Identity & Access Management (IAM) and Customer IAM (CIAM): A Pulse Survey of several global corporations over their current usage and exploitation of automated IAM and CIAM solutions

ANASTASIOS LIVERETOS, IVO DRAGANOV,
Technical University of Sofia,
8 Kliment Ohridski Blvd., Sofia, 1756
BULGARIA

Abstract: In this paper results from a survey made among 24 global corporations, operating in 17 different industries, about the automated Identity and Access Management (IAM) and Customer Identity and Access Management (CIAM) solutions, currently employed by them, are presented. The survey is organized in 5 parts, containing eligibility statement, a couple of questions on the implementation of Identity Governance and Administration (IGA) technology, question on the IAM process, and separately – on the CIAM process, followed by a question on particular use-cases. The results are mostly consistent with the current trends in the field, found by other recent studies on a world scale. There are, however, interesting examples of exceptions into the application of IAM solutions for a few major companies and numerous specifics on the particular expectations and the actual success rate of handling all identities in the rest of the respondents. Useful directions for deeper investigation of the technical and organizational aspects of an effective implementation of IAM solutions could be derived from these results, followed by recommendations for more efficient exploitation.

Keywords: Identity and Access Management, Customer Identity and Access Management, Identity Governance and Administration, System Integration, Data Migration, Business Process, Data Privacy Risk.

Received: July 9, 2021. Revised: August 11, 2022. Accepted: September 14, 2022. Published: October 6, 2022.

1. Introduction

THE unpredictability of human behavior has led companies to develop Identity and Access Management (IAM) capabilities. Humans, if left to operate in an environment free of boundaries, tend to overexploit the situation and overuse their freedom within this environment. When this translates into a corporation, it may put at risk systems, data & data quality, intellectual property, industrial competitive advantages, etc. [1], [2].

IAM is the means for a company to protect its assets from any wrongful usage. IAM includes the specific technology, relevant processes and trained people, who in combination guarantee that access is given to the right users at the right time for the right resources within a given environment [3]. The complexity of IAM coupled with a lack of culture for compliance provides one of the biggest challenges in implementing Identity Governance and Administration (IGA). Endorsement from senior leadership is often more needed than proving the ROI of an investment in this area [4].

F5 Networks, in their white paper published in 2016, recognize the distribution of applications as an area of attention for IGA. With applications varying from cloud-based to SaaS to local and every hybrid combination of them, managing identities is an increasingly complex task [5]. Multitenancy and third-party managed infrastructure with a continuous shift towards a cloud environment makes it necessary to have an IAM mechanism [6].

Moreover, customer centricity, powered mostly by e-commerce, drives organizations to prioritize customer experience and ability to scale. Traditional authentication methods may lead to a degraded customer experience. Thus, customer verification process follows different techniques, supported by different Customer Identity and Access Management (CIAM) solutions [7]. Balancing between data security and user experience is the main challenge [8].

In this paper we will discuss how several big corporations have been addressing their IAM capability building, what technology they use, what is their strategy on IGA and what are their plans regarding CIAM.

2. Methodology

In June 2021 a questionnaire (appendix 1) was purposely developed and shared with corporations worldwide.

The structure of the questionnaire was as follows:

- Eligibility statement;
- 2 questions on IGA technology;
- 3 questions on IAM process;
- 2 questions on CIAM process;
- 1 question on use-cases.

24 replies were received from companies functioning in 17 different industries (appendix 2).

3. Results and Analysis

3.1 Main observations

The main observations are:

- 2 of 24 (8%) do not use any centralized IGA solution for either their IAM or CIAM. Thus, they did not pass the eligibility statement.
- 11 of 22 (50%) use Sailpoint (https://www.sailpoint.com/) as their central IGA solution.
- 14 of 22 (64%) use additional and different CIAM solutions, on top of their IAM ones, to support external identities.
- 12 of 14 (86%) use CIAM solutions for providing a better user experience to their external identities – mostly driven by customer service focus.
- 13 of 22 (59%) have IAM solutions on premise; 5 of 22 (23%) have IAM as Software as a Service (SaaS), 4 of 22 (18%) have both on premise and SaaS.

3.2 Eligibility Statement

Q. Do you currently leverage at least one central IGA solution as part of your overall IAM strategy?

The distribution of the answers is given in Fig. 1.

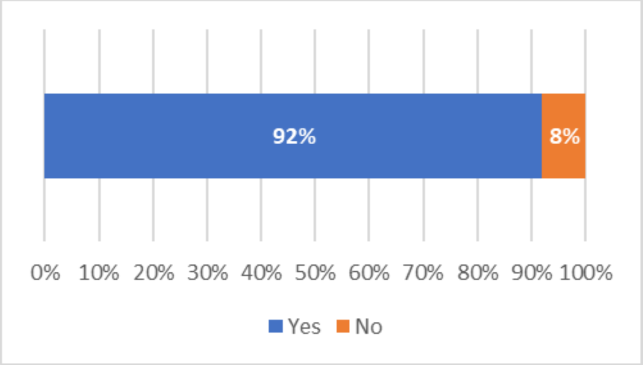

Fig. 1 Eligibility statement answers distribution

Company 3 (healthcare) and Company 24 (Tobacco) replied that they use no central IGA solution. The remaining 22 companies confirmed the usage of at least one IGA solution.

