STATE OF IaaS CLOUD INFRASTRUCTURE SECURITY AND GOVERNANCE
A Global Survey of Executives and Governance Professionals

September
2020

dimensional research
Sponsored by SailPoint
Introduction

This paper reviews a global research survey focusing on executive and governance professionals to understand current cloud infrastructure (IaaS) utilization and management practices. A total of 321 participants directly involved with IaaS compliance and governance completed the survey about their company’s adoption, use, and governance of IaaS environments. Individuals surveyed included executives and managers.

The research investigated current issues, risks, and challenges with IaaS environments as well as the tools used to manage access and governance of those environments. The data was examined to determine trends, risks, and opportunities for improvement to current IaaS challenges.

Executive Summary

This research finds a large majority (74%) of companies use more than one IaaS provider today, with almost half using three or more. The use of multiple IaaS vendors is a strategic practice of matching workloads, minimizing costs, and providing on-going business flexibility. Some companies report using as many as 7 or more IaaS providers.

Most participants, however, reported audit, compliance, and security issues with their IaaS environments. IaaS environments were reported to be complex, experience rapid, large scale changes, and often lack automation which makes controlling user access difficult. Nearly 7 out of 10 companies reported they use multiple tools for their IaaS environments. This leads to a staggering 97% reporting problems managing IaaS access. Adding to these challenges, nearly 1 in 3 companies use multiple teams to manage user access. 45% have experienced cyber security attacks and 25% suffered a data breach.

This all contributes to the finding that 91% of companies require manual processes to properly document and report on IaaS user access and activities. One surprising finding is that over 1/3 of companies do not perform regular governance reviews of user entitlements and actions. Yet, ironically, 8 out of 10 participants believe they have acceptable user access control for their IaaS environments. This represents a significant disconnect between actual compliance issues and the business risks the company is experiencing. Companies looking to minimize risk and increase efficiencies need to look at optimizing governance processes, as well as upgrading and consolidating tools that manage IaaS access and control.
Key Findings

- **Companies Use More than One IaaS Provider by Design**
  - 74% of companies use more than one IaaS provider, 42% use three or more
  - Most choose IaaS providers strategically based on workload, pricing, and business flexibility

- **Security, Compliance and Audit Issues Fueled by Visibility and Control Deficiencies**
  - Compliance, audit, and security issues top challenges with IaaS environments
  - 97% of companies experience problems managing IaaS access
  - 45% have dealt with cyber security attacks and 25% experienced a data breach
  - Nearly 1/3 of companies are managing access with different teams

- **Governance and Access Processes Lacking**
  - 91% of companies require manual processes to prepare user access reports for IaaS environments
  - Over 1/3 of companies do not perform governance reviews of IaaS user access and 32% admit they should
  - Surprisingly, 82% believe they have an acceptable user access control over their IaaS platforms which is counter to prior findings

Detailed Findings

**Use of Multiple IaaS Providers is Common**

Although IaaS has been around for about ten years, this research sought to understand current real-world adoptions and utilization trends. The findings reveal that 74% of companies currently use more than one IaaS provider, and just over 4 out of 10 companies (42%) are relying on three or more service providers. When IaaS adoption began, companies would often evaluate and try more than one provider, trying to identify key features and waiting for stable market leaders to emerge, which then traditionally leads to vendor consolidation.
While Microsoft Azure tend to be the most relied-on IaaS provider globally, there are some strong regional preferences. North America (NA) companies exhibit a preference for Amazon Web Services and Asia Pacific (APAC) businesses show strong patronage of Google Cloud. Europe, Middle East and Africa (EMEA) along with APAC companies utilize IBM SmartCloud much more than NA. In general, EMEA and APAC businesses exhibit greater diversity in IaaS provider utilization than NA.
Multiple IaaS Solution Use is Strategic

However, this data indicates years after IaaS adoption began that using multiple IaaS providers is common and, most importantly, intentional. 91% of companies shared that using multiple IaaS solutions is in fact part of their IT strategy. Historically, using cloud resources has often yielded forgotten and abandoned resources that the company is paying for, but that is not the case with IaaS.

When asked why their company chose to use multiple IaaS providers, participants provided numerous business reasons. Topping the list was matching workloads to best platforms (61%), and following that was best pricing at 51%. Completing the top 3 is preventing vendor lock-in (43%) which provides company agility and on-going cost management options. The next two answers of disaster recovery and international requirements were close at 38% and 35% respectively. All five of these answers represent a conscious approach to managing IT and the business for maximum flexibly, cost control, resiliency, and compliance needs.

