



**DIACC**  **CCIAN**

**2022 Industry Survey Report**

The intent of the DIACC Industry Survey was to identify any pain points Canadian industries have that prevent the use of trusted Digital Identity. This survey was created in the Summer of 2021 with the support and input of the DIACC's Outreach Expert Committee.

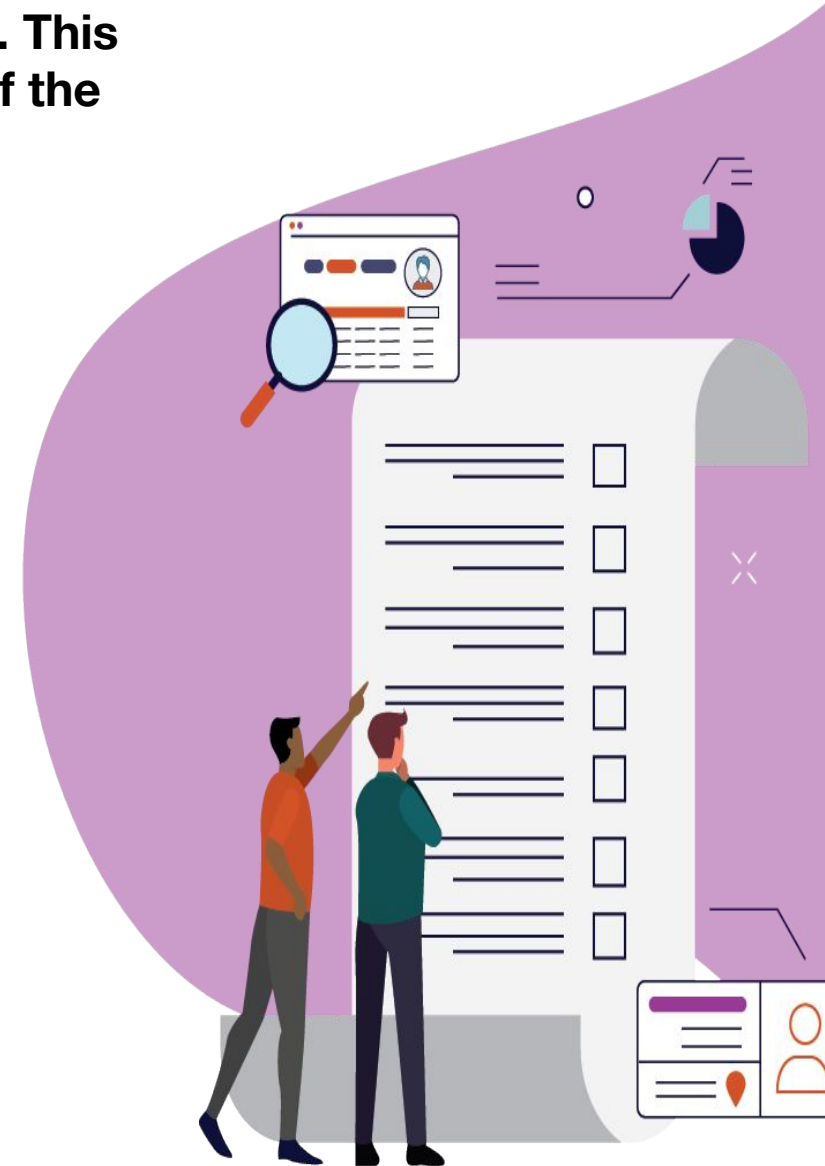
Responses were received from representatives in Federal, Provincial, Municipal, and international jurisdictions and across various industries.

Insights gained include...

**60%** of respondents agreed there are barriers or blockers that would prevent their clients, end-users, members, and/or customers from using Digital ID instead of physical ID.

**54%** of respondents agreed that ongoing transaction costs or minimum usage fees to offer and accept Digital ID to be a barrier for their organizations.

**31%** of respondents strongly agree that Digital ID would increase accessibility and inclusion for their users.



# Progress on Digital ID



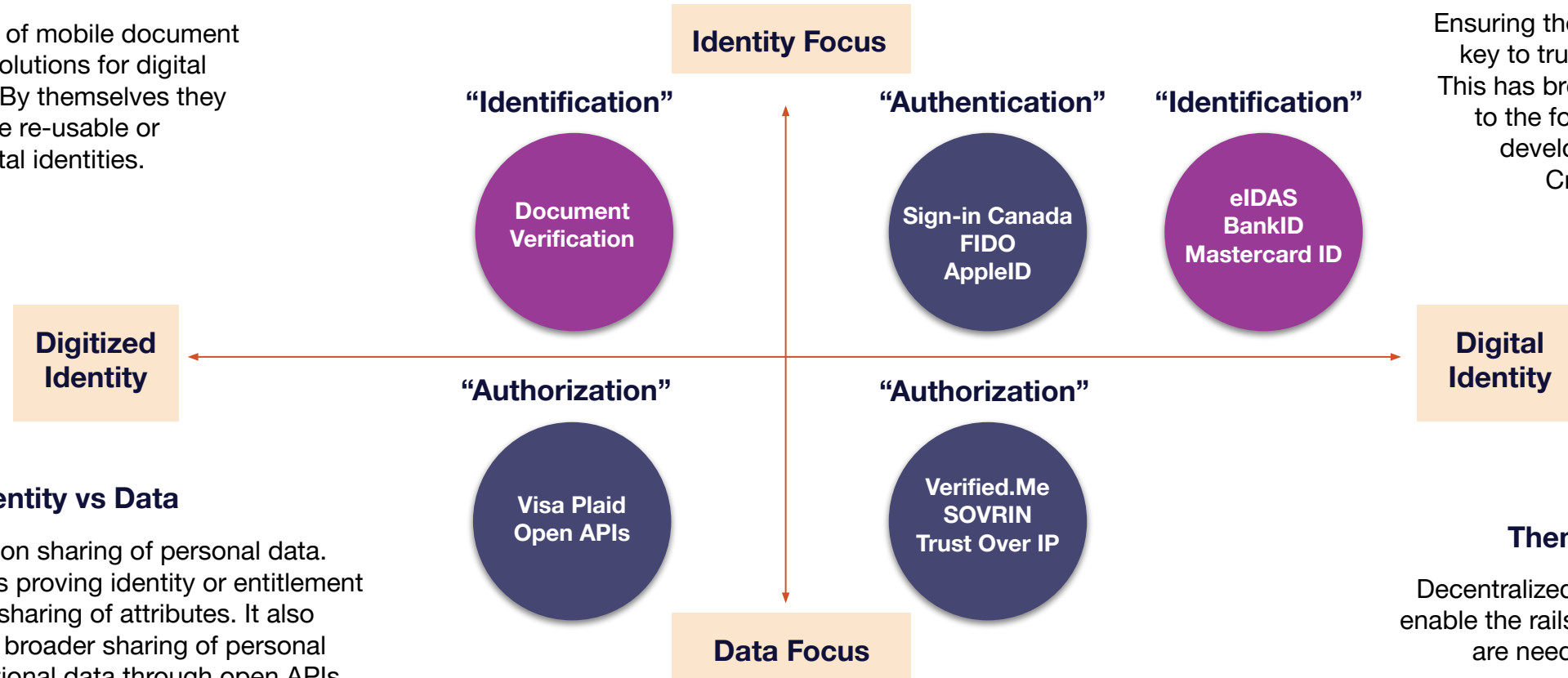
# What does digital identity look like today?

## Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

## Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.



## Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

## Theme: Governance

Decentralized identity standards enable the rails. Trust frameworks are needed to set the rules.

# Key Challenges & Opportunities

## Creating Market Conditions



### Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.



### Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

## Promoting Market Growth



### Sustainability

While each scenario provides a varying perspective, commercial sustainability and viability are either unclear, underdeveloped, or unproven. Considerations for liability should also be included in this category of challenges as the responsibility around personal data exchanged needs to be carefully examined.



