Report

IBRS state of identity

Report from the frontline

Table of contents

Introduction 4
Methodology 5
Key findings 6
Section 1: Evolving strategically 6
Section 2: Complex identity in the connected & collaborative era 6
Section 3: Operational challenges 6
Section 4: Seamless experiences 6
Section 1: Evolving Strategically 7
Making a case for a strategic vision 7
Table 1: Tips for creating and identifying strategic vision 8
Security and compliance 8
Security leadership 8
Align to the current business objectives 8
Operational efficiency and cost savings 8
User experience and productivity 8
Collaboration with other teams 9
Table 2: Tips for collaboration on the identity program 9
Shared goals and objectives 9
Regular communication 9
Cross-functional workshops and training 10
Clear roles and responsibilities 10
Joint projects and initivatives 10
Section 2: Complex identity in the connected and collaborative era 11
Scalability and flexibility 11
Table 3: Tips for scalability and flexibility 11
Identity governance strategy must be adaptable 11
Identity governance frameworks must be flexible 12
Support the changing landscape for authentication 12
Solution selection 13

Managing federated identities . . . 13
Table 4: Tips for managing federated identities . . . 13
Access control . . . 13
Continuous monitoring . . . 14
Identity lifecycle management . . . 14
Rapid role changes . . . 14
Table 5: Tips to address rapid role changes . . . 15
Implement an identity governance solution . . . 15
Implement automated provisioning and de-provisioning . . . 15
Integrate identity mangement with core systems . . . 15
Compliance & working with auditors . . . 16
Table 6: Tips for compliance & working with auditors . . . 17
Stay informed . . . 17
Foster collaboration with auditors . . . 17
Educate auditors on organisational context . . . 17
Section 3: Operational challenges . . . 18
Automation and integration of heterogeneous systems . . . 18
Table 7: Tips for automation and integration . . . 19
Categorise applications . . . 19
Role discovery and privileges should be automated and continuous . . . 20
Section 4: Governance of privileged accounts . . . 21
Table 8: Tips for privileged access governance . . . 21
Factor in non-human identities with privileged access . . . 21
Regular role calls . . . 21
Conclusion . . . 22

Introduction

As technology and new ways of working continue to advance at an unprecedented rate, businesses face new and increasingly complex challenges when managing identity and access. This has never been more true than in today's digital age, where enterprise identity management and identity governance are critical components of overall security and compliance strategies.

This whitepaper aims to provide practical and actionable advice for identity specialists and busy business executives wanting to understand more about the issue and the opportunities.

Taken from the most extensive study into identity ever conducted in the region and two deep-dive roundtables with Australia's leading companies, this paper covers many modern challenges, including justifying future investments in identity governance, the increasingly complex contexts for governance, the need for greater control of federated identities, and the changing structure and skills needed by identity teams. It also addresses the costs associated with identity governance, auditing and certification fatigue, and determining roles in increasingly porous organisations.

Throughout the paper, we provide actionable advice and practical solutions for the modern challenges of enterprise identity management and identity governance. We aim to empower identity specialists and busy business executives to take control of their identity management strategies and ensure their organisations are secure, compliant and ready for whatever the future holds. We hope this whitepaper will serve as a valuable resource for all those looking to navigate the complex world of identity management in the modern era.

Methodology

Based on research conducted by IBRS, this report features two deep-dive roundtables with 32 of Australia’s leaders in identity. It is backed by a survey of 565 ICT and security executives and 30 face-to-face interviews . The research focused on modern challenges facing enterprise identity management and identity governance, including justifying investments, controlling federated identities, determining roles, and dealing with certification fatigue.

In this paper, IBRS has selected paraphrased roundtable participants and interviewee comments to illustrate key learnings and advice. Comments were edited for readability, but the intent has not been altered. In several sections of this report, specific vendors, including Microsoft, ServiceNow, Darktrace and SailPoint are mentioned by the participants. IBRS is not endorsing these vendors but is reporting on the participants’ views.

While sponsored by SailPoint as part of its ongoing commitment to providing research-based insights to the Australian and New Zealand markets, the research was conducted independently by IRBS, under Chatham House Rule and without vendor involvement in interviews or roundtable sessions. IBRS thanks SailPoint for its support.

“The State of Identity in Australia and New Zealand,” SailPoint, IBRS, 2023.