**Why is your company using more than one IaaS cloud provider?**

- Matching best platforms to workloads: 61%
- Best pricing at the time: 51%
- Prevent vendor lock-in: 43%
- Disaster recovery strategy (business continuity): 38%
- International requirements (data sovereignty, GDPR, etc.): 35%
- Other teams selected different vendors: 34%
- Acquisition or merger: 27%
These results were broken down by region with some strong differences as NA companies focuses more matching the workload to the right vendors’ platforms. While both EMEA and APAC companies exhibit higher price sensitivity. Predictably both EMEA and APAC businesses are driven by international requirements such as data sovereignty.
IaaS Environments Suffer from Compliance and Audit Problems

Given the strategic use of IaaS, the research investigated what issues have occurred in IaaS environments. In fact, 88% of participants reported IaaS issues. Perhaps surprising is that both compliance issues and audit challenges tied at top spot at 52%, which beat out security issues (45%), and actual data breaches (26%). In most research, security issues typically lead most issue categories for IT environments, making these findings noteworthy.

Examining the results provides some clues as to the cause, such as wrong individuals having privileged access in nearly one-third (32%) of the companies, along with unauthorized users reported in a quarter of the companies (25%), both of which create compliance and audit failings as well as business risk.

Which of the following has occurred within your IaaS environments?

- Compliance issues (wrong people with access, violations, etc.) 52%
- Audit challenges (proper reporting of data to comply, meeting reporting deadlines, etc.) 52%
- Cybersecurity attacks (DDoS, advance persistent threat [APT], etc.) 45%
- Privileged access provided to wrong individuals 32%
- Data breach 26%
- Unauthorized users 25%
- None of the above 12%
These findings examined by region reveal that APAC companies experience significantly more IaaS issues than those in NA or EMEA. Yet, previously we noted that they use predominantly the same IaaS providers as EMEA and to a lesser degree NA. Thus, it is likely their tools and processes produce this increased exposure.
Managing IaaS Access is Challenging

Given the preceding finding about IaaS problems the research sought to learn what made access management difficult. In fact, 93% of participants listed challenges to managing IaaS user access. Topping the findings was complexity (59%) which counters the belief that using and managing cloud infrastructure is easy. Velocity of change (45%) and lack of automation (44%) compound the problem. Just below those is using multiple tools (40%) to manage access, which seems to create a perfect storm causing the earlier noted compliance and audit issues.

![Diagram: What makes managing access for your IaaS environments difficult?]

- Complexity: 59%
- Velocity of change: 45%
- Lack of automation: 44%
- Using multiple IAM tools: 40%
- Scale: 39%
- Nothing makes managing IaaS access difficult: 7%

SailPoint Cloud Governance helps you discover, protect and govern access to all apps, data, and privileged accounts across your entire multi-cloud environment all from a centralized view. SailPoint gives you a comprehensive view of access to all resources across your multi-cloud infrastructure.

From a single dashboard, our AI insights help you make faster, more informed access decisions, detect potential risks and easily enforce access policies for all users.

- See who has user access across your multi-cloud infrastructure
- Protect both privileged and non-privileged accounts
- Monitor user access for suspicious activity in real-time
- Prevent unauthorized access from human & non-human identities
Multiple Solutions Creating Problems

This research drilled down further on the use of multiple IaaS access tools. The chart below provides direct insight into a problem. Tied at 68% is the use of IaaS provider solutions as well as commercial identity management solutions which indicates that a larger number of companies are using overlapping solutions from an IaaS provider and their commercial solution. But the situation is worse than it seems, when we are reminded that most companies are using multiple IaaS providers. It seems a likely scenario that companies are using several different IaaS provider access solutions in conjunction with the commercial access solution, thus generating numerous access tools being used and different ones for each IaaS environment.

<table>
<thead>
<tr>
<th>Solution Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS cloud provider supplied access and identity tool</td>
<td>68%</td>
</tr>
<tr>
<td>Identity management solution (inclusive of apps, data, cloud platforms)</td>
<td>68%</td>
</tr>
<tr>
<td>In-house developed solution</td>
<td>39%</td>
</tr>
<tr>
<td>We don’t manage access to our IaaS environments</td>
<td>2%</td>
</tr>
</tbody>
</table>

31% of participants then admitted they have multiple teams manage access. This combination of multiple clouds, multiple access tools, and multiple teams is providing context for the cited audit and compliance issues earlier in the report.

Does the same team manage access and governance of your organization’s on-premises applications and cloud applications?

- Yes, the same team manages both environments 69%
- No, we have different teams 29%
- We don’t manage access of and governance for both cloud and on-premises applications 2%
Current IaaS Access Tools are Failing to Provide Governance

Perhaps not surprising at this point is that 97% of participants provided a list of issues they have with IaaS user access solutions. The first five challenges are nearly tied, separated by a mere 2%. At the top is difficulty in enforcing governance requirements (39%) which now ties tool challenges to previous reported compliance and audit issues. Incomplete view across IaaS platforms (38%) is directly attributed to multiple access tools and teams today. Three challenges tied for the third spot (37%) are lack of visibility into DevOps teams’ actions, lack of features to manage and secure privileged user access, and lack of visibility into unused privileged user access. These three data points indicate that even with the numerous access management tools in use, teams don’t have needed features for visibility and control, and thus can’t properly govern their IaaS environments.