3.3 Overview of IGA solutions

IGA solution suppliers

Many variables influence peoples' behavioral intentions with the selection of IGA solutions. These factors include usefulness, simplicity of use, task–technology fit, trusting attitudes, confidence in the Internet (including information sharing), privacy concerns, and cost [9].

The results from answering the question above are presented in Fig. 2.

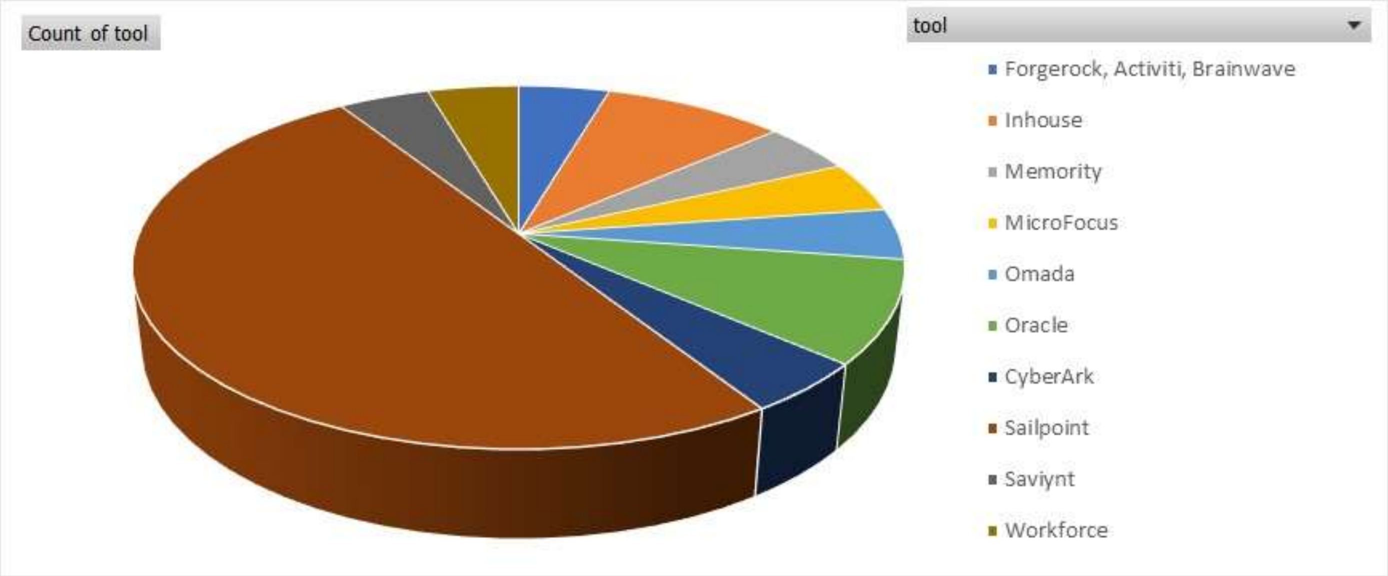

Fig. 2 Central IGA solution distribution

11 of 22 (50%) of the respondents use SailPoint. 6 of them use SailPoint IdentityIQ; 2 use SailPoint IdentityNow.

Of the 11 respondents, who do not use SailPoint, 2 use Oracle Identity Management and the remaining 9 use various different solutions or combination of solutions.

3 of the respondents are in the process of implementing an IGA solution. Company 15 (HealthCare) is looking into Workforce Tuebora (https://www.tuebora.com/) as a cloud-based solution and Company 19 (FMCG) is moving to MicroFocus (https://www.microfocus.com/en-us/home).

Company 21 (Tobacco) is currently using a combination of several different solutions, most of which legacy ones, for the variable personas/user groups. It is however in the process of moving to a unique modern solution for all IGA.

Central IGA Solution and System Integration

19 of 22 (86%) have integrated Microsoft Azure AD (https://azure.microsoft.com/en-us/) with their central IGA solution. It is evident that IGA solutions primarily address internal users.

11 of 22 (50%) have integrated SAP ERP (https://www.sap.com/products/enterprise-management-erp.html) and Salesforce (https://www.salesforce.com/). 4 of 22 (18%) have integrated Okta (https://www.okta.com/) and Ping (https://www.pingidentity.com/en.html).

The various integrations being made are shown in Fig. 3.

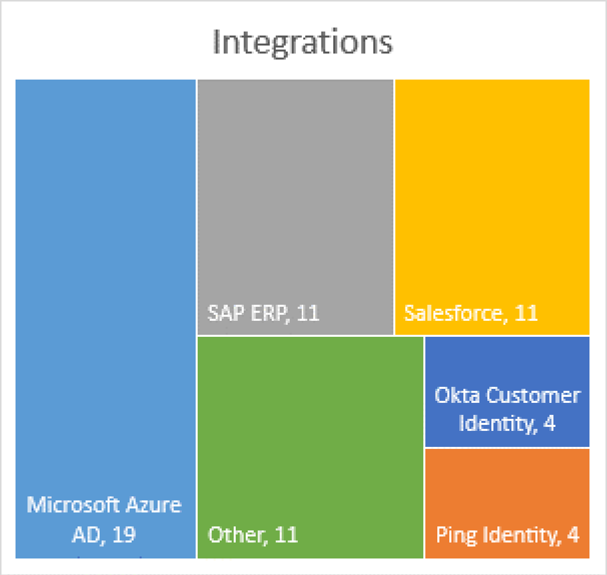

Fig. 3 Eligibility statement answers distribution

4 respondents integrate with variable Oracle solutions such as Oracle Database, Oracle Enterprise Performance management, Oracle Lightweight Directory Access Protocol, Oracle e-Business Suite, Oracle Cloud Enterprise Resource Planning and Oracle Human Capital Management. Moreover, 2 respondents each have integrated ServiceNow and Workday.

Finally, various respondents have integrated Microsoft Office 365, SAP Ariba, TrackWise QMS, CyberArk, Amazon Web Services, Google Cloud Platform, Memority, Usercube and ForgeRock.

Coverage of IGA solution

Legacy Systems, Bring Your Own Device (BYOD), Shadow IT, Cloud Computing and Unstructured Data make it almost impossible for organizations to manage centrally user access for all systems and applications [10].

50% of the participants operate less than 30% of their systems with their primary IGA solution (Fig.4.). 4 of 22 (18%) have managed to integrate >80% of their systems.

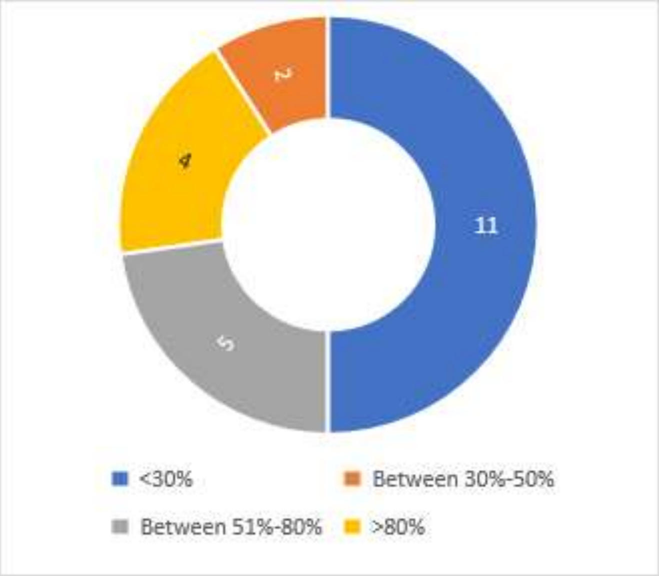

Fig. 4 Coverage of applied IGA solutions

Despite the focus of all participating corporations on risk mitigation, cybersecurity, data governance, it is evident that there is a lot of ground to be covered in securing the gateways via centralized and unified solutions.

3.4 Identity and Access Management (IAM)

IAM Model

IAM's gyrations from a mature, consolidated state (on-premises) back to once again straining to support too many directories and user sign-ons (in the cloud) suggest that rationalizing and simplifying IAM (and IT) is not a one-time fix, but a generational challenge the industry experiences each time new infrastructure platforms, applications, and use cases appear [11].

13 of 22 (59%) of the participants base their IAM solutions on premise and only 2 of 22 (9%) have completely outsourced the complete service (Fig. 5).

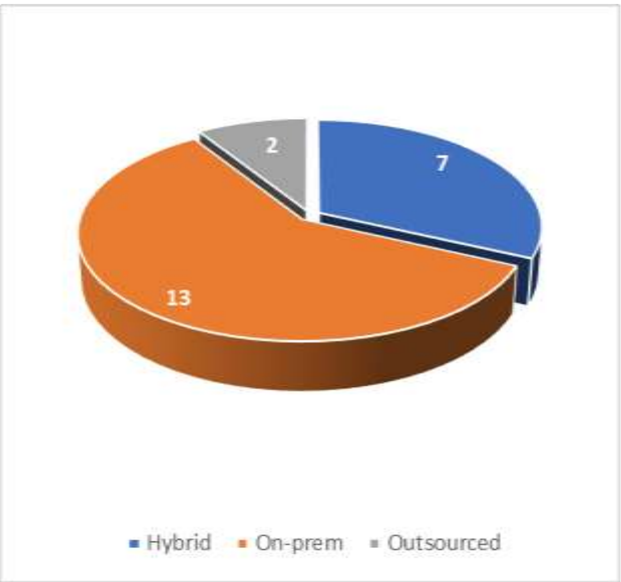

Fig. 5 Type of IAM solutions, based on co-location

When diving into the qualitative information provided by the respondents, we have identified the following:

On Premise:

- 6 of 13 (46%) have developed internal skills to manage their on-prem solution.
- 4 of 13 (31%) are considering outsourcing some function, especially in the are of operational support and "offloading" of storage and infrastructure.

Hybrid:

- 5 of 22 (23%) use a hybrid model based on SaaS; 3 of these have developed internal skills to manage the SaaS solution.
- 2 of 22 (9%) have both on-prem and outsourced solutions strictly separated based on the type of persona/user.

Internally managed vs Outsourced

It is often considered as best practice to coordinate with third-party management (outsourced) and maintain internal development teams for new or changing systems, regardless of if they are on premise or in the cloud [12], [13].