Key findings

Enterprise identity teams face several challenges in the increasingly complex contexts of identity governance. Some of these challenges include:

Section 1: Evolving strategically

Making a case for a strategic vision: Enterprise identity teams must be able to articulate a clear and compelling strategic vision for identity governance. The vision must outline the organisation's long-term goals, objectives, and roadmap for identity governance.

Collaboration with other teams: Identity governance requires strong communication and collaboration skills. Identity teams must work closely with other groups, such as IT, HR, and legal departments, to develop and implement effective identity governance strategies.

Section 2: Complex identity in the connected & collaborative era

Scalability and flexibility: With the rise of cloud services, organisations often need to interact with external partners and customers, requiring the management of federated identities across multiple platforms. The need for federated identities leads to increased complexity in identity governance, as teams must establish trust between systems while maintaining security and compliance standards.

Rapid role changes: The speed at which staff and managers change roles can create difficulties in managing access rights and privileges. Identity teams must constantly update and monitor access controls to ensure that employees have the appropriate permissions for their current roles and that access is revoked when roles change, or employees leave the organisation.

Compliance & working with auditors: The constantly evolving regulatory landscape adds another layer of complexity to identity governance. Identity teams must stay up-to-date with relevant laws and regulations and ensure their identity management practices comply with these requirements. Compliance is often deeply connected to audits from an identity team's perspective. Participants detailed shortfalls of audit service providers and the challenges of making security audits 'practical and realistic.' A key finding concerning audits is educating specific auditor personnel before audits and providing an organisational context.

Section 3: Operational challenges

Heterogeneous systems: Organisations often use various systems and applications, each with its identity and access management requirements. Heterogeneous environments make it challenging for identity teams to establish a unified and consistent approach to governance, as they must navigate the intricacies of each system.

Automation and integration: Automating identity management processes can help streamline governance and reduce the potential for human error. However, implementing and integrating automation with existing systems can be complex and resource-intensive.

Privileged access management: A critical challenge for enterprise identity teams is managing privileged access, particularly when administrators grant software solutions administration-level access rights.

Section 4: Seamless experiences

Balancing security and user experience: Identity teams must balance strong security measures against seamless user experiences. Balancing these two requirements can be challenging, as robust security measures like multi-factor authentication can sometimes hinder user experience or impede productivity.

Section 1:

Evolving strategically

Making a case for a strategic vision

During the roundtables, participants compared and contrasted how they communicated the case for additional investment into identity. While approaches differed significantly, all agreed that developing and communicating a strategic vision for identity governance is crucial, and tailoring it to the specific expectations and attitudes of board-level executives is essential.

Participants argued that there are two broad ways to approach board-level executives when making the business case for modern identity investment. Identity executives must carefully assess which approach will resonate most with their organisation's leadership, as this can significantly impact the success of their pitch.

Compliance-Driven Approach: The first approach emphasises the need for compliance, focusing on privacy, security, risk management, and legal aspects. When taking this approach, identity executives should demonstrate how investing in modern identity solutions will help the organisation meet regulatory requirements, protect sensitive data, and mitigate risks associated with identity management. This approach may appeal to executives who prioritise maintaining a strong security posture and are highly risk-averse.

Efficiency-Driven Approach: The second approach highlights the potential for improved efficiency and business outcomes from modern identity investment. Identity executives can showcase the tangible benefits of investing in identity solutions by discussing easier access to resources, better customer/client experiences, improvements to sales/market rates, automation, and more cost-effective controls over access rights. This approach may be more compelling to executives focused on driving business growth, increasing operational efficiency, and improving the overall user experience. It is more aspirational than the compliance-driven approach.

We summarised and organised the participant's recommendations into several categories for developing and communicating a strategic vision for identity.