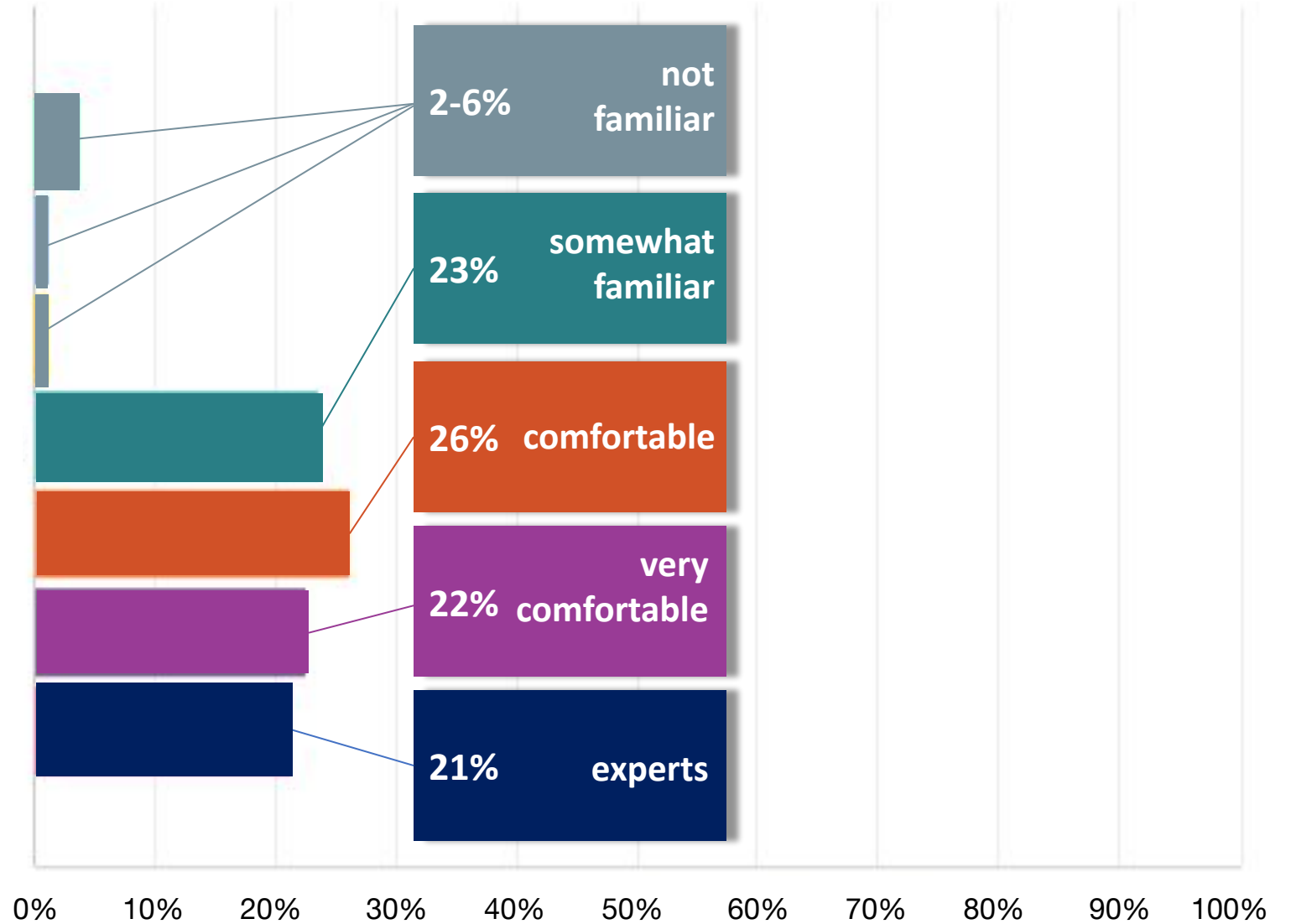
### Inclusion

Ensuring that a critical mass of providers and users adopt digital identity products is significant across all scenarios, while also ensuring those that are typically excluded can get access to services or can be provided with better experiences than those that exist today.

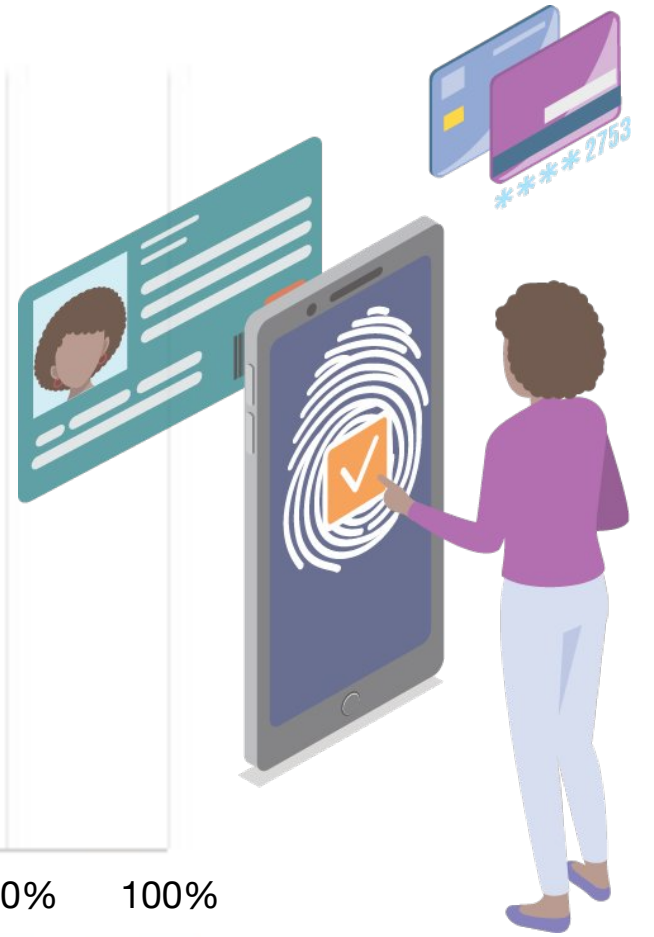
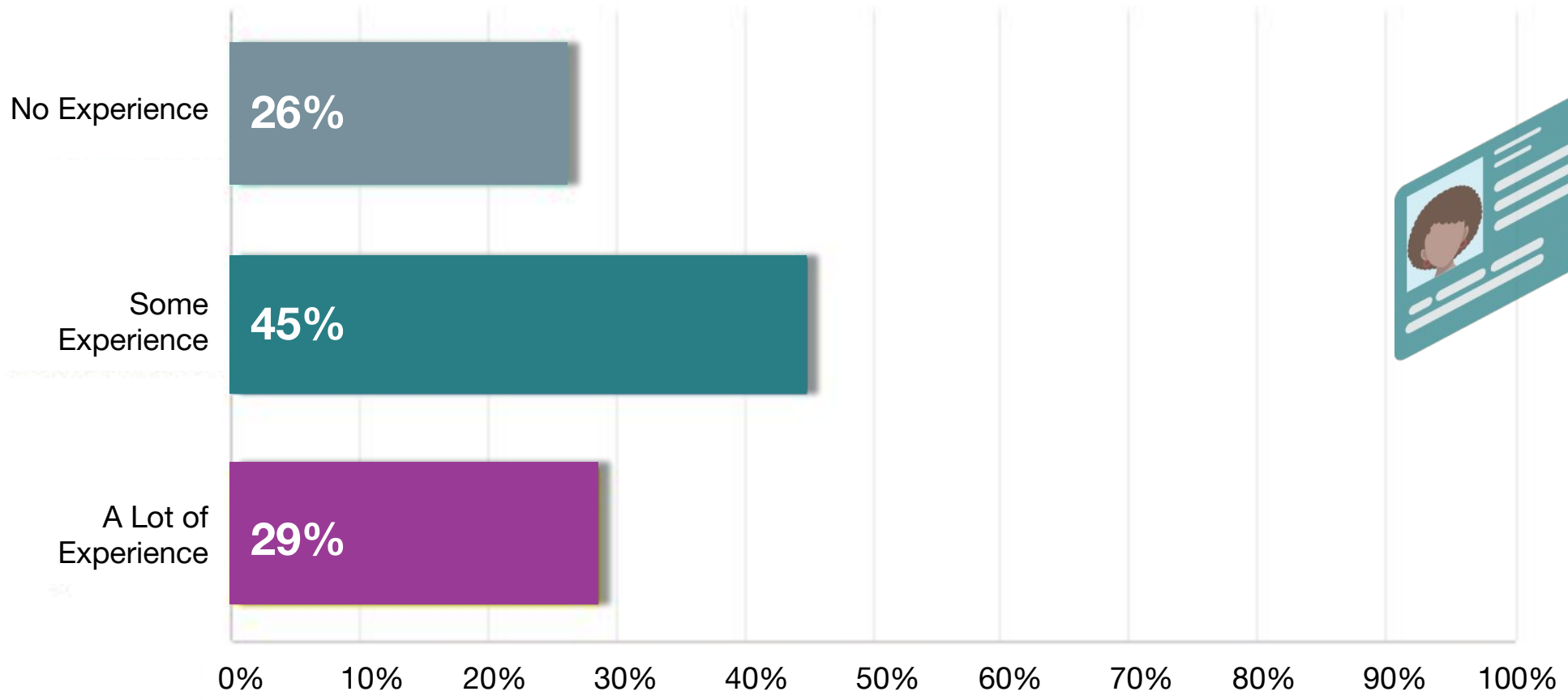
# Examples of Barriers and how we can help



