SailPoint

WHITE PAPER

Seven Key Success Factors for Identity Governance

Insights and Advice from Real-World Implementations

You have been given a high-profile mission: address urgent audit and compliance requirements by implementing an identity governance solution across your organization. You know the scope of the project will include changes to the processes and technology you use today, in addition to the people involved, but you still have questions. Where do you start? How do you know where to focus? How have other organizations been successful?

From our hundreds of identity governance projects, we've learned valuable lessons in order to present real-world advice on how to plan, staff and implement identity governance projects, as well as how to avoid common mistakes and missteps. The take-aways from these real-world implementations offer insights from those that were involved, who share examples of what worked (and what didn't), common issues and barriers, and tactics to smooth the implementation.

All Identity Governance Programs Are Not Created Equal

Identity governance solutions play a key role in helping organizations meet compliance requirements. By automating processes for access certifications and policy enforcement, identity governance solutions can help your organization inventory, analyze and understand the access privileges granted to employees, contractors and partners – as well as answer the critical question: "Who has access to what?" These solutions can also allow you to increase efficiency and reduce costs by replacing slow, outdated compliance processes with modern, software-driven ones.

It's important to realize, however, that successful identity governance is not simply a matter of technology. In order to strengthen controls, improve audit performance and reduce compliance costs, you'll need a combination of people, process and technology. In fact, most organizations find that the people and process issues demand even more attention than the software. Successful organizations start with defining goals and metrics, building governance frameworks, staffing key positions and gaining internal support – before they install software.

Some projects never get off the ground, some fail to demonstrate clear business results and others get bogged down in complexity. How your team plans, allocates resources and champions the project can make an enormous difference in performance, results, the costs you will incur and the risk mitigation you will achieve.

Factor 1

Start with a Clear Understanding of Business Needs

Many organizations assume the first step is sending out a Request for Proposal (RFP) to various software vendors, but you need to begin your identity governance project with a clear understanding of where you are today in comparison to where you want to be. Before you've even thought about what technology to procure, it's critical that you develop a strategy. Real results will come from business process improvements, not software.

As the Manager of IT Security Compliance at one institution pointed out, "It's the wrong approach to buy a tool and then figure out access policies and controls." The first steps must be to define the goals that the new identity governance program will set out to achieve. Start by analyzing existing processes and tools and then list out their strengths and shortcomings, which will give you a solid foundation to understand your current situation. Only after you've completed the appropriate level of due diligence on your current processes and policies will you be ready to select a technology solution.

Bear in mind, a good identity governance strategy will be specific about business goals (audit performance, cost reduction), desired changes (fewer deficiencies, quicker access review cycles, faster remediations), the steps (process and organizational changes), and the information (metrics and data) to get there.

Don't let technolgy lead the program; identity your probems and how to solve them first.

Factor
2

Address the "People Component" as a First Priority

Identity governance projects often struggle when the project team doesn't truly understand the business needs, the complex rules and politics of the organization or the points of view of various stakeholders.

There is often a large gap in understanding between the technical side of the house and the business users, and this type of project typically requires the participation of many different groups within the organization:

1. **IT and security teams:** owners of technology implementations, evaluations and decisions. Often responsible for access governance and risk even though they don't own the data or applications.
2. **Business managers:** primary users of applications, many of whom understand data and risk, but do not feel ownership of access governance. May resist the need to understand and use IT tools.
3. **Business application owners:** technical owners of business applications and data, with valuable knowledge about the users and authorization models, and may act as gatekeepers over data.
4. **Audit and compliance personnel:** drive audit requirements and perform audit procedures. Interact with both IT and business staff to obtain the data needed to prove adequacy of controls.
5. **Operational risk managers:** dedicated personnel that provide risk oversight. Interact with audit, business and IT staff to assess and mitigate operational risks.
6. **Human resources personnel:** expected to provide identity data on employees and contractors.
7. **Senior executives:** provide budget and support. Very few projects are successful without them.