Which of the following challenges have you experienced with solutions used to manage access across your IaaS environments?

- Difficulty enforcing governance requirements (reviewing access, separation of duty checks, automated lifecycle management): 39%
- Incomplete view of access across all cloud platforms: 38%
- Lack of visibility of DevOps team’s activities (creation, deletion of data and workloads): 37%
- Inefficient capabilities to manage and secure privileged credentials: 37%
- Lack of visibility to unused privileged access: 37%
- Inability to generate audit trails of who accessed what and when: 33%
- Reliance on manual reporting of access to cloud platforms and workloads: 33%
- Lack of integration with your organization’s overall identity program: 33%
- There are no challenges to managing IaaS access: 3%
- None of the above: 2%
Providing evidence to the previous findings of APAC companies having significantly more IaaS issues, APAC participants reveal more challenges with tools in nearly every category over NA and EMEA users. EMEA companies report the fewest challenges perhaps due to higher data control and security requirements which can drive more stringent processes and better tool utilization. The fact remains there are far too many IaaS access tool issues.
IaaS User Access Report is Lengthy, Requiring Manual Processes

Given the preceding findings on governance issues with companies’ IaaS environments it was expected to find that 91% of companies perform manual steps in preparing IaaS user access reports. The use of numerous IaaS tools with missing features are likely contributors to this finding.

The research finds that 39% of executives state it takes days, weeks, or months to create user access reports as well as the diversion of personnel resources to create the report. This reporting delay creates more difficulty meeting compliance requirements. Slow reporting also creates an overall governance issue, creating delays in detecting and addressing inappropriate access.
Governance Processes Missing in One-Third of Companies

An unexpected finding from the research is that over one-third of participants don’t schedule regular governance reviews of user access to their company’s IaaS environments. Given the top issues of compliance, audit problems, and security issues, it appears irresponsible to not have a simple access review process. In fact, 32% of participants agree that it is a good idea that their company should employ on-going governance reviews of access but do not currently do so.

![Pie chart showing the responses to the question: Does your organization schedule on-going governance reviews of current user access to your IaaS environments?](image)

- Yes 66%
- No, but it is a good idea 32%
- No, and we don’t need that level of governance 2%
Complete Disconnect

The research by design gave participants an opportunity to rate their company’s approach to IaaS governance and access management. Surprisingly, 82% said they provide acceptable control over their IaaS environments. This is despite previous admissions of compliance and audit issues, lack of tools features for control and visibility, and the fact that some companies reported lacking key governance processes. This disconnect represents the worst kind of risk to a company - either they are unaware of the risk or simply dismiss it. But this risk is not just from compliance or audit penalties but is a risk to business operations and company liability for accidental or intentional actions to applications, services, and data.

Conclusion

This research finds that companies are intentionally using multiple IaaS cloud providers for strategic business reasons. This is a trend that is expected to continue. But those environments have risk for their company as participants cited audit challenges, compliance issues, security attacks, and data breaches. Those surveyed shared that the IaaS environments are complex and rapidly changing but relying on numerous tools and multiple teams to manage user access. The data in this report reveals the tools are not adequate and are partially responsible for current IaaS access issues and cultivate the opportunity for further IT and business problems.

This research indicates that companies need to make a concerted effort to consolidate and improve their IaaS access management solutions. IaaS governance tools need to provide automation that matches the speed and complexity of the applications, services, and data in the IaaS environments. The improved tools should automate reporting for audit and compliance which increases visibility and reduces resource waste. Lastly, the solution should create and reinforce proper identity and governance processes. IaaS and cloud resources are huge resource options for IT and run applications that directly enable the business, but they represent a significant business risk should access fall into the wrong hands.
Survey Methodology

A cross section of IT and business roles at managerial and executive levels were invited to participate in a survey on their company’s use of IaaS environments, as well as tools and processes to manage user access needed for governance and compliance requirements. All participants were directly responsible for IaaS compliance and governance at enterprise companies.

A total of 321 qualified participants completed the global primary research survey to understand current cloud infrastructure (IaaS) utilization and practices. The research also investigated current cloud usage and tools as well as defining current governance capabilities, needs, and gaps.

The survey was administered electronically, and participants were offered a token compensation for their participation. Participants were from all 5 continents.
About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit www.dimensionalresearch.com.

About SailPoint

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world’s most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers’ dynamic business needs. For more information, visit www.sailpoint.com.