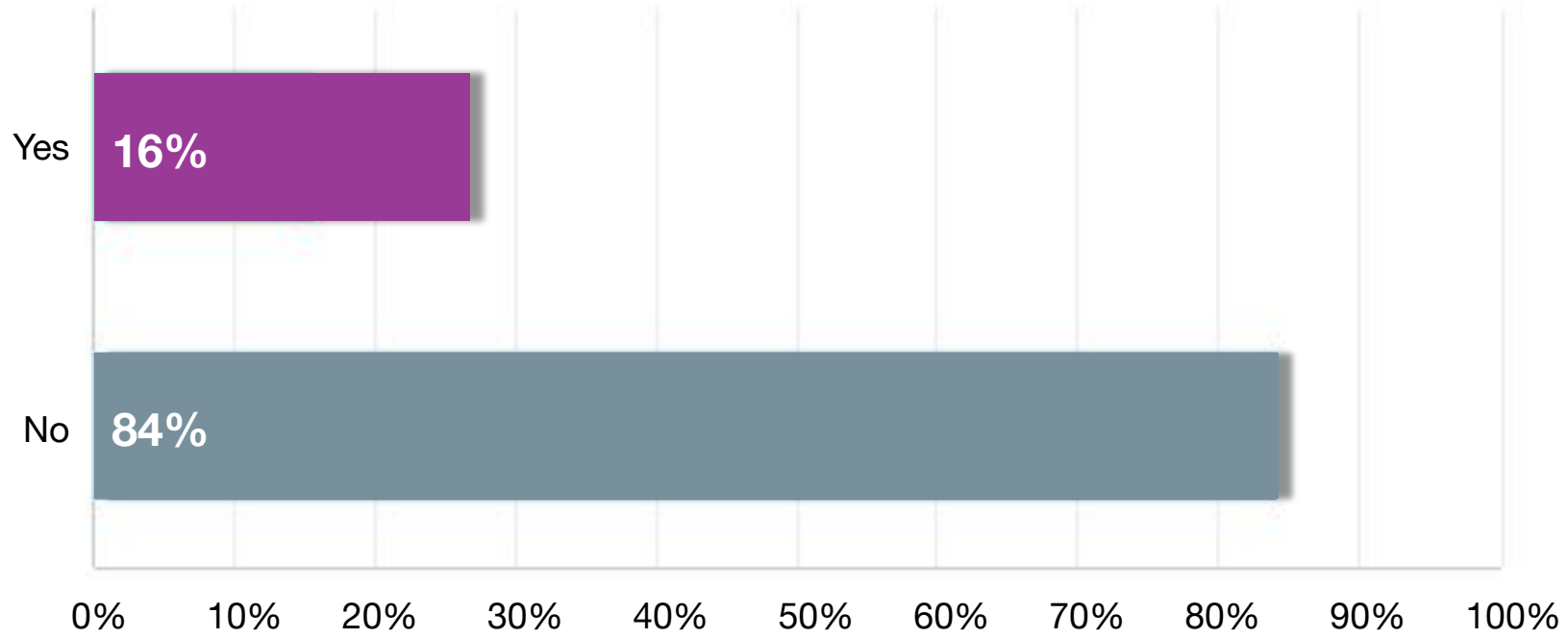
# How comfortable are you with the concepts of Digital ID and what it can be used for?



