SailPoint

What's Your Identity Score?

Report Results

Thank you for taking SailPoint’s Identity Score survey. In this report, you’ll find information about your identity scores, recommendations based on your scores and best practices for how to move your organization forward securely and confidently.

What’s an Identity Score?

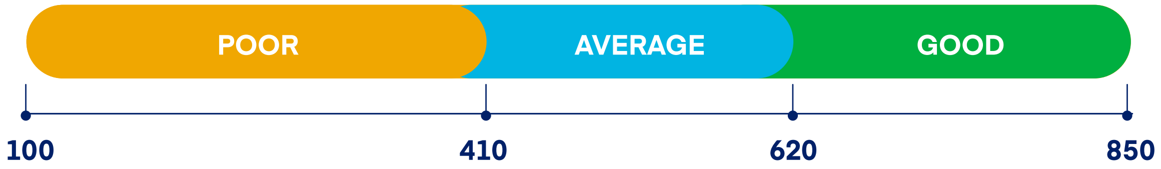
identity score *(ahy-**den**-ti-tee **skohr**)*
A score that denotes the possible risk level of an organization, based on high-level questions about the current status and workings of its identity processes.

It is important to note that your identity score is not based on a comprehensive examination of your identity processes, but rather a high-level survey. Therefore, the diagnoses contained within this report could change with more information from a deeper conversation. Nevertheless, as long as your answers were given to the best of your knowledge, your scores should provide insights on where your organization lies in its level of risk.

In addition to your overall identity score, your answers were assessed in three categories to further determine your organization’s identity efforts’ maturity. For all category scores and the overall score, the value is calculated based upon the answers provided and then weighted appropriately given the question’s criticality.

Overall Identity Score

The overall identity score is based upon a number range of 100 – 850, much like a credit score. Most organizations fall within the 411 – 620 range, with a good score rated above 620 and a poor score rated under 411. The overall score is calculated by the answers given across the entire survey. While the overall score gives you a view into how your identity efforts compare to best practices, your individual rankings in the three categories defined below help identify specific areas for improvement.



Visibility & Control

This section focuses largely on what your organization can see in terms of its identities’ access to organizational resources and data. This section also seeks to understand how well your organization controls that access during certain events, such as when a user moves, transfers or leaves within the organization. Scores in this section fall into three ranges: “**poor**,” “**average**” and “**good**.”

POOR
AVERAGE
GOOD

Identity Governance Processes

The goal of this section is to determine how well your organization has utilized tools, such as automation, and how you’ve supported identity governance efforts with policies and processes for business users. Scores in this section fall into three ranges: “**poor**,” “**average**” and “**good**.”

POOR
AVERAGE
GOOD

Governing Access to Files

Securing access to unstructured data stored in files (such as .DOC, .PDF, .XLS, .PPT) is an important part of a secure organization. This section focuses on how well your organization monitors and controls access to this type of sensitive data, which can be stored within both on-premises and cloud-based file storage systems. Since governing access to folders and shares is a relatively new venture for most organizations, scores in this section fall into two ranges: “**poor**” and “**average**.”

POOR
AVERAGE

Methodology

SailPoint partnered with Identropy, an identity management and consulting firm that helps organizations successfully deploy and manage identity, to create this survey. This report aims to help enterprises around the world examine their identity efforts and learn how to improve them. Both companies have decades of real world experience with identity implementations, from organizations with millions of users to enterprises in every industry. Using their combined expertise, SailPoint and Identropy first mapped what a comprehensive identity program is in today's environment. Then, we determined what an ideal implementation and maintenance process looks like and how the maturity and efficiency of these processes impact an organization's risk of a data breach. SailPoint then surveyed customers around the world, who are at various stages in their identity program, to build an industry benchmark.

Your Identity Scores

The information below shows where your organization scored based on the answers you gave during the Identity Score survey.

Visibility & Control	Identity Governance Processes	Governing Access to Files
GOOD	GOOD	AVERAGE

In the sections that follow, we discuss what a comprehensive, enterprise identity governance program should look like, methods to get your organization’s identity house in order, as well as specific recommendations for your organization based on your categorical scores.

The security and confidence that comes from a comprehensive identity governance solution allows your organization to focus instead on what really matters. Chase new market opportunities. Innovate your products or services. Expand to new geographies. Gain a larger competitive advantage. The power of identity means your organization can be confident, fearless and unstoppable.

GOOD

Your Identity Score: **Visibility & Control**

You Can't Protect What You Can't See

The ultimate goal for an identity program in any organization is to be able to know, at a given time, the answer to the question, "Who has access to what?" And the answer shouldn't come from the manual tabulation of every user's access to every application, system and data storage location. That question must be answerable for any employee, no matter their job profile or location. You need to be able to see access for contractors and vendors, for users located halfway around the world and on whatever device they choose to work.

The same is true for your organization's applications and systems. Whether you install them on-premises or choose to utilize cloud-based applications and services, your identity program needs to have a holistic view into your users' access to all applications and the data within. Only by gaining full visibility and having all the relevant information can your organization then make the right decisions when events occur.

Extend your identity governance efforts by leveraging the robust connectivity and integration capabilities of IdentityNow and IdentityIQ to govern user access to all legacy and new systems and applications found across your entire global infrastructure.

The good news is that you're already doing well in this area. You have a good amount of visibility into your systems and are generally pretty confident that access is appropriate for your users' current roles in the organization. Of course, there's always room to grow.

1/3

organizations can produce a report that shows all users and their access to all applications, systems and data[1]

How to Improve Your Score

□ Future-proof your identity program by verifying your identity governance solution is:

- Agile enough to adapt to any environment – both cloud-based and on-premises applications, as well as structured and unstructured data.
- Unified with every aspect of the IT infrastructure: identities, resources (any object that may be acted on by an identity, from data to applications and more), entitlements and events.
- Extensible with APIs, formal integrations and plugins for greater flexibility to address the unique requirements of your organization This extensibility will assist in ensuring the future applications and systems you use can be supported by your identity governance platform.

[1] *2017 Identity Score Survey Benchmark*, SailPoint

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

The open identity platform is here. SailPoint's open identity platform provides the foundation that brings identity context to all facets of the business – even to systems and applications that are proprietary, antiquated or brand new.

□ Ensure you are connecting *all* current systems and applications to your identity governance solution. Don't forget to investigate the existence of applications that may have been procured as a result of shadow IT.

□ Verify your organization is running a "least privilege" model – where identities only receive the smallest amount of entitlements required for their role – to granting user access to resources.

- Ensure this is true for all your organization's users, including contractors, partners, suppliers, etc.
- Generalize the use of your role models across the entire organization to more effectively automate access control.
- Set up controls to find occurrences of and remediations for issues such as:
    - Entitlement creep
    - Separation-of-duty violations
    - Orphan accounts

□ Publish the full list of security policies and procedures that govern what your users can and cannot do, and run a continuous education program to preclude some of the more easily preventable risks, e.g. BYOD, weak passwords, credential sharing, etc.

□ Demonstrate the current achievements of your identity efforts. (Having organizational buy-in helps to smooth the process for any additions you need to procure for future identity endeavors.)

- Tailor messages to each of your important stakeholders, and make an effort to show each group their own unique data and performance over time.
- Utilize internal portals (emails, training events, presentations, etc.) to share that success.

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

□ Extend your identity governance solution to create an identity-aware infrastructure where identity context is shared across operational and security systems.

1. Utilize an open identity platform to be the foundation of your identity program.
2. Leverage plugins or extensions to share and collect identity data with and from other parts of your security and operational infrastructure.

Did You Know? SailPoint's PAM module for IdentityIQ can help you govern and establish 360˚ visibility over your privileged accounts in the same way you do for any other accounts, while also simplifying and centralizing their administration. Learn more at **sailpoint.com/pamreport**.

For more specific recommendations, we recommend **scheduling a call with one of our identity experts (sailpoint.com/contact)** to talk more in-depth about how to get started and what you should do next.

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

GOOD

Your Identity Score:
Identity Governance Processes

The Proper Foundation Determines Success vs. Failure

While software can do a great number of things to help your organization become more secure, it's the combination of technology, processes and people that deliver the strongest identity governance programs.

It is important to closely review the features available from your chosen identity solution and leverage them to automate manual and tedious processes to improve the efficiency of your IT staff, while enabling your users in a timely fashion. The automation of certain processes – and automating the audits on those processes – can streamline the work your IT and business users have to perform on a regular basis.

> Organizations, on average, only automate half the identity governance processes that could be automated.[1]

Another goal is to empower your users to easily follow the policies your organization sets forth regarding security. If it's too cumbersome to request new access to an application (e.g. access requests are not an automated process enforced and governed by role models), users will either find a way to circumvent the process through insecure methods such as credential sharing, or they will simply be less productive.

Fortunately for your organization, you've done a good job of creating those processes and policies to properly support your identity program. Identity automation depends on creating governance models – risk models, role models, etc. – by which you can create the rules necessary to have your identity governance solution do part of the thinking for you. However, in order to be as efficient as you can be, there's more for you to do.

7/10

organizations **do not have policies in place** for their role models[1]

How to Improve Your Score

□ Use risk models to gauge priority, and create and employ role models for governing groups of access for all your users.

1. Build a complete set of role models for each position in high-risk departments first – IT, Finance, HR, etc. – by determining the default set of entitlements the position should have.
    - Stay with low-level entitlements, leaving administrative and privileged access out of your models. These entitlements

[1] *2017 Identity Score Survey Benchmark*, SailPoint

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

are simply too important and dangerous to be freely given without oversight.

- Don't forget to do this for *all* systems, applications and data – leaving out any of the three opens your organization to potential risk.

2. Repeat this process for your medium-risk users and then your low-risk users until the entire organization has applicable role models.

□ Ensure you have automated all the identity processes that can be automated:

- When a new user joins, grant them the basic access they need in order to perform their job on day one.
- When a user changes jobs, automatically terminate any extraneous access from their old role, and grant new access based on their new title. (Double-check that your separation-of-duty rules are enabled to handle any potential entitlement violations when this change occurs.)
- When someone leaves your organization, immediately terminate all access to organizational resources – systems, applications and data.
- Give your users the ability to reset their password and unlock their accounts through a self-service portal.
- Automate through self-service user requests to new systems, applications and data that are pre-approved for their role (and automate alerts for requests for non-pre-approved resources to the appropriate person).
- Set a schedule by which business managers will perform periodical access certifications, and automate the certification process to eliminate manual tools such as spreadsheets.
- Build a formalized channel for your users to request procurement of new applications, but don't make it overly complicated. This can help to combat shadow IT.
- Regularly review that your automated processes are working as intended.

Implementing automated compliance management from IdentityIQ or IdentityNow allows you to enforce corporate access policies, prevent segregation-of-duty violations and re-certify user access.

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

□ Extend all the above steps to include information and events from your third-party security applications, such as:

- Helpdesk and IT Operations Applications
- Security Information and Event Management (SIEM)
- User Entity Behavior and Analytics (UEBA)
- Mobile Device Management (MDM)
- IT Service Management (ITSM)

The automation power of a full identity governance platform is a powerful tool. For instance, integrating your files and storage systems to be part of your governance efforts allows you to actively monitor access to sensitive information, and alert IT and data owners if suspicious activity is detected. Real-time alerting and automated remediation triggers can then stop malicious behavior in its tracks by cutting off user access and reporting event details to IT and the security operation center.

In addition, this comprehensive identity governance approach gives you the power to identify where else the user account has access and investigate if signs of malicious behavior also exist – proactively addressing potential compromised accounts and data breach activity.

If your identity governance solution is not yet integrated with the other security solutions your organization utilizes, it's time to investigate doing so to bring more identity context to the rest of your infrastructure. Once your organization is on an open identity platform and empowered by the flexibility this platform can offer, you can then start to bring all your company's resources under governance, creating an identity-aware enterprise.

The identity-aware enterprise can detect, prevent and help remediate incoming threats, dangerous entitlement combinations, violations of security policy and many other events that present risks to organizations today. This allows you to be better prepared to handle the threats your organization faces on a regular basis, while also enabling your workforce to work within the policy parameters that help keep you secure and compliant.

Schedule a call with one of our identity experts (sailpoint.com/contact) to learn where automation could specifically help your organization's identity efforts.

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

AVERAGE

Your Identity Score: **Governing Access to Files**

Bring Order to Chaotic Data

Data has become a huge problem. People generate so much data, it's estimated that only 0.5% is ever actually analyzed or used.[2] When taking into consideration only corporate data, Gartner estimates more than 70% of organizations' collective unstructured data is what is known as "dark" data – old, outdated and unused. To add to the complexity, this data also resides on a myriad of on-premises file servers and convenient cloud file shares such as Dropbox, SharePoint, Box, Google Drive and OneDrive.

If this data were just pictures of company outings and Thursday's lunch menus, it may not be as big of an issue as it is. But in the tera- and petabytes of information that organizations keep as unstructured data – PDFs, presentations, spreadsheets, etc. – also lies sensitive data. Personal employee information may be kept in spreadsheets and sent across email. Financial projections may have been taken from a database and put into a slide deck to share with your board of directors. A potential merger may have a digital version of the contract saved in a cloud storage space.

It's easy for even the right people with the right access to unknowingly create an exposure point by saving sensitive data to an unprotected file type or storage area. Without a cohesive and comprehensive identity governance program that includes governing access to this data, organizations are exposed to data breach risk and in violation of industry compliance regulations.

By 2019, organizations with complementary/integrated identity governance and data access governance capabilities will suffer **30% fewer data breaches**.[3]

A comprehensive identity governance approach helps ensure you can identify where sensitive information resides, remove excess permissions and apply appropriate access controls. In addition, this type of comprehensive approach enables organizations to implement an integrated approach to detecting and remediating malicious behavior.

The other point of contention with many organizations is that unstructured data is a new problem. Many haven't even begun to manage access to it. Thus, for this report, our scores only break down into two ratings: average and poor.