Table 1: Tips for creating an identity strategic vision

Compliance-driven approach	Efficiency-driven approach
Security and compliance “Highlight the role of a robust identity management strategy in reducing the risk of security breaches, protecting sensitive data, and ensuring regulatory compliance. This is particularly good to do when audits have shown weaknesses or major breaches.” “Detail how the strategic vision will address current and emerging threats, such as insider risks, privileged access management with cloud services [especially software as a SaaS], and the challenges associated with hybrid and remote work environments.” **Security leadership** “Highlight the need for cross-functional collaboration and support from key stakeholders, such as IT, HR, and legal departments… Discuss the importance of fostering a culture of security awareness, providing ongoing training, and ensuring that all employees understand their role in risk management. Then link this to the guardrails that identity governance can make possible.”	**Align to the current business objectives** “Start by emphasising how the strategic vision for identity governance aligns with the organisation’s broader goals and objectives - don’t just tag it as a cybersecurity technology. Show how an effective identity management strategy can enable business growth, improve customer experiences, and support digital transformation initiatives.” **Operational efficiency and cost savings** “Explain how the strategic vision can lead to operational efficiencies and cost savings by streamlining identity management processes, automating repetitive tasks, and minimising errors.” “Use data that demonstrates how identity automation can reduce helpdesk costs, grant faster onboarding and offboarding processes, and make management of access rights and permissions less costly. Basically, show how new identity governance solutions can pay for themselves while improving the company’s risk stance.” **User experience and productivity** “Showcase how the strategic vision for identity governance will improve user experiences and productivity by simplifying access to systems and applications. Stress the importance of balancing security measures with user-friendliness to ensure minimal disruption to employees’ daily activities.” “Implementing single sign-on (SSO) and reducing the burden of managing multiple credentials is a big win. You can use that goodwill to generate an appetite for additional identity governance capabilities.”

In some cases, it may be possible to combine both approaches to make an even more powerful case for modern identity investment. By illustrating the interconnected nature of compliance and efficiency, identity executives can demonstrate how a robust identity management strategy can help the organisation stay compliant and drive operational excellence and business growth. However, it's essential to gauge the organisation's leadership priorities and tailor the message accordingly to ensure the case for modern identity investment is as compelling as possible.

By addressing these aspects and presenting a well-structured, comprehensive strategic vision for identity governance, enterprise identity teams can secure buy-in from stakeholders, obtain the necessary resources and support, and successfully drive their organisation's identity management initiatives forward.

Collaboration with other teams

Developing and implementing effective identity governance strategies require identity teams to work closely with various other teams within the organisation. This interdepartmental collaboration is crucial for ensuring a comprehensive and holistic approach to identity management. The ability to communicate and collaborate effectively is vital for the success of these efforts. Participants noted the following:

Table 2: Tips for collaboration on the identity program

Shared goals and objectives Establishing shared goals and objectives between identity teams and other departments is crucial for facilitating collaboration. By aligning the priorities of all parties involved, organisations can ensure that their identity governance strategies align with the overall business objectives and drive value across the entire organisation.	"Finding common ground between identity teams and other departments is key. By identifying shared objectives, we avoid having to continually re-make the case for identity investments. Remember implementing identity access and governance changes impacts everyone, so it's good to get ahead of any potential push-back or issues." "Our cross-departmental efforts thrive when we have clearly defined goals that resonate with everyone involved."
Regular communication Maintaining open lines of communication is essential for promoting collaboration between identity teams and other departments. Regular meetings, updates, and information-sharing sessions can help keep all stakeholders informed and engaged, allowing them to provide valuable input and feedback throughout the development and implementation of identity governance strategies.	"Putting identity into the language and day-to-day workflow of business stakeholders is essential. So we encourage regular dialogue between identity teams and other departments. It's crucial for staying aligned and addressing potential challenges." "Some business groups are investing in SaaS with very little input from the technology groups. We need to show them that by working with us, they can reduce the risks and make working with their latest solutions easier and safer. So SEO has become a big part of our outreach."

Cross-functional workshops and training

Organising cross-functional workshops and training sessions can help foster a deeper understanding of the challenges and opportunities associated with identity governance. By allowing teams to learn from one another, organisations can encourage a collaborative approach to problem-solving and decision-making.

"Technology alone won't cut it. Investing in cross-functional training is a powerful way to bridge the knowledge gap between identity teams and other departments."

Clear roles and responsibilities

Clearly defining the roles and responsibilities of each team involved in the identity governance process can help prevent misunderstandings and ensure everyone is working towards the same goals. By establishing clear expectations and accountability, organisations can facilitate collaboration and promote a sense of ownership among all stakeholders.

"One of the most important aspects of cross-departmental collaboration is ensuring everyone knows their roles and responsibilities. This clarity fosters a sense of ownership and drives successful outcomes for our identity governance initiatives."

Joint projects and initiatives

Encouraging joint projects and initiatives between identity teams and other departments can help to build trust and foster a collaborative working relationship. By working together on shared objectives, teams can better understand each other's challenges, strengths, and expertise, leading to more effective collaboration.

"We start with HR. By working together on shared projects to improve the onboard experience of new staff, we've deepened our understanding of the challenges faced by other departments. In particular, we were able to see just how difficult a change of manager can be to administer, with all of the knock-on identity issues it creates. Without treating identity as a joint effort, we'd simply not be aware of the issues."

Section 2:

Complex identity in the connected & collaborative era

Scalability and flexibility

A key challenge for many participants was adapting the identity programs to cope with change and growth. As organisations grow and evolve, identity teams must develop frameworks that can adapt to changing needs and expand to accommodate increased user numbers and new systems. Participants agreed that a scalable and flexible identity strategy is needed. Recommendations from participants included:

Table 3: Tips for scalability and flexibility

Identity governance strategy must be adaptable An adaptable identity governance strategy is essential for navigating the ever-changing organisational needs, regulations, and technology landscape. By prioritising adaptability, businesses can maintain compliance, enhance security, and improve user experience, ensuring their identity governance efforts' long-term success and resilience. Organisations should focus on developing a strategy that can quickly respond to new requirements, integrate emerging technologies, and support varied authentication methods	"Embracing new technologies and platforms is critical for modern identity management. A flexible governance framework should be able to incorporate emerging systems without requiring a complete overhaul of the existing infrastructure. It also had to factor in legacy on-premises solutions."

Identity governance frameworks must be flexible

Identity governance frameworks must be sufficiently flexible to adapt to evolving organisational needs, regulatory changes, and technological advancements. A flexible framework enables the seamless integration of new systems, accommodates changing requirements, and supports various authentication methods. To ensure long-term success, organisations should invest in adaptable identity governance solutions that can easily be updated and scaled to meet emerging challenges and opportunities. This is not just a matter of technical architecture but having processes in place to facilitate rapid change and adaption.

“As regulatory landscapes change, it’s crucial to have a flexible identity governance strategy that can adapt to new compliance requirements, reducing the risk of non-compliance and potential penalties.”

“There is a pressing need to improve how we handle hybrid work. Managing users and resources in decentralised and hybrid environments requires a flexible approach to identity governance that maintains security and compliance across various locations and networks.”

“Mergers and acquisitions require a flexible governance framework that can quickly integrate disparate identity management systems and consolidate user bases, minimising disruptions to business operations.”

“If you are in government, your identity framework must support machinery of government changes. This can be challenging when people are technically moved but need access to legacy systems and information. Planning for this scenario and having everything ready to go is essential. Think of it as a business continuity plan.”

Support the changing landscape for authentication

As the authentication landscape evolves, organisations must address changing expectations from staff and external stakeholders while embracing emerging technologies like ‘passwordless’ solutions. A flexible strategy that accommodates diverse authentication methods and keeps pace with new standards is crucial. By staying ahead of trends, enhancing security, and improving user experiences, businesses can adapt to the demands of stakeholders and promote the adoption of innovative authentication practices within their identity governance framework.

“A flexible identity governance framework must support a range of authentication methods, enabling organisations to adopt new authentication technologies as they become available and enhance both security and user experience.”

“When Microsoft first introduced Windows Hello, we rejected it for not being sufficiently secure. After improvements and some time in the market, we feel it is good enough for us. Because we have an open approach to authentication, accommodate it relatively easily within our identity framework.”

Solution selection Selecting the right identity solution requires carefully assessing current needs, scalability, and the ability to integrate with existing and future systems. Ensure that your identity governance framework defines the solutions needed rather than being dictated by the solutions. Adopt a modular and extensible approach, allowing for specialised tools to be used and replaced as required. This strategy helps manage costs effectively, supports growth, and accommodates the evolving identity landscape.	"There are still big gaps in all solutions. Microsoft is evolving its services quickly, but there are still gaps. We've taken the approach that identity solutions should be modular and extensible. That way, we can use specialised tools to get what we need right now and then, as the Microsoft 365 environment evolves, swap out the third-party products if it makes sense. "We don't want identity solutions to define our framework, but rather our framework to define what solutions we need." "A scalable identity governance framework helps organisations manage costs more effectively by allowing them to invest in solutions that meet their current needs while providing capacity for future growth."

Managing federated identities

In today's interconnected world, managing federated identities has become essential to identity governance. One critical challenge organisations face is governing the lifecycles of external and other federated identities. In addition, participants noted that the most common federated identity solution - Microsoft's Azure Active Directory - is not always suitable for all their federated identity needs. In some cases, third-party solutions or other workarounds are required. This is less a complaint about Microsoft's platform and more an issue of the sheer complexity of the environment for organisations that have complex contract workforce or that are going through mergers, acquisitions or machinery of government changes.

Table 4: Tips for managing federated identities

Access control Define clear access policies for federated identities, ensuring that external partners and customers have appropriate permissions to access relevant resources without compromising security.	"A key best practice for us has been implementing the principle of least privilege for federated identities... only granting access to the resources necessary for their [contractor] tasks." "We've found success in regularly reviewing and updating access policies for federated identities. This ensures that our external partners and customers have the appropriate permissions, and we can quickly adapt to any changes in our business or security landscape."

Continuous monitoring

Regularly assess and monitor the effectiveness of federated identity management processes to identify potential vulnerabilities, detect suspicious activities, and ensure the ongoing security of your systems.

"You absolutely need to be proactively detecting anomalies and potential vulnerabilities. We invested in a solution that monitors access and user behaviour - especially of that external [federated] identities. While the solution [we use] will not stop an initial intrusion, it detects aberrant behaviour and, if the risk is high, blocks the access and flags the security team."

Identity lifecycle management

Streamline the onboarding and offboarding processes for external partners and customers, managing their access rights throughout their lifecycle to minimise security risks and maintain operational efficiency.

"In our experience, closely monitoring the user lifecycle of external partners and customers has allowed us to promptly adapt access rights as needed. You need more than [Azure] Active Directory to do that well. We've put in place SailPoint as part of the solution, in particular, to help us identify and manage roles and apply governance over them."

Rapid role changes

One of the significant challenges identity teams face today is the rapid pace at which staff and managers change roles within organisations. This constant flux can create difficulties in managing access rights and privileges, as it demands continuous updates to access controls, ensuring employees have the appropriate permissions for their current roles. Furthermore, as roles change or employees leave the organisation, it becomes imperative to revoke access promptly to prevent potential security risks.

To effectively address this challenge, identity teams must adopt proactive strategies such as automating the provisioning and de-provisioning processes, closely integrating identity management with HR systems, and implementing either role-based access control (RBAC) or, for more complex environments, attribute-based access controls (ABAC).

The participants of the roundtable all stressed the need for automating the management of identities - including non-human identities. Modern Information Technology Service Management (ITSM) solutions (such as ServiceNow) were often part of the overall solution for larger organisations. The use of specialised identity governance solutions (such as SailPoint, who sponsored this research) where also mentioned favourably by the larger, more complex organisations, as such solutions act as 'master controllers' for the identity lifecycles. In these environments, the ITSM solutions act as intermediaries between core software solutions (ERP, CRM, FinOps, etc.) and the identity platform, while the specialised identity governance solutions moderate identity lifecycles. Of particular note was the use of ITSM tools to facilitate identity roles and permissions within legacy systems - discussed in more detail later in this paper.

Smaller organisations expressed that investments in tier-one ITSM tools were not feasible due to cost, scale and available skills. However, they did see opportunities for specialised governance solutions (again, mentioning SailPoint specifically) to offset the manual activities associated with identity discovery, role definitions, lifecycles and governance.

As detailed in section 1 of this paper, collaboration is also crucial for managing the rapid role changes within organisations. Maintaining clear communication channels with HR and other departments provides valuable information about upcoming role changes, enabling a more efficient and accurate update of access controls.

Table 5: Tips to address rapid role changes

Implement an identity governance solution Investing in a comprehensive identity governance solution can centralise and streamline the management of access rights and privileges across the organisation. These solutions offer advanced features like automated provisioning and de-provisioning, policy enforcement, and reporting, enabling identity teams to handle rapid role changes efficiently. By providing a holistic view of access rights and user activity, identity governance solutions can also help identity teams identify potential risks and ensure compliance with internal policies and external regulations.	"Implementing SailPoint was initially a challenging process - we had put a lot of effort into getting all business units on board. But the effort paid off. Automating and centralising our access management processes improved our security posture - directly impacting our security audit ratings. It also brought greater efficiency and transparency to identities, saving our team and other parts of the organisation a lot of manual work, which we report back to the business stakeholders."
Implement automated provisioning and de-provisioning Automating the process of granting and revoking access rights can significantly reduce the time and effort needed to manage role changes. Automated systems can be configured to update access controls based on predefined rules or triggers quickly, ensuring employees have the appropriate permissions for their current roles and limiting the potential for security breaches.	"I can't emphasise enough the importance of automating the provisioning and de-provisioning processes. It has significantly reduced the burden on our team and improved our ability to manage access rights in the face of frequent role changes."
Integrate identity management with core systems Establish a strong connection between your identity management platform and core systems - especially HR - to facilitate real-time updates on role changes, new hires, and departures. This integration enables a more efficient and accurate update of access controls, ensuring that employees' access rights remain aligned with their current roles and responsibilities. Note: integration is detailed more fully later in this paper.	"Integrating our identity management platform with our core systems, particularly HR, has been challenging but rewarding. It took a lot of effort and collaboration between teams, and we've established real-time updates on role changes, management changes, onboarding and offboarding. The key learning from our program was to get all the business teams involved, show what's in it for them, and focus on a few key roles for onboarding."

