ultimately save them time.

IdentityIQ File Access Manager allows data owners to:

— Get visibility over the data they own

— Self-configure alerts that are brought directly to their attention

— Create a task list to keep owners on track

— Provide controlled access through self-service access requests

— Give IT compliance insight through periodic entitlement reviews

— Add access and remove high-risk access through actionable intelligence

[1] Managing Unstructured Big Data in Healthcare System," Healthcare Informatics Research, January 31, 2019.
[2] IBM and Ponemon Institute 2020 Cost of Data Breach Report," page 12.

Compliance
Healthcare organizations in regulated industries will always be concerned with maintaining compliance. The security of electronically protected health information (ePHI) is an imperative for healthcare organizations who need to meet regulatory and compliance guidelines.

IdentityIQ File Access Manager helps compliance efforts by providing:

— Visibility into the location of sensitive documents

— Validation that sensitive documents aren't being leaked outside of protected areas

— Activity monitoring to help ensure that only the proper identities are accessing the data

Conclusion

Compliance with laws and regulations is important for healthcare entities but it should be the spur that helps you secure your organization's sensitive data, not the end result. SailPoint can help you get compliant, stay compliant, and—more importantly—help ensure the security of your enterprise's sensitive data.

At KPMG we understand that healthcare and life science organizations are operating in a highly regulated environment, with changing business models, disruptive technologies, and significant amounts of data. We offer a market-leading portfolio of methodologies, tools and services to assist you in the areas of value-based growth strategies.

— KPMG is a top deployment partner of SailPoint solutions with a focus on achieving business goals through technology.

— As a SailPoint Delivery Admiral since 2018, we've delivered over 200 engagements including some of the largest and most complex deployments of SailPoint IdentityIQ.

— KPMG's SailPoint implementation methodology is based on industry leading practices and is continually refined by collaboration between our delivery teams. We strive to learn every day, on every implementation, and to improve our processes continually.

KPMG enhanced our IAM implementation methodology through investments in building an extensive catalog of intellectual property, enablers, and accelerators. This helps us design platforms that meet our clients' business needs today and are ready for the future, designed to accelerate long-term return on investment.

[3] Source: Xxx

Contact us

Jim Wilhelm
Principal, Advisory
T: 267-256-7271
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Director
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia