SailPoint

WHITE PAPER

Building a Business Case for **Identity Governance**

What's Driving Identity Programs Today?

Identity programs are primarily driven by challenges in three areas: compliance, operational efficiency and user productivity. Building a business case for identity and access management involves demonstrating how identity can effectively address these challenges and then justifying the cost based on the expected business benefits. Improving security can also be an important program driver and should be included in any identity business case, but the financial benefits of such a program, while clearly reducing risk, tend to be more difficult to quantify. The following section describes some of the typical challenges that drive organizations to pursue identity programs.

Meeting Audit and Compliance Requirements

Organizations continue to work toward improving their overall compliance with regulations that govern data privacy and security – while concurrently controlling the cost of that compliance. This becomes increasingly challenging as the number of regulations increases, the amount of data to be maintained grows and operations become more complex in light of emerging trends such as cloud computing. Identity governance programs are designed to deliver end-to-end visibility and automate controls across an organization's systems and applications. They make it easier and more cost-efficient to establish a desired-state model for compliance, enforce conformance to the model and attest to the effectiveness of internal controls. Ongoing access certifications become both more effective and less resourceintensive through the strategic use of automated identity controls such as policy enforcement and role-based access models.

Lowering IT and Helpdesk Operating Costs

Many organizations are still using fragmented, manual processes for adding, changing and removing user access privileges. The result is inefficient and costly execution of access requests, password resets and other access changes – and a heavy burden on IT and helpdesk staff. By automating these processes, organizations can reduce the number of requests from business users, the number of approvals required to grant access and the number of calls to the help desk.

Streamlining Delivery of Access to the Business

Given the fast-paced and dynamic environment of business today, IT organizations are challenged to keep up with the demand for identity services, and to do so in a compliant manner. Business users cannot wait days or weeks for access to systems required to perform their job duties. The right identity governance solution can streamline the delivery of user access and significantly reduce the time to implement access changes, while continuously enforcing governance rules and compliance policies. It can also empower business users to become active participants in identity processes, enabling them to manage their own access and passwords.

Ensuring Security and Reducing Risk

Security risks are a fact of life for every organization, which must put controls in place to protect against both internal and external threats. Unfortunately, security is an issue that only seems to be getting worse. According to a report from Risk Based Security (RBS), 2016 saw 4,149 data breaches that released over 4.2 billion records. Implementing an identity governance solution can play a significant role in strengthening security by helping your organization detect and remediate vulnerabilities: users with excess or inappropriate access privileges, terminated workers who still have access privileges, policy violations such as separation-of-duty (SoD) and poorly-managed privileged user accounts.

A Stepwise Approach to Building Your Case

At a time when IT budgets remain tight, a carefully constructed business case is essential to unlocking funding for identity programs. The following four-part process will help justify spending based on the value of the program to the business.

Step 1

Assess Needs

The business case for any proposed identity program always starts with one fundamental question: Why is it needed? Or, more specifically, what business problems do you intend to solve with identity governance, and how will it ultimately deliver value to the organization? The first step in building the business case is, therefore, assessing internal needs to identify and prioritize challenges that are likely to drive the most value. Thinking back to the preceding section of this paper, consider the challenges described in compliance, IT operations, user productivity and security. What challenges within these areas does the organization face? Which are the most pressing? Which are most likely to move the business forward or, if not addressed, open the business up to more risk? It's important to be extremely specific about the challenge or area to be addressed.

Here are some questions you may ask while assessing the needs of your organization:

- **Compliance:** How much does compliance cost your organization today? How effective is your compliance program? Was there an audit failure? What specific controls did the auditors fail? Did they include any comments or recommendations that would be useful to you in preventing future problems?
- **IT Operations:** Is the helpdesk inundated with service requests? Can you document exactly what issues are causing the overload? Is it requests for access changes or password resets?
- **User Productivity:** Are new users sitting idle waiting for the access they need to become productive? Do employees waste time navigating disparate login processes for a variety of applications? Are users locked out of systems while they wait for the helpdesk to assist them?
- **Security:** Is the organization's board of directors asking you to step up security? Is the problem a fear of external threats based on what's been in the papers lately?

Are there indications of a real risk of insider threats, such as a large population of super users or orphan accounts? Do you have overprivileged users?

The general drivers for action are well-recognized – compliance mandates, cost reduction, business enablement, risk avoidance – but identifying the things that are specific to your organization is essential to laying the foundation for a strong business case. The rest of the steps in the process all build on the needs assessment that's conducted at the very beginning.

Step 2

Establish Baselines

Establishing a baseline requires you to analyze what's working and what's not in your current environment. For example, if there is an issue in access delivery, what are the identity processes currently being used? How do users request access? Is there a form they fill out and submit to the helpdesk? Does the helpdesk take over the process from there? How? Creating a map that thoroughly documents all the parts of the process – identifying which parts are done manually, which are automated, how long they take and so on – will ultimately make it possible to understand how the work gets done and the associated costs.

Understanding who participates in the process is critical to setting a useful baseline. It's easy to underestimate the number of people who are affected by a process and it's also easy to fail to see how they are affected. It's important to identify all key participants – from the IT operations team, to helpdesk staff, to business users – and to understand the role they play and how they view their part in the process. Documenting their perceptions and issues is important, because their collective view can play a key part in getting funding for a program.

Once your current processes and participants are documented, that information can be used to determine the cost of the current approach. And while hard costs will likely have the greatest effect on the financial model, soft costs may resonate even more strongly with a business audience. The pain and frustration they experience from failed processes may be difficult to quantify in financial terms, but it can help present a strong business case to participants who are in a position to influence funding.

The baseline works almost like the "current location" function of a GPS. To map out a path to your goal, you must have a starting point.

In that sense, the next two steps build on the first two, because they're based on understanding the current situation: current capabilities, processes, participants and costs. Only with that understanding is it possible to set goals for your identity program going forward.

Step 3

Set Goals

Persuasive business cases are built by outlining a path to achieve real business goals. That may sound like an obvious point, but it can be easy to get bogged down in technical terms and lose sight of the business benefits that are likely to motivate decision makers to fund a program. The people who make funding decisions are generally business-oriented rather than technology-driven. They want to hear about the specific goals and measurable objectives in terms of what they mean to business users and business processes, as well as their impact on the overall risk posture of the organization.

So while the selection of a particular technology solution may come down to its architecture or another technical aspect, decisions at the business-case level are made based on what kind of solution the organization is acquiring, how much it's going to cost and what its ultimate business value will be.

A second point to remember in setting goals is that they must be clearly measurable. If, for example, you've projected that you're going to save the business $10 million over the next five years, you have to be able to show how you're going to attach specific measurements related to that goal. Similarly, if you've projected that you're going to reduce helpdesk calls for password resets or provisioning requests, you must be able to show how you're going to measure the reduction. If you can't measure it because you don't have visibility to the relevant information, it's best not to include the goal in the business case.

The final point for goal-setting is to be realistic, which can mean starting small and showing incremental value over time. This allows the team to establish credibility by not overstating the expected benefits. For example, a program can be broken down into multiple phases, rather than be undertaken all at once. Successes in the first phase can be used to document and validate the assumptions that drove the program to begin with, establishing that the projected benefits are indeed realistic and attainable. This can help unlock funding for future phases – potentially in far greater amounts than might have otherwise been initially available.

Automation is a valuable tool for making provisioning processes more efficient and accurate while at the same time lowering costs – but automating every system and every process across an organization can require a great deal of time and expense, potentially offsetting those benefits. Start small and build upon early success.

Step 4

Create the Financial Model

Calculating business value involves the process of weighing the benefits of a program against its costs. Estimating costs is a matter of thinking through how the program will unfold and what costs will be associated with every aspect of it. Will you be acquiring software? Hardware? Both? Will you require implementation services to deploy the program or will you handle it in-house? If it's the latter, will you have to add staff? What sort of ongoing support or maintenance will be needed for the program? Again, will you need an external service provider for this or can it be handled internally with existing staff?

Your next step is to quantify the program's benefits. You will need to document the specific improvements and how you will save the organization money with a new identity governance solution. How much will you save by reducing compliance costs? How much will you save by reducing helpdesk incidents? How much time will you save users waiting for access?