In our survey, contrary to what bibliography suggests,14 of 24 (58%) of the participants manage their IAM solution 100% internally (Fig.6). It is our observation that most Companies considered any risk with accesses best managed, if it is done by internal resources.

Only 3 of 24 (2 of which are the ones with no centralised IGA solution) are 100% outsourced.

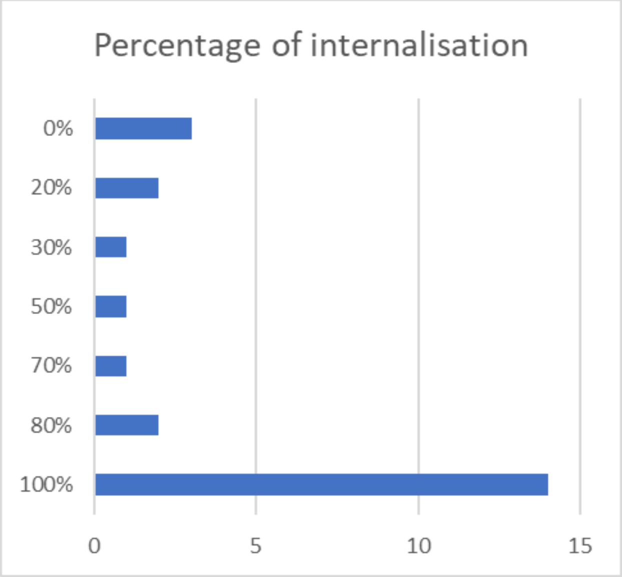

Fig. 6 Internalization level of IGA solutions

Stated benefits of Outsourcing IAM Solutions

- Company 17 (Power Systems) has outsourced 100% of its IAM to Infosys and Cognizant, aiming to achieve cost benefits and higher compliance and governance standards.
- Company 20 (HealthCare) has outsourced 80% in order to benefit from economies of scale and access to up-to-date technologies.
- Company 13 (Petroleum) has outsourced 70%, relieving its internal employees from the repetitive, low value adding activities.
- Company 11 (Financial Services) has outsourced only 20% and uses it for providing agility and adaptability to changing business priorities.

Size of IAM teams and relevant challenges

The size of the combined internal and contractors IAM teams varied a lot in our sample. Companies 10 (Winery) and 12 (FMCG) reported only 3 internal resources and no contractors working on IAM. At the same time, Company 15 (HealthCare) reported 90 internal and 60 external resources working for IAM. We attempted to run several correlation reviews on our sample, trying to link the size of the IAM team to either total HC or Revenue of the relevant company, but not such correlation was observed. We consider the responses on this question as not adequately qualified for drawing any significant conclusions.

IAM and Zero Trust Principles

"Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location" [14].

Most of our participants identified IAM as the means to address Zero Trust Principles and specifically the following:

Multi Factor Authentication (MFA): 9 of 22 (41%) moved to MFA for access control. All participants indicated that where passwords are used as the "something you know" element of the MFA, these are strong, following specific requirements (length, usage of lower and upper case, special characters, numbers) and in a lot of cases replaced by pass-phrases.

Privileged Access: 4 of 22 (18%) specifically mentioned switching to role-based access provision, which is automatically provided by the IGA solution.

Predictive Access: Company 18 (Pharmaceutical) plans to deploy access provision based on peer group patterns. The aim is to provision, deprovision and reprovision accesses automatically, if certain criteria are met.

Least Privileged Principle: Participants quoted that standing privileges are frequently reviewed and removed. Only standard role/attribute-based access are provided. Any additional accesses are granted based on request and specific approval. Company 1 (FMCG) specifically provided their strategy as shown in the following pyramid, indicating the discrete access levels and how they are provided (Fig. 7).