# Do you have experience using Digital ID as an end user?



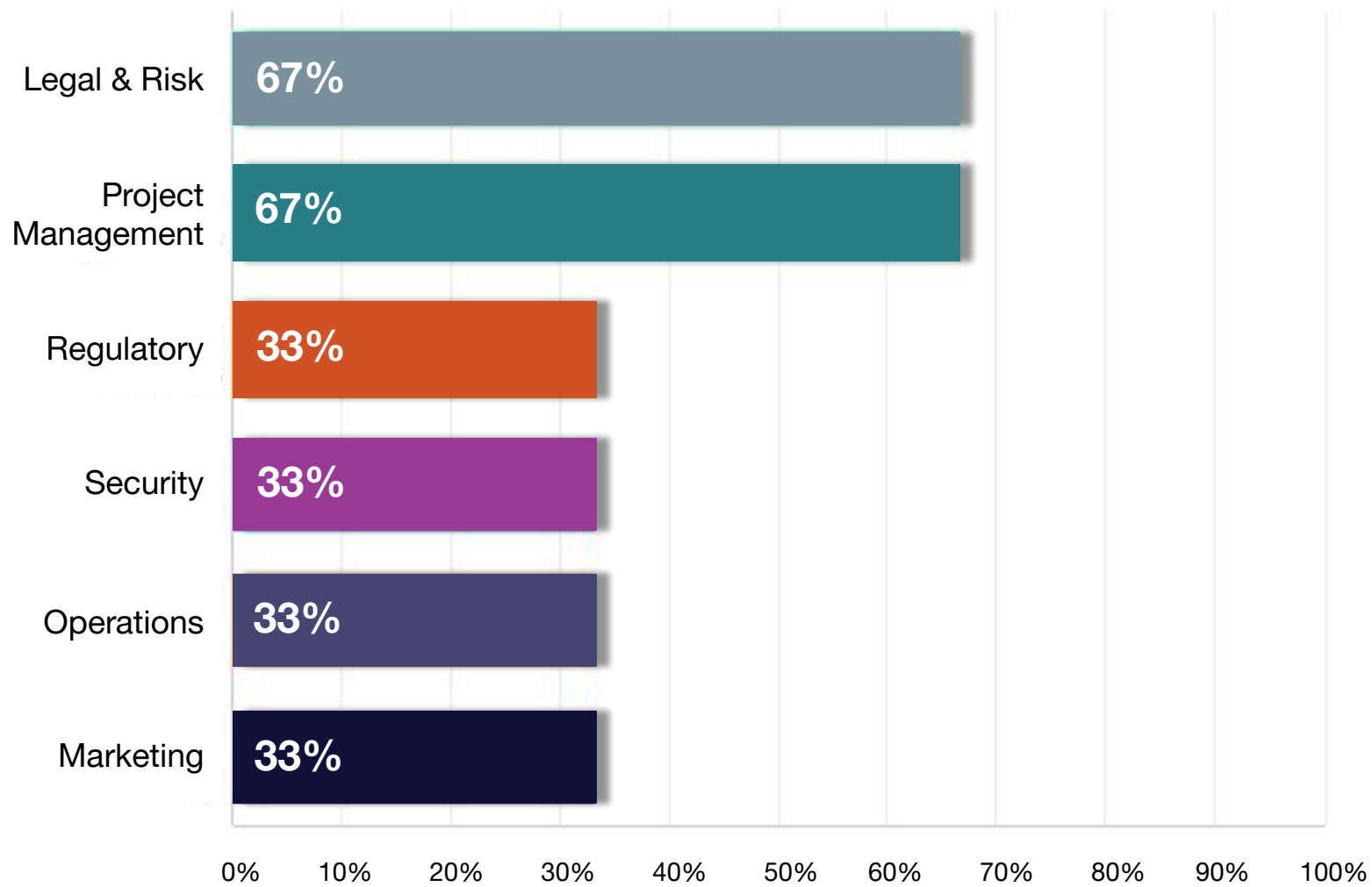




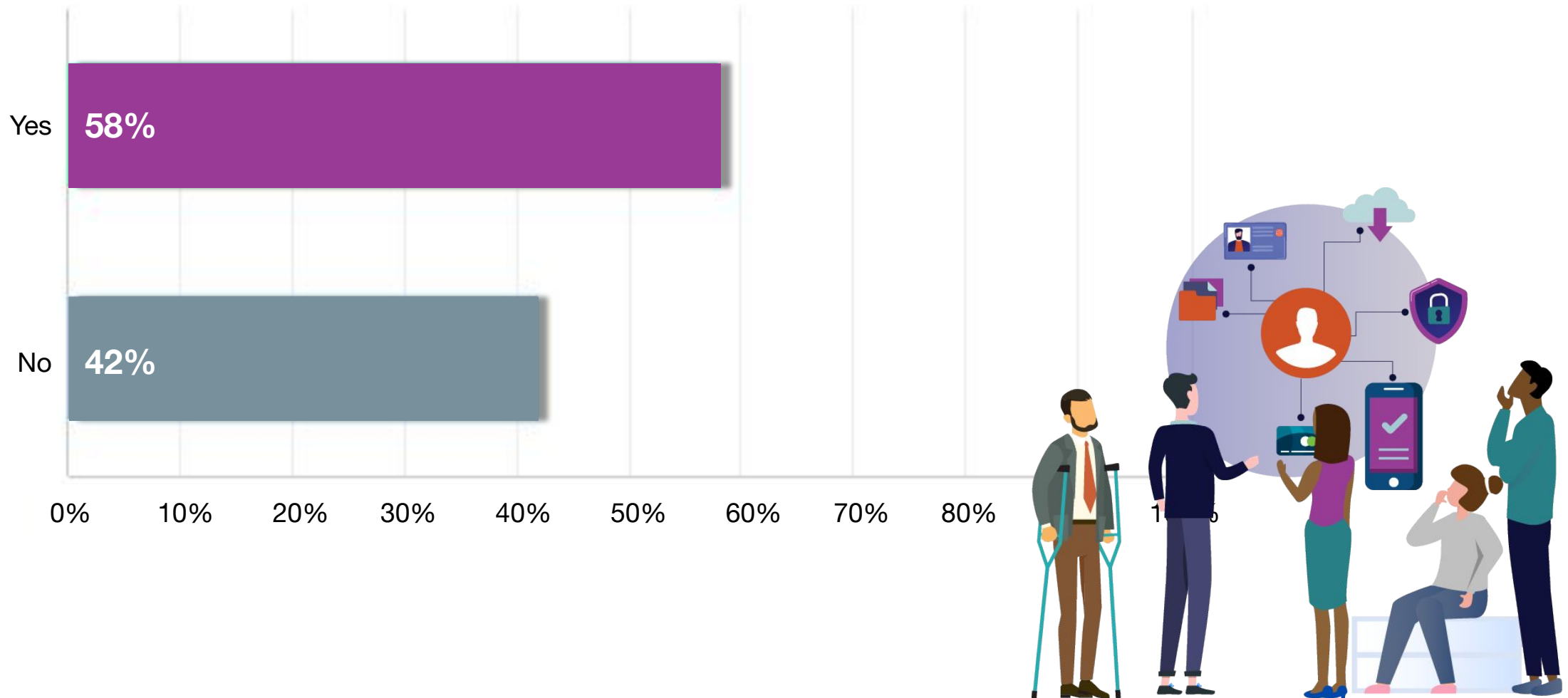
**Do you have experience using or implementing Digital ID at your organization?**



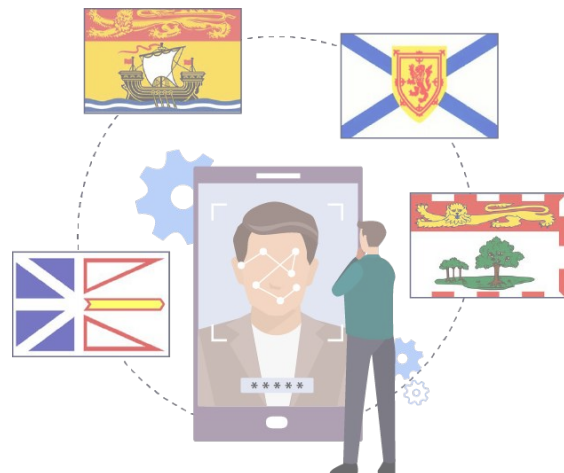
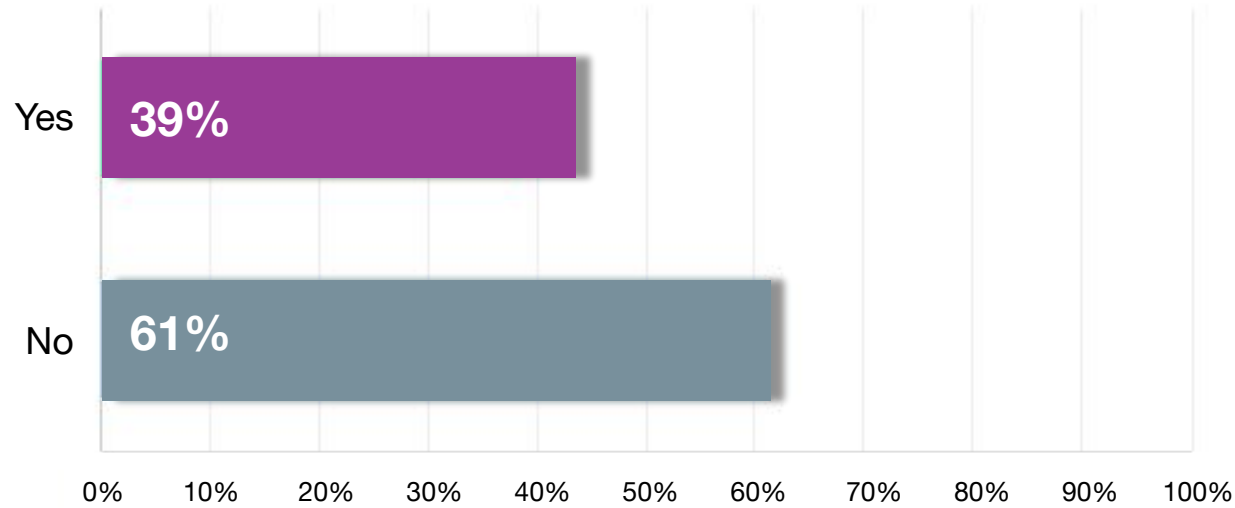
# What's your current level of involvement with the use of Digital ID?



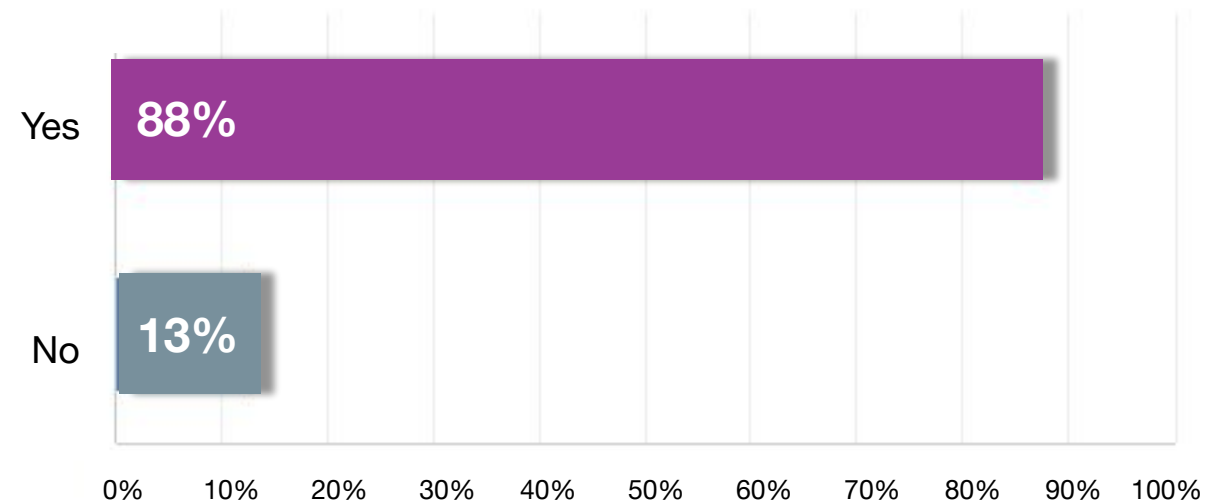
# Would you be willing to use Digital ID to access various services if done in a secure, privacy respecting way?



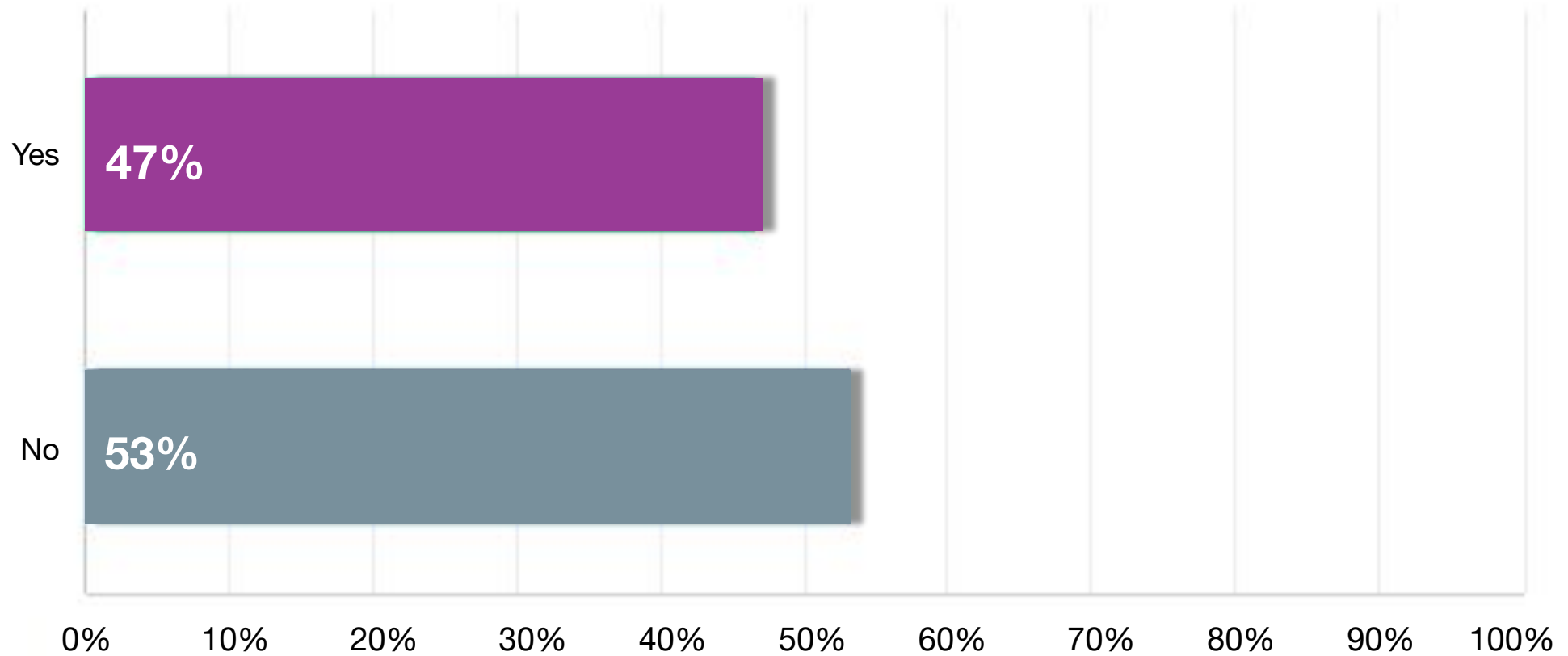
# Is Digital ID currently being used in your province, country, or state?



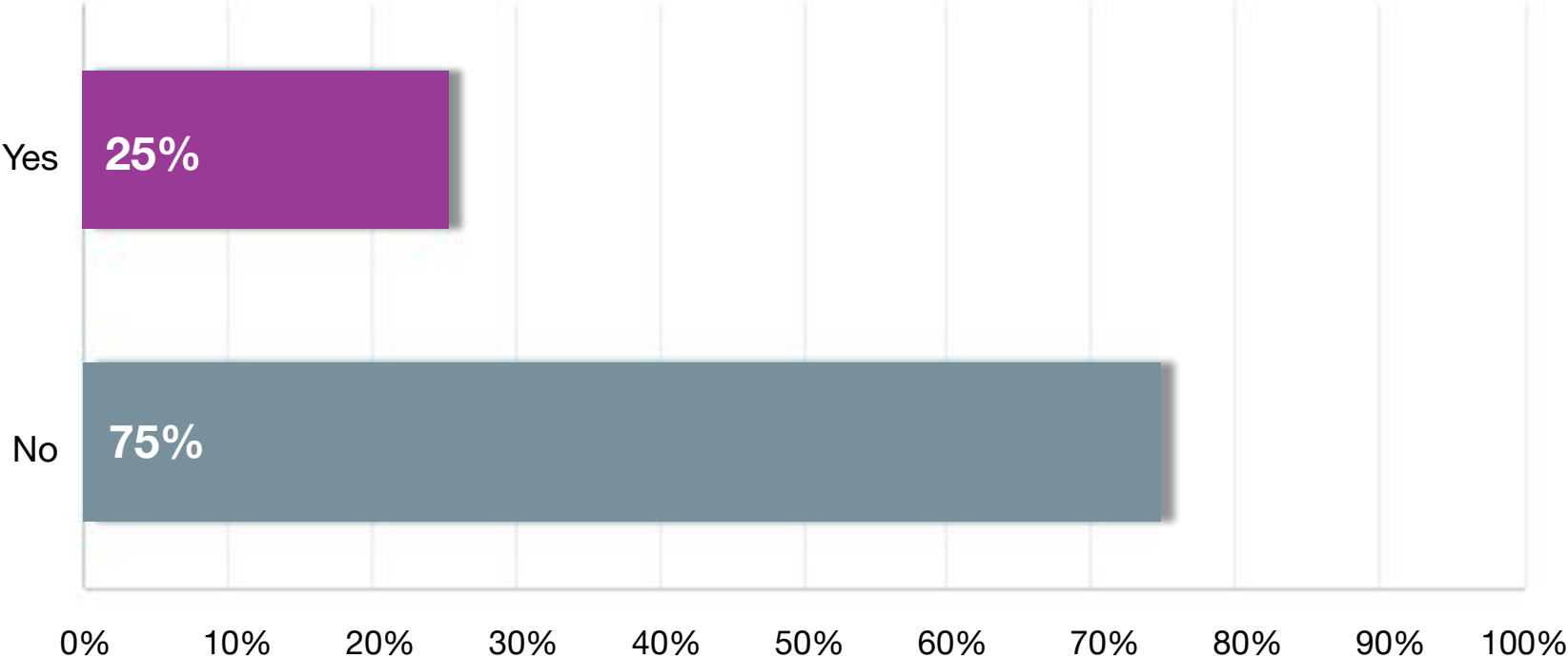
# Is this Digital ID being offered by a government?

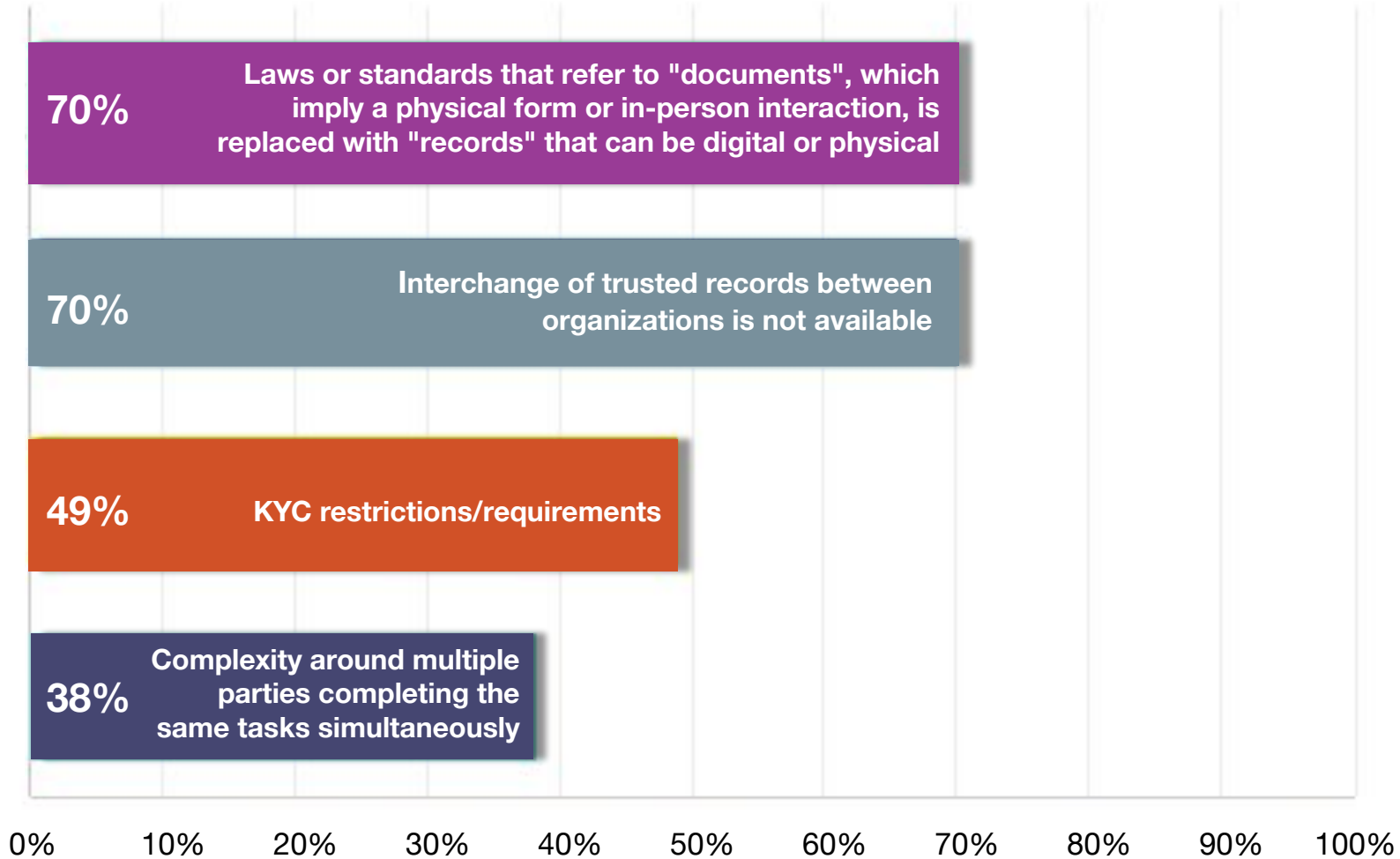


# Does your government have a Digital ID system in place that you do or do not use?



# Do any laws, business practices, codes of conduct, or rules of your sector prohibit you from offering or accepting Digital ID?