Your identity governance project plan should be designed to facilitate communication, collaboration, cross-functional processes and data flow among these groups.

Success requires you to combine the people who know what needs to be done with those who know how to do it – don't expect software to do this.

Factor 3

Work to Achieve Business Accountability

Managing user accounts and privileges and ensuring effective access control is not a mission that is commonly embraced by business users. In many of the organizations interviewed for this paper, the IT staff assumed (and eventually owned) responsibility for identity governance. Business application owners were not held accountable for ensuring adequate governance and compliance with internal controls. As a result, IT had responsibility for a set of risks that were actually business risks.

Our business units don't understand they are accountable for user access.

To succeed with an identity governance program, it's vital that the accountability and ownership of risk is assigned to its rightful owner: the business side of the house. Business users and application owners understand high-risk data and transactions, they understand employees' roles as well as the applications and data those users need to perform their job duties, and they are best qualified to define and enforce policies and controls that minimize those access risks.

Businesspeople often don't understand the technical side of identity and access governance, so it's natural for them to assume that IT and security teams should own governance. Business users may also feel that identity and access governance is a distraction from their real mission: generating revenue and profits for the organization. You must, in your project, get your business users to understand their role in the success of the project's implementation and what may happen when it succeeds or the consequences if it fails.

Factor 4

Choose Your Project Leader Based on Your Organization's Needs

The success of your identity governance project will depend upon the performance of key team members – the program or project manager in particular. It's vital that you find an individual with the right skills and motivation to truly lead the effort.

The ideal leader will bring a combination of business and technical skills. Business experience helps to ensure the project delivers business value and meets corporate objectives; technical knowledge will help to ensure a successful execution. Team leaders must also be strong communicators who can win over resistance and promote the project throughout the business, which means they must be respected in their areas of responsibility. Project leaders will play a key role in advocating change and ensuring the participation of departments and individuals that may not share their vision or commitment to the project.

You should recruit leaders who have credibility and can sell the message and how it affects business – someone who can align everyone internally.

Factor 5

Find and Maintain Strong Executive Leadership

All successful identity governance projects require executive sponsorship. From the planning phase through implementation, the right executive will be needed to champion the vision and importance to the company, secure the required resources and drive stakeholder participation.

It's important to recognize that identity governance is not a bottom-up, grassroots project. Much of the change management and championing needs to come top-down from senior management. An executive sponsor will play a key role in engaging with business unit managers, application owners, audit and compliance staff, partners and vendors to ensure they are supporting the project and are committed to its success.

This type of project will stall, **then fail** without executive support.

Changing business processes and people's behavior is a difficult task. Executive leadership is needed to convince the organization of the strategic importance of the project, ensure adequate IT staffing and funding, mediate departmental conflicts and set priorities.

Factor 6

Communicate Results Early and Often

Getting and maintaining stakeholder and executive buy-in will require an investment in communication. Don't wait until the project goes live to divulge plans, goals and expectations. And don't simply focus on execution plans and timetables; most stakeholders want to know why the project is important (e.g., risk exposures and possible consequences), what benefits it's attempting to achieve and what changes are coming that impact them.

You should show performance results as soon as you have meaningful metrics. Executives and business units will care about audit performance, as well as efficiency and process improvement; audit and compliance staff will care about control metrics; IT staff will care about implementation metrics and the impact of improved controls.

How you present data to people is critical. Don't assume people understand what you are asking for – you need to put it in their language.

Factor 7

Avoid the "Big Bang" Approach; Start Small and Build Momentum

Identity governance projects are very well-suited for phased implementation rollouts. You can focus initial phases of the project on a set of users or applications (e.g., one business unit), or you can limit functionality to one aspect of governance (e.g., access reviews).

A phased approach will be more manageable for the team to implement and will allow them to gain skills and experience that will benefit the project as you get further along. You will gain the flexibility to adapt your approach based on what you learn during early phases of the project, rather than being locked in to an enterprise-wide schedule and plan. Most organizations report that the work gets easier with time, as you build familiarity with your identity governance tool, application integration, end user training and communication, etc.