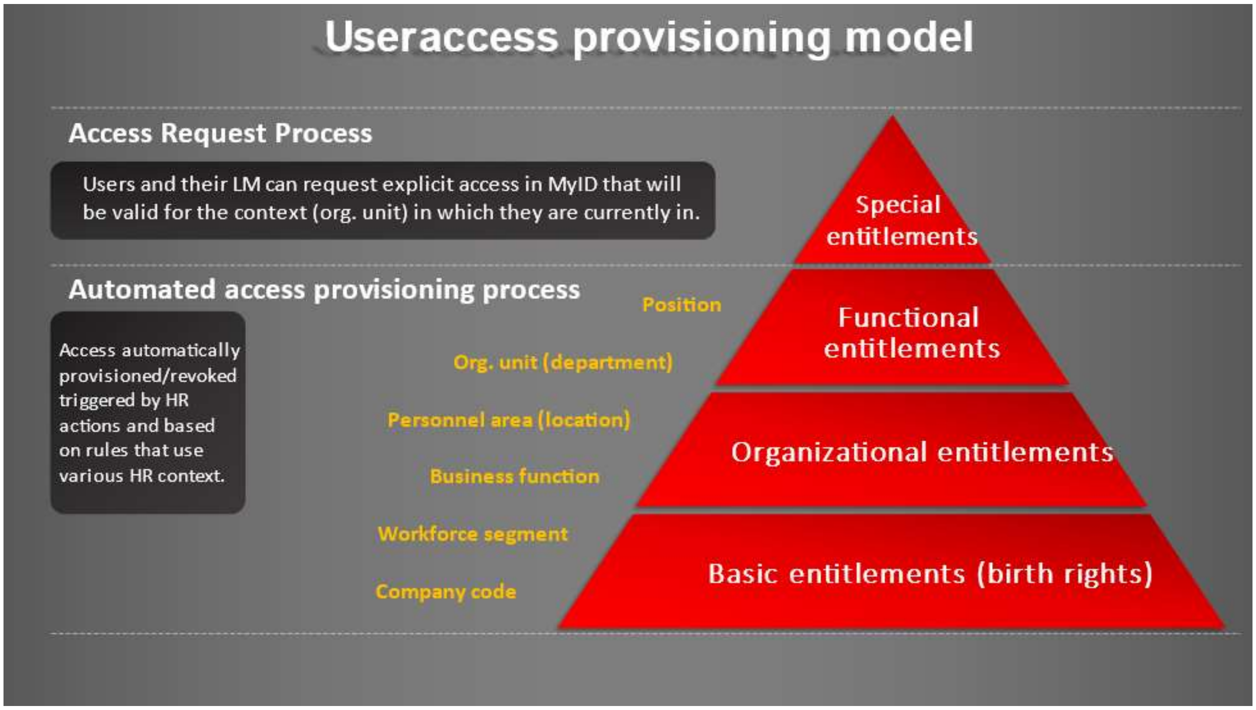
Useraccess provisioning model
Access Request Process
Users and their LM can request explicit access in MyID that will be valid for the context (org. unit) in which they are currently in.
Automated access provisioning process
Access automatically provisioned/revoked triggered by HR actions and based on rules that use various HR context.
Position
Org. unit (department)
Personnel area (location)
Business function
Workforce segment
Company code
Special entitlements
Functional entitlements
Organizational entitlements
Basic entitlements (birth rights)

Fig. 7 User access provisioning model.
(This is artwork of the corresponding author of the report, as part of his employment with Company 1.)

Manual IAM provision

Hub City Media an IAM consultancy firm points out the risk of managing accesses manually, maintaining numerous spreadsheets and having poor processes leading to subjective rather than objective provision/deprovision of accesses. An experienced IGA team is not -on its own- adequate to contain the risk. Technology solutions are nowadays quite advanced in containing these risks [15].

We asked the participants to evaluate whether for systems where access is managed manually (i.e., directly in the system by the user administrator, rather than by the IAM system), there may be a greater risk of error (e.g., excessive access, continued access for employees no longer with the organization, etc.). 17 of 24 (71%) replied that this is a major challenge, with the remaining 7 (or 29%) appreciating that this provides a minor challenge. None of the participants replied that there’s no challenge at all.

3.5 Customer Identity and Access Management (CIAM)

CIAM Solution Suppliers

CIAM requirements are very different to those for IAM. The key features of CIAM include: Cloud-based hosting, Platform-based functionality, Strong authentication and syndication, Integration, Scalability and Interface customability [16]. These very particularities drive organisations into adopting additional solutions to support them with the management of their external identities (Fig. 8.).

14 of 22 (64%) of the participants leverage at least one CIAM solution, along with their IAM ones, to support the identities of their external personas/users.

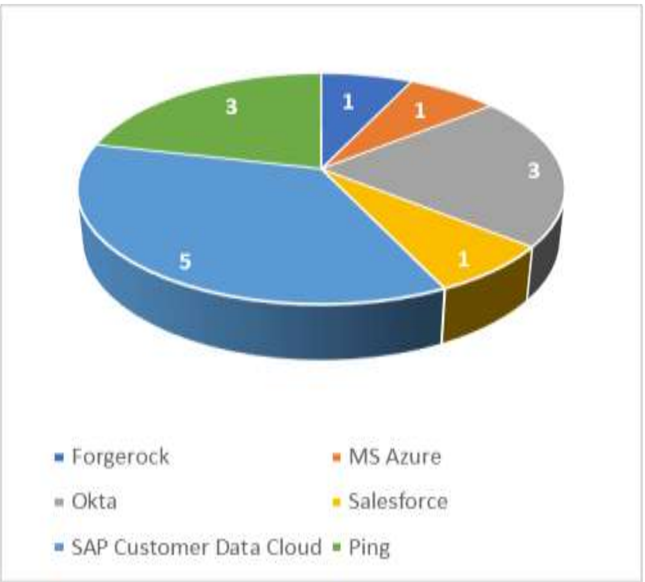

Fig. 8 Distribution of CIAM solutions suppliers

5 of 14 (36%) of the respondents use SAP Customer Data Cloud (previously known as Gigya). Moreover, Company 2 (Pharmaceuticals), which is currently using MS Azure, is in the process of migrating to SAP Customer Data Cloud, too.

3 of 14 (21%) use Okta and another 3 use Ping Identity. Of the latter 3, Company 9 (HR Services) is also using CA

Siteminder and Company 18 (Pharmaceuticals) is using SailPoint.

Amongst the Companies that are not currently using any CIAM solution, Company 7 (Automotive) is looking into Azure AD and Company 22 (Energy) is investing into building a home-grown solution for managing external identities.

CIAM business drivers

The majority, 12 of 14 (86%), of the participants rely on their CIAM solution to "unify user experience", while 10 (or 71%) are aiming to "replace homegrown systems" (Fig. 9).