**What changes are needed to facilitate Digital ID for your organization or sector to provide products and services?**

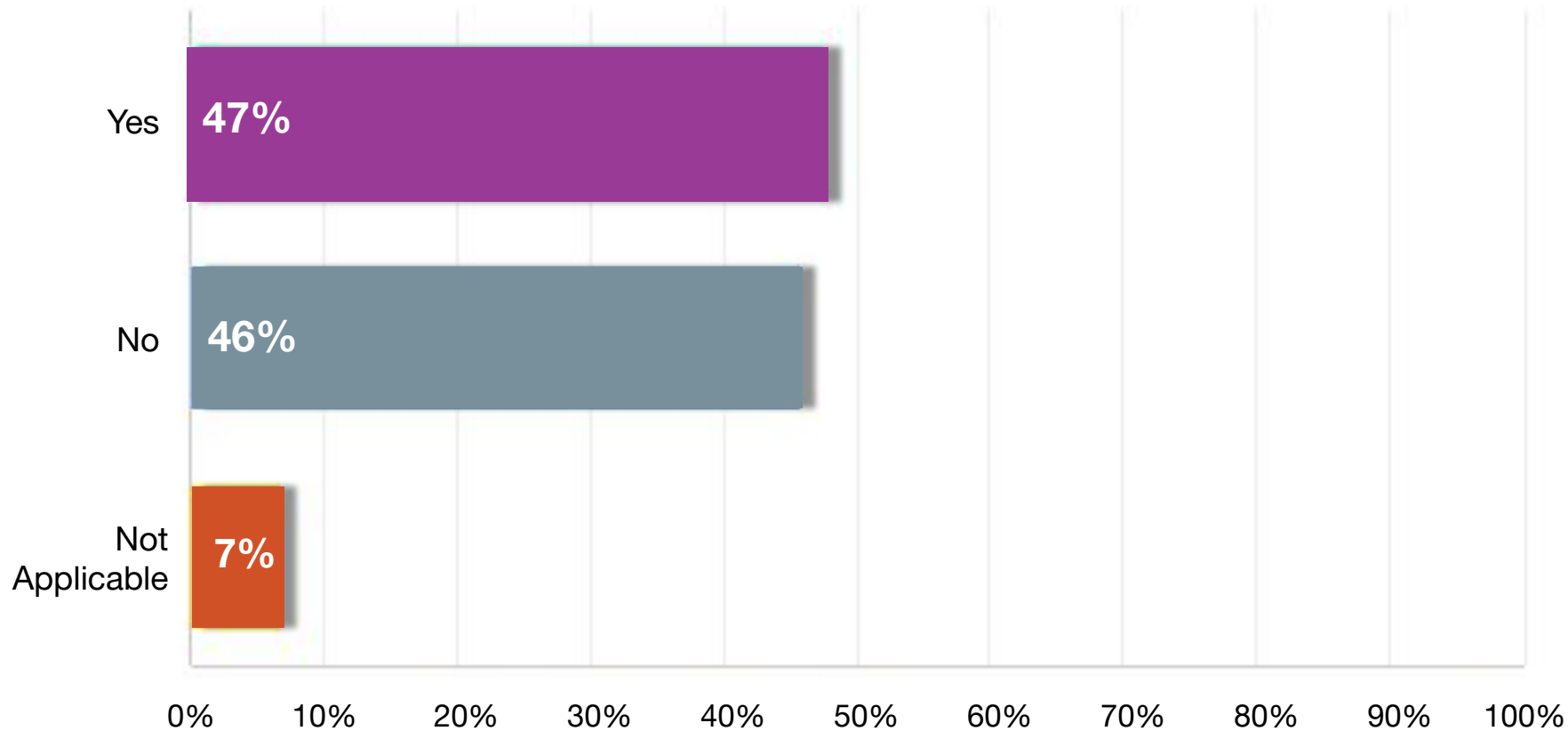


# Are aware of any Digital ID regulations or rules that are beneficial for your sector?

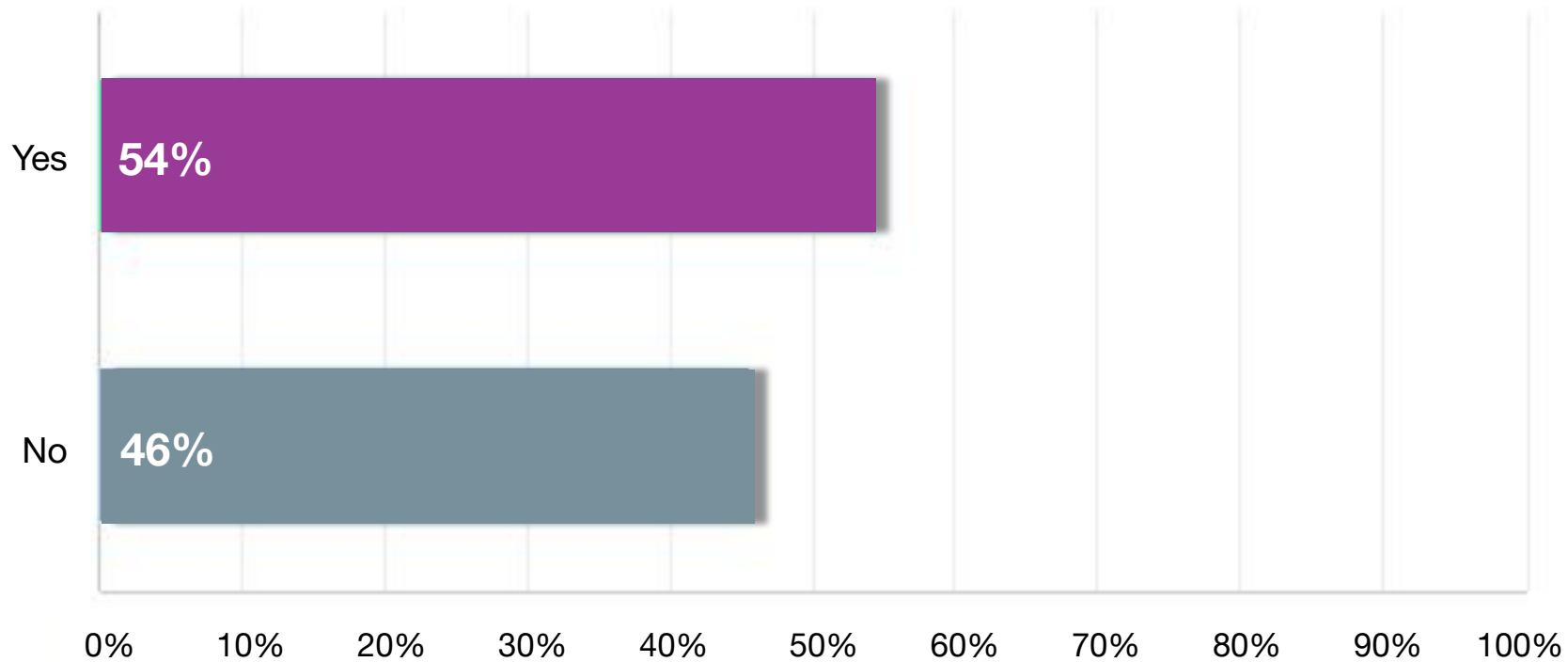




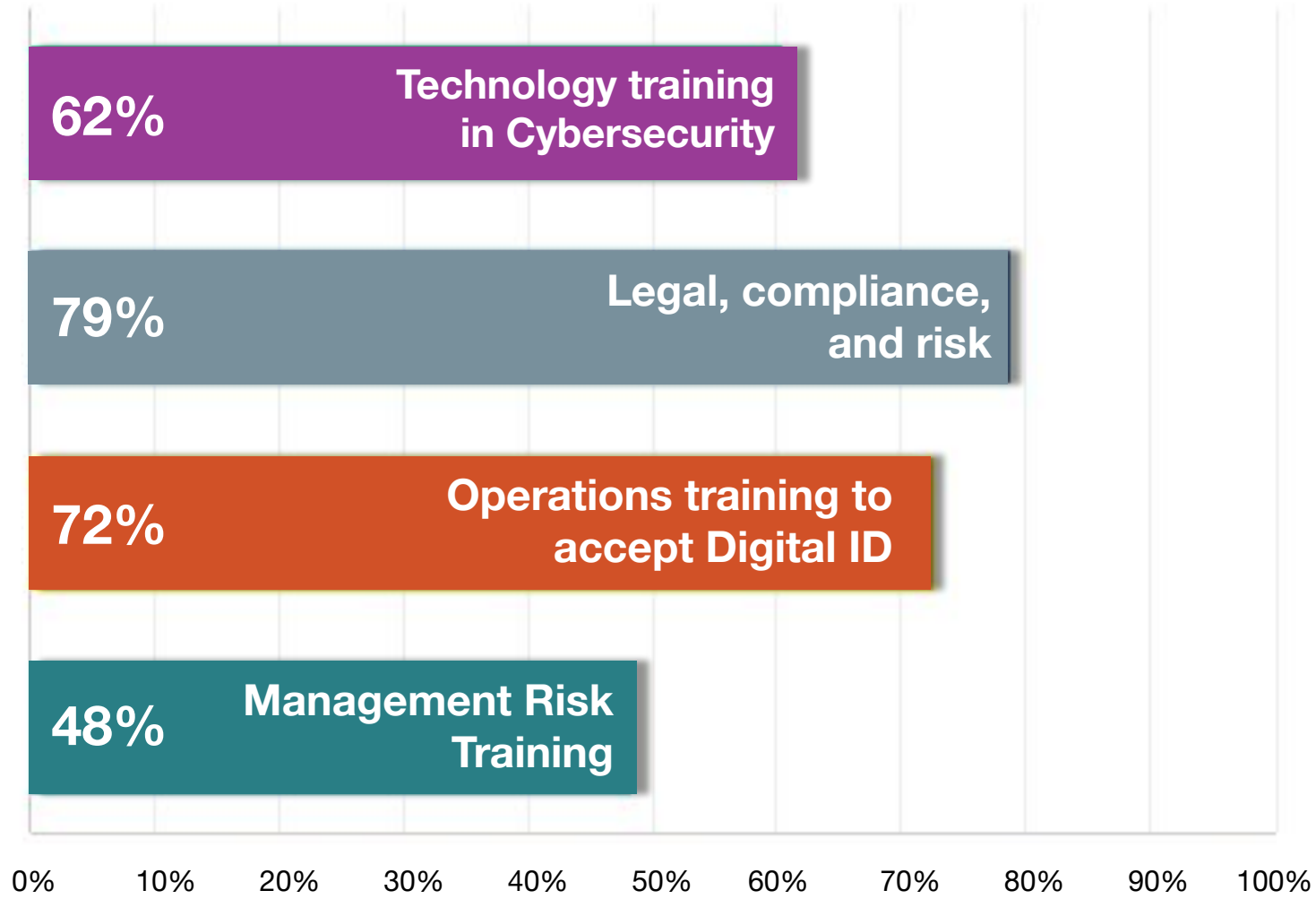
## Do you foresee the set-up cost for Digital ID to be a barrier for your organization or sector?