Compliance & working with auditors

A critical aspect of maintaining compliance is navigating the complex world of audits, which are often deeply intertwined with compliance efforts.

From an identity team's perspective, there are several challenges in working with audit service providers. One issue is the potential for audits to become overly theoretical, lacking practicality and realism in the organisation's operations. To overcome this, several participants noted that it is vital to foster a collaborative relationship with auditors, educating them on the specific context of the organisation and its identity governance practices. This can help ensure that audits are more targeted, relevant, and ultimately beneficial to the organisation's overall security posture.

Another key finding related to audits is the need to provide auditors with a comprehensive understanding of the organisation's identity governance landscape. This involves sharing detailed information about systems, processes, and controls in place and addressing any concerns or potential vulnerabilities identified by auditors. By working closely with auditors and maintaining open lines of communication, identity teams can better align their efforts with regulatory requirements and improve their overall approach to identity governance.

Table 6: Tips for compliance & working with auditors

Stay informed Identity teams need to stay informed about the latest changes and requirements related to their industry. By closely monitoring regulatory updates and requirements, identity teams can adapt their governance practices to ensure compliance and effectively mitigate potential risks associated with non-compliance	"This is not only about identity, but identity is the first bulwark in cyber. Our CISO has made it a priority to continuously monitor the regulatory landscape - especially due to the legislative kickback from recent breaches. We have a formal process to review and adjust our identity governance policies and procedures as the landscape changes. It's also the same process we use when new solutions or approaches become available, but that's more for external facing identity management."
Foster collaboration with auditors Identity teams should work hand-in-hand with auditors well before the planned audit, with each party clearly understanding the other's objectives. By fostering a collaborative approach, identity teams can build a more effective compliance program that considers auditors' governance requirements while supporting the organisation's business objectives.	"Honestly, most audits are cookie-cutter, check-box exercises conducted by juniors. And that does not benefit anyone. You get audit reports that simply don't reflect the reality of the business….By working closely with auditors and establishing a strong partnership, we've ensured our identity governance practices align with regulatory requirements in a way that meets reality."
Educate auditors on the organisational context Identity teams should provide auditors with detailed information about the organisation's identity governance landscape, including policies, procedures, and frameworks and how the organisation functions and its objectives. It is essential to point out where generic approaches to identity do not match the organisations' technology and workplace environment. This will help auditors better understand the scope and complexities of the organisation's identity environment, enabling them to conduct more effective and targeted audits. By educating auditors on the organisational context, identity teams can ensure that audits are more meaningful and beneficial.	"Providing auditors with a comprehensive understanding of our organisation's unique identity governance landscape has been critical in ensuring that their recommendations are practical, relevant, and tailored to our specific needs."

Section 3:

Operational challenges

Automation and integration of heterogeneous systems

Most organisations have a broad mix of systems and applications, each with unique identity and access management requirements. This heterogeneity can make it difficult for identity teams to establish a unified and consistent approach to identity governance, as they must navigate the intricacies of each system. A key challenge is integrating legacy (often on-premises) solutions into the identity ecosystem due to a lack of direct integration with m modern identity solutions, APIs or documented interfaces. Even so, most participants believe that the work required to automate identity controls over these aging systems is warranted, as it improves governance (and thus better compliance with audits) and streamlines onboarding and offboarding processes.

However, implementing and integrating automation with existing systems can be complex and resource-intensive. To overcome these challenges, identity teams must prioritise close collaboration with ICT operations teams and, increasingly, the business groups with administrative control over SaaS solutions.