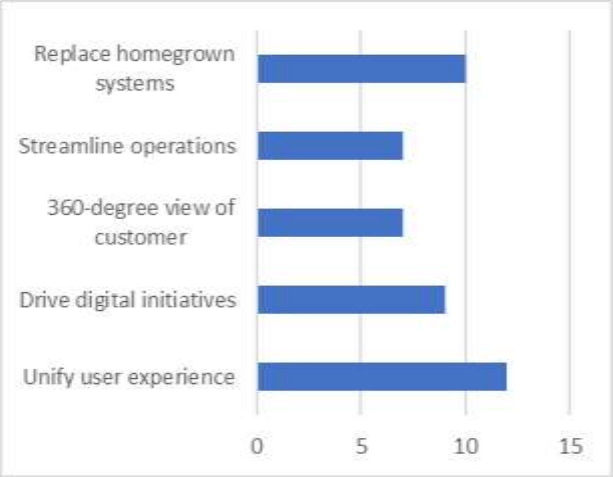

Fig. 9 CIAM business drivers

Similar results are published in July 21 by EMA in their research on "Achieving business success with CIAM". 80.1% of their participants (201 business professionals) recognized an increase in customer satisfaction once CIAM was introduced [17].

Benefits of Adopting CIAM

The benefits of adopting CIAM solutions are presented in Fig. 10.

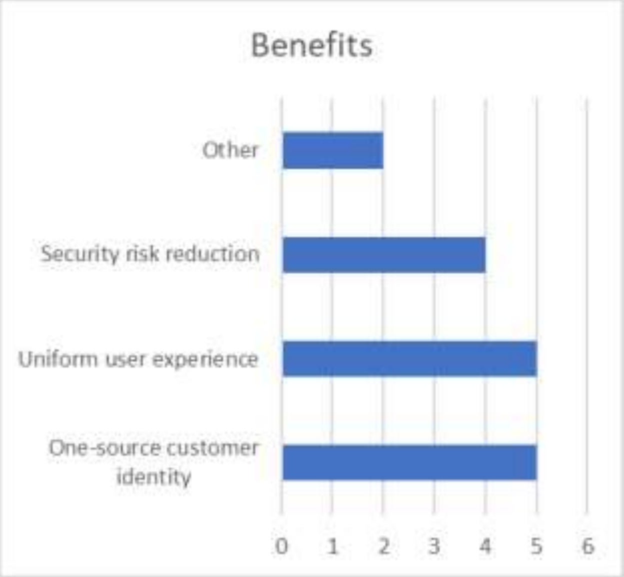

Fig. 10 Benefits of adopting CIAM solutions

One-Source Customer Identity: 5 participants indicated the one-source customer identity as the main benefit captured by CIAM. In their qualitative comments they also mentioned: "unified onboarding and easy enforcement of access policies" and "access management made easy for customers who pay subscriptions".

Uniform user experience: 5 participants see the benefit from the side of the external identity as the experience to accessing the Company's resources is expected to be easier and more friendly with the introduction of a CIAM solution. They also commented on "better user engagement", "ability to federate" and "better uptime and operations management for the customer portals".

Security Risk Reduction: 4 participants pointed out security as a benefit of CIAM. Special mentioning was made on "better legal compliance management", "managing local regulations in multi-location businesses" and "introducing secure methods to log in via mobile and/or social media".

Other: CIAM has helped reduce the volume of manually executed access control and have supported the integration of downstream processes such as consent management.

Challenges of Adopting CIAM

The resulting distribution of the various challenges, met during the adoption of a CIAM solution by the respondents, is given in Fig. 11.

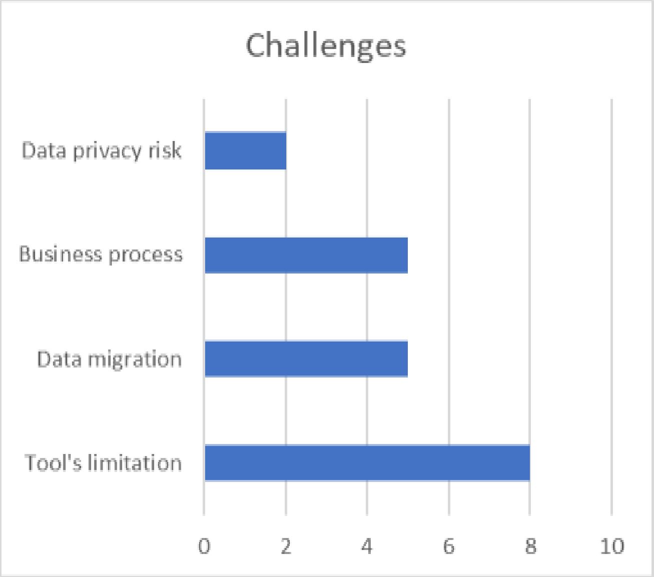

Fig. 11 Challenges of adopting CIAM solutions

Tool's limitation: Number one challenge, faced by 8 participants is the limitation of the CIAM tool itself. Each Company has its own processes and there is currently not one single tool in the market adequate to encompass all particularities. The result is that Companies are forced to implement several customisations on the solutions, increasing therefor the cost of implementation and maintenance and making it very difficult to upgrade. Building a CIAM solution, which can support the various home-grown applications is seen as a significant roadblocker. Moreover, most tools lack business analytics functionalities.