[2] *The Data Made Me Do It*, MIT Technology Review
[3] *Enhancing Data Loss Prevention, Dealing with Ransomware: Why Identity and Data Security Need to Converge*, Gartner

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

1/2

organizations govern access to their **unstructured data**[1]

Your organization falls into the former category; your governance of data – both structured and unstructured – is about on par with other enterprises today. Even though you may recognize unstructured data is a problem, you have yet to enforce a fully holistic governance program. Data breaches are rampant, invasive and only getting worse. Many involve unsecured unstructured data, such as hackers releasing email attachments after gaining access to compromised email accounts. The huge amount of sensitive information that resides in corporate data stores is daunting, and properly governing access to all data must be a top priority for your organization.

How to Improve Your Score

□ Find and classify all your data.

- Interview your data application owners for file shares and data stores to understand what kind of data they use and where they usually store it.
- Procure an identity governance solution that supports the ability to perform data discovery by scanning your typical unstructured data repositories: email systems, file shares and collaborative portals, in addition to your cloud applications such as Dropbox and Office 365.
- This same identity governance solution can also begin to classify your data and score it in terms of risk, marking certain files or repositories as sensitive information.
- Sensitive data sometimes lies forgotten, so be sure to audit the health of your data to ensure you do not have any that is dark.

□ Move your sensitive data to secure storage locations.

- Once you have found sensitive information, it may be residing in an inappropriate or unsecure location and must be moved to a storage area where you can effectively monitor and govern access to it.
- Ensure that wherever you move your sensitive data to, only the right people have the right access to those systems. Inherited entitlements from group permissions and roles can be complex to govern, and must be kept in mind when storing sensitive information.

□ Elect owners for all your data by asking the users of your data to collaboratively vote on who should own it. More than likely, the most prolific user will not be the one that is chosen, but instead someone in a supervisory or project management role.

[1] *2017 Identity Score Survey Benchmark*, SailPoint

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

□ Automate processes to address the governance of access to files containing sensitive information.

- Set up regular recertification processes to maintain the correct level of access to help ensure user access is relevant to their current responsibilities.
- Monitor the health of your data and have data owners focus on the risk levels of the data over which they have stewardship.
- Create alerts when abnormal behavior is detected (large-scale downloads or uploads, unapproved file types, etc).
- Clean up/archive old and stale data that could be housing sensitive information and be a potential data breach risk.

With organizations possessing so much data, most of which has content unknown and held in multiple repositories, identifying, classifying and gaining control over it is a daunting task. But properly governing access to your data isn’t going to get easier as time goes on, and you must consider unstructured data as part of your larger identity governance processes now in order to be fully secure.

You can greatly minimize your exposure to data breaches by extending your identity governance efforts to protect and secure access to sensitive information found in the files generated by your workforce – text documents, presentations and spreadsheets – that are stored across your cloud and on-premises file shares.

Tight integration between SailPoint SecurityIQ and IdentityIQ provides a comprehensive solution to govern access to all data found in structured databases and unstructured file folders.

No matter what, access to all your organization’s data needs to be secured. **Schedule a call with one of our identity experts (sailpoint.com/contact)** to learn your next steps for governing your data, structured and unstructured.

Please note: these recommendations are given based upon a quick and basic survey of your organization’s security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

Your Solution:
SailPoint's Open Identity Platform

Your ultimate goal is to create an identity-aware enterprise, where identity context can be shared with and collected from all IT operational and security applications in your infrastructure. But this can't happen without a true identity governance platform.

Identity governance is a cross-organizational discipline that provides the intelligence and business insights needed to strengthen controls and protect information assets. With identity governance, organizations gain 360-degree visibility into and control over "who has access to what." This provides the transparency needed to reduce potential security and compliance exposures and liabilities.

Identity governance also helps organizations improve efficiency by replacing paper-based and manual processes with automated tools. Not only can your organization significantly reduce the cost of endeavors such as user enablement and compliance, it is possible to also establish repeatable practices for more consistent, auditable and reliable processes. Taking an automated approach helps to build predictability and repeatability into the compliance tasks and workflows, while also helping an organization to respond more rapidly to control weaknesses and detected violations.

Businesses who invest in an open identity platform will be able manage and secure their most vulnerable resource – their identities. By securing and governing identities, organizations will protect their business while enabling it to rapidly embrace future opportunities for expansion.

SailPoint Can Help

REQUEST A DEMO

Talk With Us to Learn How Identity Governance Can Help You:

- Increase IT efficiency through automated provisioning and governance tools
- Strengthen security by knowing exactly "who has access to what" and what users are doing with their access
- Enhance compliance efforts through a holistic identity program

Please note: these recommendations are given based upon a quick and basic survey of your organization's security program. The full environment of your organization may or may not be accurately represented based upon your answers. We are happy to give more detailed recommendations after a deeper conversation with you.

SailPoint | What's Your Identity Score?

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.