Here are some common metrics you should consider to quantify the financial benefits of your program:

Security

- Reduced time to compile access certification reports
- Reduced time to review and complete access certifications
- Reduced time to detect and remediate access policy violations
- Reduced time to compile audit reports

IT Operational Efficiency

- Reduced number of helpdesk incidents relating to passwords
- Reduced number of helpdesk incidents relating to access requests/changes
- Quicker helpdesk resolution times

- Fewer helpdesk escalations
- Reduced number of access changes performed by application administrators

User Productivity

- Quicker new hire provisioning
- Quicker ad hoc access changes and provisioning
- Quicker approval times on change requests
- Quicker resolution of password incidents (forgotten passwords, resets)

Reducing Security Vulnerabilities

- Expanded access certification coverage - more applications/users
- Quicker deprovisioning of terminated workers
- Orphan accounts detected and removed
- Higher number of excess privileges revoked
- Higher number of service accounts and duplicate accounts revoked
- Expanded number of applications with enforced password policy
- Expanded number of applications with multi-factor authentication

Once you understand the costs and benefits associated with a program, there's more than one way to measure its value. Every organization has its own preferred financial metrics. It may be based on the payback period, i.e., how quickly the investment in the program can be paid back in terms of months or years. It may be based on the return on investment (ROI), i.e., how quickly it can be paid back in terms of the value of the time and resources invested. The key is to align the financial model with the benchmarks that management expects to see. Payback period and ROI are typical metrics used by many organizations and are both easy calculations to include as a part of your financial model.

Once you've documented the specific metrics, you can begin to actually build out the individual components of the financial model, both on the cost side and on the value side.

SailPoint Can Help

SailPoint's open identity platform provides a strong, ROI-focused foundation for programs to address compliance, operational efficiency, user productivity and security challenges. With SailPoint, you can realize the benefits of automated access certifications and policy enforcement, access requests, provisioning and password management. Our next-generation approach is designed to help ensure the long-term success of any identity program while helping to minimize costs.

Meet Compliance Demands and Improve Audit Performance
SailPoint automates the common auditing, reporting and management activities associated with a strong compliance program, and integrates identity processes such as access certification and policy enforcement to deliver the strong detective controls that auditors demand. Improve operational efficiency

With SailPoint, you can significantly reduce IT support and helpdesk incidents relating to access changes and password issues. Using self-service password management and access request capabilities, end users can be self-sufficient, resulting in significant cost savings. And with SailPoint's provisioning solution, the majority of access changes can be handled automatically, eliminating the need for manual changes by administrators.

Streamline Access Delivery and Improve User Productivity
SailPoint's password management capabilities provide self-service password reset, so there's no need to wait on assistance from the helpdesk. SailPoint's automated provisioning quickly delivers access to new users, who no longer have to wait days to be productive. The secure access request service extends fast, secure access to users outside of typical lifecycle events such as joining or leaving an organization.

Manage Risk and Strengthen Security
Organizations can strengthen security and access controls to manage risk, using automated detective and preventive controls with SailPoint. Enforcement of strong password policies, automated policy checking, and periodic access reviews ensure that the right people have the right access to the right resources, and that organizational resources are not at risk of being misused or used fraudulently.

Real-world Successes

SailPoint has helped hundreds of customers achieve quantifiable benefits in compliance, operational efficiency, user productivity and security. Here are some recent examples:

Security: Eliminating excess entitlements
One of the most common results organizations see after using SailPoint to automate access certifications is a dramatic reduction in the number of excess access entitlements held by users. One international bank reported a 50% reduction in total entitlements after the first cycle of automated certifications with SailPoint. While 20 to 40% reductions are typical, up to 60% has been documented.

Compliance: Reducing resource requirements
A global insurance company saved the equivalent of 50 full-time employees annually in controls testing and documentation alone. The company accomplished this by using SailPoint to automate access certifications and access policy enforcement, and by reducing the number of auditors required to test the controls and document the processes.

Compliance: Increasing efficiency in access reviews
By automating access certifications with SailPoint, a multi-national financial services provider slashed the time it took to review and certify users' access by two-thirds. User access reviews that formerly took three months are now being completed in just four weeks.

Access Request and Provisioning: Improving user productivity
A major oil and gas company implemented SailPoint access request and reduced its average request fulfillment time from one week to two hours. Many access requests are now being completed in as little as 20 minutes.

Provisioning: Reducing IT operations costs
By using SailPoint to automate self-service access requests across the enterprise, a large process manufacturer was able to reduce IT operations costs by $1,000,000 in one year.

Password Management: Eliminating costly IT helpdesk calls
A global apparel and footwear manufacturer was able to replace an outdated password management solution and reduced IT helpdesk calls by 60%.

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 virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

WP1008-1710