Data migration: 5 participants indicated that due to the big number of legacy systems, it is very difficult to have them all onboarded on their CIAM solution, as the Master Data are not always unified. Company 17 (Power Systems) very clearly stated “reclaiming identities from prior LDAP to the new solution is a nightmare and still not done”.

Business process: The external identities vary from technical to non- technical, from on-line to off-line, from vendors to customers to contractors etc. Establishing business processes to automatically identify the persona of the user and apply the right criteria for authenticating and authorising them to the company’s resources is a major challenge.

Data Privacy Risk: Ensuring a continuous and robust control of all personal data of all external identities, so that the Company complies with the General Data Protection Regulation (GDPR) or other similar requirements is challenging, due to the number and the frequency of change of the external identities. Obtaining and managing consent when handling customers' personal data is fraught with difficulties [18]. “Because of this, organizations are turning to artificial intelligence (AI) technology, such as machine learning (ML)… to increase access security, while preserving the integrity of user identities” [19].

Identities of IGA and CIAM

Our last question focused on the different identities managed by either IGA or CIAM, with the following feedback:

Table 1. Management of identities

Identities	Managed by IGA	Managed by CIAM
Worker types	17	1
Personas	11	13
Privileged IDs	16	
Non-human	13	4
Others		

All participants treat their employees and privileged IDs as internal identities and manage them through IGA. A big majority of the respondents treat the personas related to contractors and vendors also the same way and manage them through IGA.

The main persona identified for management through CIAM was, as expected, the customers. These are treated as external identities for all participants, who replied that they use a CIAM solution.

4. Conclusion

Our analysis of the responses collected provided the ground for the following main observations and call for further review:

- Most companies are content having a reliable IGA solution in terms of managing internal identities. There is a variety of processes covered as well as where the line is drawn between internal and external management of the solution. The most critical decision point remains the risk aversion, which reconfirms several other similar exercises already performed [20], [21], [22]. A further deep dive is required for evaluating the technical differences among the various IGA solutions.

- The expansion of the covered identities to the external ones has already started. Most companies are at least looking into different solutions to be used and personas to be covered. Covid-19 and the acceleration of online marketing channels has reconfirmed the need of secure, customer centric access provisioning [23], [24]. The relevant tools are not as mature as the ones for IGA. Technical limitations coupled with business specifics make the implementation of CIAM a challenge for most companies. A further analysis on the standard and customizable features of the solutions is needed.

Appendix I
Questionnaire

QUESTION: Do you currently leverage at least one central IGA solution as part of your overall IAM strategy?

_ Yes
_ No (If selected, you have completed the survey.)

1. What central IGA solution are you currently using? Please list the supplier and product name.

2. Your central IGA solution:

a. Which of the following main systems are used and integrated with your central IGA solution?

_ SAP ERP
_ Microsoft Azure Active Directory
_ Janrain
_ Auth0
_ ForgeRock
_ IBM Security Access Manager
_ Okta Customer Identity
_ Ping Identity
_ Salesforce
_ Other. Please specify:

b. What percentage of systems are currently operating with your primary IGA tool in the organization today?

_ <30%
_ Between 30%-50%
_ Between 51%-80%
_ >80%

3. Identity management operating model:

a. Briefly, please describe the management model of your IAM solution(s) (i.e., is your solution on-premises or SaaS-based? Is it managed internally or being outsourced? Etc.)

b. If applicable, what is the breakdown of the IAM solutions that are managed internally and being outsourced?

_% managed internally
_% outsourced

c. If your IAM solutions are outsourced, what (if any) benefits are you experiencing?

d. More specifically, what IAM sub-processes have you outsourced and insourced?

4. How many resources does your IAM team have in each of the following categories?

_ # of internal resources
_ # of contractors

5. For systems where access is managed manually (i.e., directly in the system by the user administrator, rather than by the IAM system), there may be a greater risk of error (e.g., excessive access, continued access for employees no longer with the organization, etc.). To what extent has this been a challenge in your organization?

_ Major challenge
_ Minor challenge
_ Not a challenge

How (if at all) have you changed your IAM program to adapt to zero trust principles? Please briefly describe any short-term and long-term initiatives you have planned.

6. Customer identity and access management (CIAM):

a. Have you added any customer identity and access management (CIAM) solutions to your current IAM infrastructure to support external identities?

_ Yes
_ No (If selected, please skip to Question 10.)

b. What CIAM solution are you using? Please list the supplier and product name.

c. What were your primary business drivers for adopting a CIAM solution? Please select (or identify) the top 3 drivers.

_ Unify user experience
_ Drive digital initiatives
_ 360-degree view of customer
_ Streamline operations
_ Replace homegrown systems
_ Other(s). Please specify:

7. What have been the key benefits and challenges you have encountered since adopting your CIAM solution?

a. Benefits:
b. Challenges:

8. Managing internal and external identities:

a. What types of user groups are considered internal identities and are therefore managed by your central IGA solution? And conversely, what types of user groups are considered external identities and are therefore managed by your CIAM solution? Please briefly explain.

b. Which of the following identities are being managed by your central IGA tool and your CIAM tool? Please mark an X in the appropriate column.