Table 7: Tips for automation and integration

Categorise applications

A quick way to understand the extent of the integration challenge is to categorise all systems within the organisations as one of four types:

Direct connection: The solution can be addressed by the identity management solution (a.g., Azure Active Directory) directly, and with an identity governance solution interrogating and automating identity-related actions via that channel.

API connection: The solution's user permissions can be directly accessed and updated via secure APIs. In these cases, organisations often used existing ITSM tools to manage the integration, with identity solutions orchestrating the identity.

Batch: The application can import and export user and related identity information. In these cases, regular (generally daily) batches of users are exported to a secure location (e.g. an SFTP source) and matched against the identity solution's records to check for consistency. Application user changes are added to a batch file (generally, a CSV is formed from systems) and uploaded. Some organisations entirely automate these processes with ITSM tools, while others have a 'semi-manual' approach.

Black box: A few systems (including specialised hardware control systems) do not have any way to manage users and related identity information. There are two approaches to addressing these solutions. The first is to create a support ticket from the identity governance solution into the ITSM solution and manually create or update the identity. The second (less used) is to leverage RPA technology.

"It is important to automate everything you can. But trying to do everything [all integerations] using a single tool or approach is simply not realistic. We started by grouping our major systems - the ones with the most identities to manage - and then directly linked all we could. For those we could not, we use batch processes. It's ugly, but it works most of the time. Extracting and comparing the identity and roles regularly is very important."

Role discovery and privileges should be automated and continuous

A key challenge mentioned by participants when bringing older solutions into the identity governance environment is that not all can expose a sufficient level of detail relating to each identity's privilege within the solution. In these cases, it is best to treat the solution as a black box (as mentioned above) and treat all identity administrative tasks as ticket requests. It is also important to collaborate with auditors so they understand the practical limitations of reviewing such solutions.

"There are some solutions that identity management and governance solutions just can't manage. Rather than hammering these into place with all sorts of hacks, which generally don't work reliably, it is best to ring-fence them with tightly controlled manual administration processes. In short, only take on the identity battles you can win."

Section 4:

Governance of privileged accounts

From an identity governance perspective, privileged access accounts involve managing and monitoring access to sensitive systems, data, and applications. Administrators often can grant themselves, others and (often overlooked) software solutions privileged access. When ungoverned, granting privileged access creates significant security risks. Identity teams must establish clear policies and procedures for granting and revoking privileged access, ensuring administrators have only the access necessary for their roles and responsibilities. Identity teams must also monitor privileged access, detecting and responding to any suspicious activity in (near) real-time. Finally, identity teams need tools and processes to discover privileged access via the activities.

Table 8: Tips for Privileged Access Governance

Factor in non-human identities with privileged access Most organisations know the principle of 'least privileged access.' However, even organisations with the governance and guardrails to support the principle often discover that new solutions (especially in ITSM, automation, security, and even identity tools!) demand high-level privileges of other solutions to function. As a result, such solutions become a potential security vulnerability that allows criminals to escalate from one system to the next. It is imperative that all non-human identities with privileged access rights are reviewed and, where possible, rights restricted. Governance over these non-human identities should be considered a high priority.	"The real problem is that vendors are giving us lazy software. Rather than allowing us to provide specific rights, some of these tools want full super-admin access. We can't lock them down to an 'as needed' basis. All we can do is monitor what these applications are doing. That adds another level of complexity to our security monitoring." "We also worry that the functions such as elevated third-party products can change without much notice, and that, combined with largely unrestricted access, keeps me up at night."
Regular role calls Use identity governance tools to regularly review the rights allocated to roles and identities with exceptions.	"We put in place a service that scans and collates all the rights and helps us review roles. Being able to sweep and govern all of the identities for roles and rights regularly has enabled us to discover some blindspots that were called out in security audits. It also saves us a lot of time."

Conclusion

This study into better practices for identity indicated that while most organisations have the basics of identity management, many still struggle to govern the complex ecosystem of human and non-human identities. Identity lifecycles are often only partially managed. When first adopting identity governance solutions, organisations reported that up to 30% of identities uncovered were functionally expired or incomplete. This issue is further exacerbated by the need to support legacy solutions, the need to manage workforce and organisational structural change, and a rise in non-human identities with elevated privileges.

At the heart of these challenges is the need to have visibility over the identity ecosystem: understanding the roles, exceptions, integrations and orchestration of identities and their lifecycle.

The tips provided in this report will assist you in your identity journey.

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

sailpoint.com