Most importantly, completing small phases in shorter periods of time (for instance, every 3 months) will allow you to show results and demonstrate clear value to the organization. More than any other factor, this will facilitate getting broader organizational buy-in, both at the business unit and executive levels.

Don't be afraid to go after the easy things first' this will help you build momentum. Leverage early success to build outward.

Key Recommendations & Takeaways

Through many implementations and their successes and hurdles, we've learned some key takeaways and recommendations that can help to increase the chances of success of your identity governance program.

1. Start with a Clear Understanding of Business Needs.

- Identify inefficiencies with existing governance practices, then consider what is needed to change or add new ones and define performance indicators (metrics) that will be used to measure results.
- Interview all stakeholders to identify requirements, what needs changed and why; then, prioritize them and base your policies and controls on the likelihood of risk and its potential consequences.
- Document roles and responsibilities that will be required to implement and support the program.
- Evaluate the quality of identity data that is currently available and how effectively it can drive governance decisions (this is often a bigger problem than organizations anticipate).

2. Address the "People Component" as a First Priority.

- Communicate your strategy so it is understood and supported by all involved.
- Frame the goals and objectives of the program so they clearly align to the business's needs.
- Use cross-functional forums to talk with and align stakeholders and track progress.
- Make roles and responsibilities clear, so each department knows what is expected.
- Conduct training so they grasp the need for and purpose of identity governance.
- Identify areas where you need to bridge gaps between business and technical staff. Many organizations use business analysts or consultants to help with this.

3. Work to Achieve Business Accountability.

- Use the carrot (e.g. reducing the burden of compliance activities) and the stick (e.g. the threat of negative audit findings) to get business units to own identity governance and risk management.
- Get assistance from groups like Internal Audit and Risk Management to help shift accountability, ensuring that controls, policies and negative audit findings are assigned with clear responsibilities.
- To underscore accountability at the business unit level, develop individual reports for business units, departments and divisions and then review these on a regular basis.

4. Choose Your Identity Governance Leader Carefully.

- If you can't find the right balance of skills in a single person, pair a business-oriented team leader with a technical team member, who can facilitate from a supporting role.
- Choose leaders that can "sell" the program, gain buy-in from business people, and have experience leading large, cross-functional programs.
- Recruit members from other departments that have the skills to spearhead the effort from their peripheral position. Building a broad platform of support will help drive the success of the project.

5. Find and Maintain Strong Executive Sponsorship.

- Don't assume the sponsor has to be from IT. Chief Executive Officers (CEOs), Chief Operating Officers (COOs) and Chief Risk Officers (CROs) have successfully championed projects.
- The right sponsor can gain support at the leadership level, communicate the project's purpose and importance to the business, and ensure the team knows their efforts are valued by management.
- The project team must work to keep the executive sponsor actively involved in the project through regular contact and updates. You want a sponsor that feels personally responsible for the project.

6. Communicate Results Early and Often.

- Use a variety of communications: emails, training events, presentations and others.
- Find the right frequency to communicate – don’t bombard groups with information they don’t need.
- Spend effort into showing each group their own unique data and performance over time.
- Focus on metrics and results that can motivate stakeholders and provide opportunities to have a two-way conversation with them; your ultimate goal is to change behavior.
- For executives, keep the report at the “big picture” level and make sure the metrics are tied to meaningful business outcomes, while briefing your executive sponsor at least twice per month.

7. Avoid the “Big Bang” Approach; Start Small and Build Momentum.

- Make sure your objectives have small timelines; start with realistic and achievable near-term goals and increase your ambitions over time. Don’t attempt more than you can handle.
- Go after the “low-hanging fruit” first. It means starting with the friendliest business units for some and the applications that integrate the easiest with your governance solution for others.
- Promote your early successes to build support and expand your scope to more applications and business units.

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.