Identities	Managed by IGA	Managed by CIAM
Worker types	17	1
Personas	11	13
Privileged IDs	16	
Non-human	13	4
Others		

Appendix II

Participants

(coded for GDPR purposes – data available by the author)

Company	**Industry**	**Emplo-yees***	**Reve-nue $bn***
Company 1	Food & Drinks	28,000	8.3
Company 2	Pharma	110,000	48.7
Company 3	HealthCare	n/a	n/a
Company 4	Hardware	28,000	16.5
Company 5	Bank	90,000	33.7
Company 6	Luxury Items	9,200	3.3
Company 7	Automotive	4,300	17.7
Company 8	HealthCare	7,500	80.4
Company 9	HR Services	58,000	14.6
Company 10	Winery	4,400	4.8
Company 11	Financial Services	n/a	n/a
Company 12	Cosmetics	33,400	1.4

Company 13	Petroleum	105,500	140.7
Company 14	Insurance	17,000	41.9
Company 15	HealthCare	300,000	268.7
Company 16	Wholesale	41,000	179.6
Company 17	Power Systems	60,000	19.8
Company 18	Pharma	27,000	7.9
Company 19	Food & Drinks	134,000	16.6
Company 20	HealthCare	49,600	29.4
Company 21	Tobacco	46,000	19.0
Company 22	Energy	14,300	100.0
Company 23	Animal Health	11,300	6.3
Company 24	Tobacco	n/a	n/a

*Latest publicly available data

References

[1] B. Ballad, T. Ballad, T., and E. Banks, “Access control, authentication, and public key infrastructure,” Jones & Bartlett Publishers, 2010.

[2] A. Puchta, F. Böhm, and G. Pernul, “Contributing to current challenges in identity and access management with visual analytics,” In IFIP Annual Conference on Data and Applications Security and Privacy, Springer, Cham, July 2019, pp. 221-239.

[3] E. Osmanoglu, “Identity and Access Management: Business Performance Through Connected Intelligence,” Newnes, 2013.

[4] J. Shaw “Top Five Challenges of Building an Identity Governance Strategy,” Infosecurity Magazin, 2021.

[5] F5 Networks, “The Challenges and Benefits of Identity and Access Management,” F5.com, 2016

[6] I. Indu, P. R. Anand, and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” Engineering science and technology, an international journal, vol. 21, no. 4, 2018, pp. 574-588.

[7] CIAM Technical Working Group, “The Unique Challenges of Customer and Identity Access Management,” Identity Defined Security Alliance, 2020, https://www.idsalliance.org/blog/2020/11/02/the-unique-challenges-of-customer-identity-and-access-management/

[8] Identity Management Institute, “Facing Customer Identity Challenges”, 2019, https://identitymanagementinstitute.org/facing-customer-identity-challenges/

[9] I. A. Mohammed, “Factors affecting user adoption of identity management systems: an empirical study,” International Journal of Innovations in Engineering Research and Technology, Vol. 8, No. 1, 2021, pp. 104-110.

[10] J. Friedman, “The Ultimate Guide to Identity Management,” CyberEdge Group, LCC, 2018.

[11] D. Blum, “Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment,” Springer, Nature, 2020, p. 333.

[12] D. Blum, “Control Access with Minimal Drag on the Business,” In Rational Cybersecurity for Business, Apress, Berkeley, CA, 2020, pp. 227-257.

[13] A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, “A comparative analysis of trust requirements in decentralized identity management,” In International Conference on Advanced Information Networking and Applications, Springer, Cham, March 2019, pp. 200-213.

[14] K. Raina, “Zero Trust Security,” 2021, https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

[15] Hub City Media, 2021, https://www.hubcitymedia.com/blog/solving-common-iga-challenges

[16] C. Basumalik, “Top 10 Customer Identity Management Solutions in 2021,” Toolbox, 2021, https://www.toolbox.com/tags/ciam/

[17] EMA, “Consumer Identity and Access Management (CIAM): Responsible Solutions for Creating Positive Consumer Experiences,” 2021, https://docs.broadcom.com/doc/ema-ciam-report

[18] D. Maxey, “The challenge of privacy and consent enforcement in large-scale enterprise application programmes,” Computer Fraud & Security, vol. 9, 2020, pp. 6-9.

[19] I. Azhar, “A significance of Identity Management as a Prerequisite for Enterprise AI on the Cloud,” International Journal of Creative Research Thoughts (IJCRT), 2021, ISSN, 2320-2882.

[20] I. Indu, P. R. Anand, and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” Engineering science and technology, an international journal, vol. 21, no. 4, 2018, pp. 574-588.

[21] I. P. Popescu, C. A. Barbu, M. E. Popescu, “Identity and access management - a risk-based approach,” In Proceedings of the 9th International Management Conference, November 2015.

[22] A. Partida, R. Criado, and M. Romance, “Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms,” Electronics, vol. 10, no. 4, 2021, p. 378.

[23] A. Sharma, S. Sharma, and M. Dave, “Identity and access management - a comprehensive study,” In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE, October 2015, pp. 1481-1485.

[24] H. Rasouli and C. Valmohammadi, “Proposing a conceptual framework for customer identity and access management: A qualitative approach,” Global Knowledge, Memory and Communication, 2019.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

Anastasios Liveretos prepared the questionnaire, processed the results from it and made conclusions.
Ivo Draganov made survey on the topic of the study.