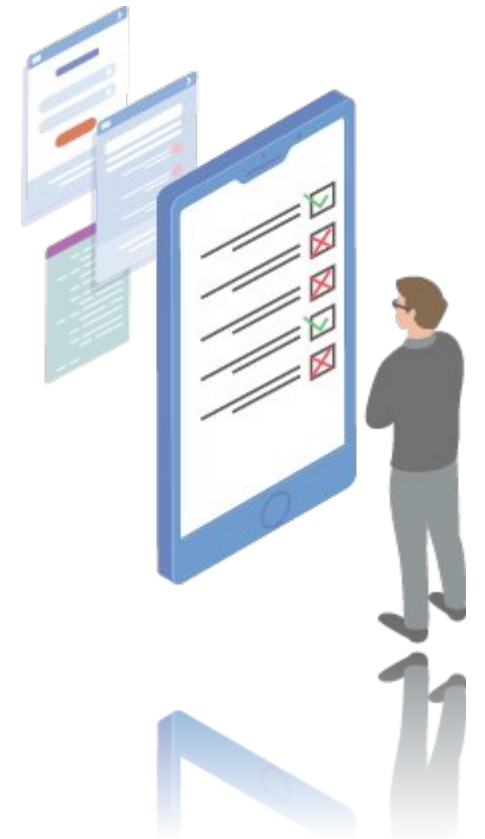
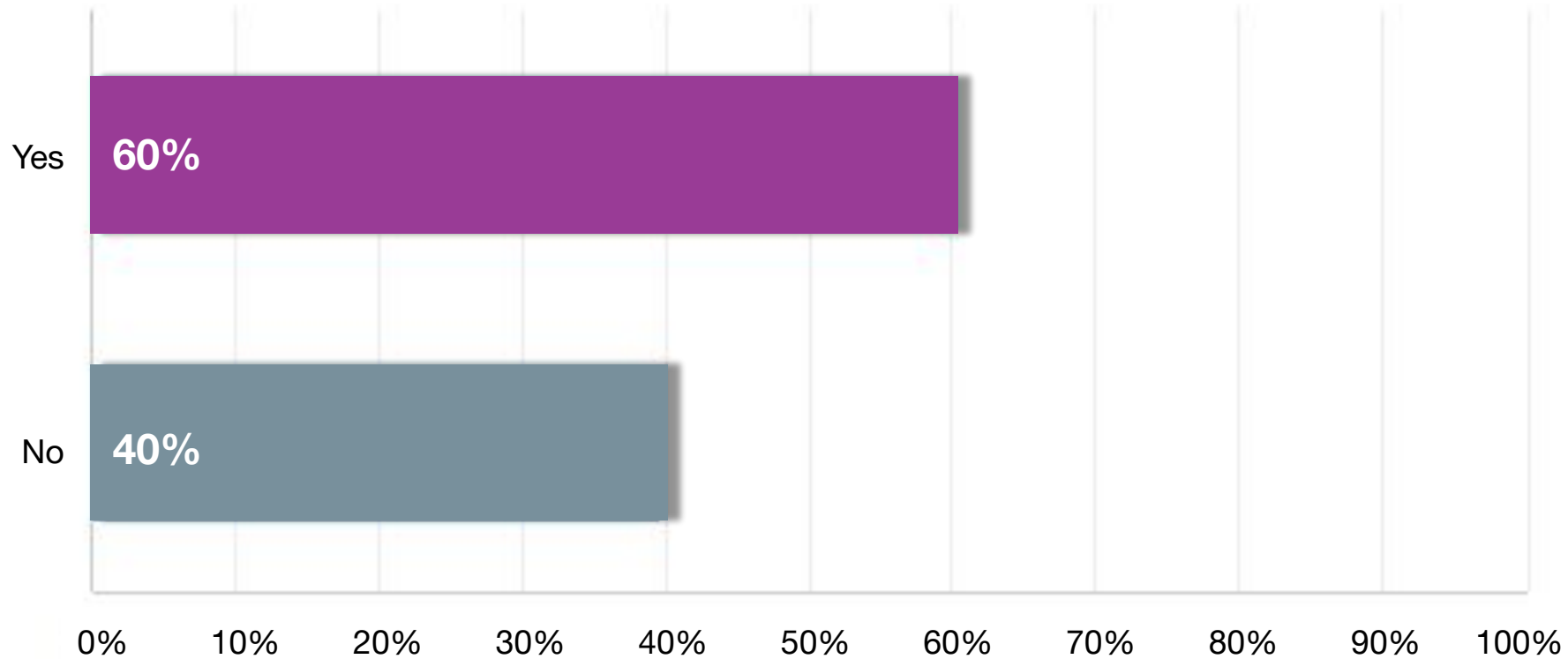
# Do you find the ongoing transaction cost or minimum usage fees to offer and accept Digital ID to be a barrier for your organization?



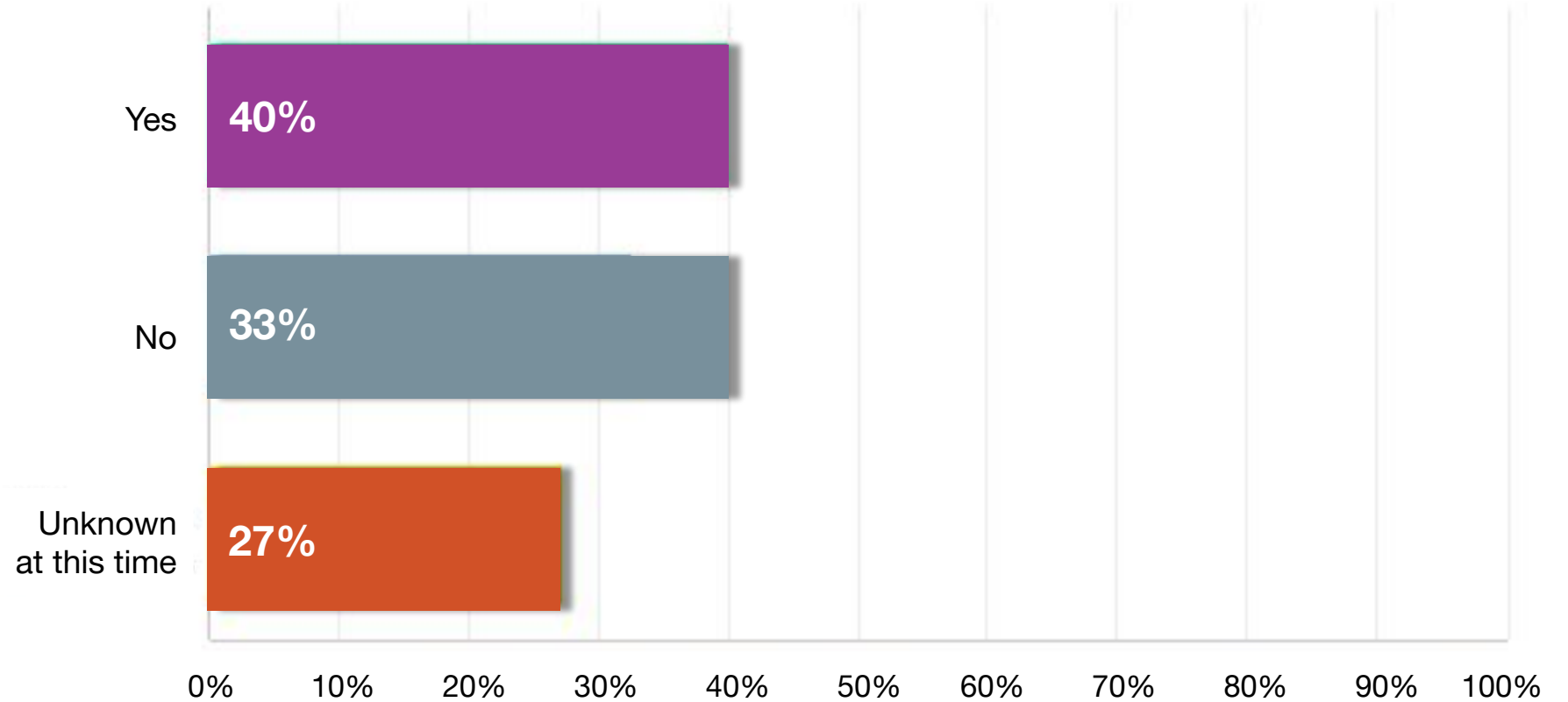
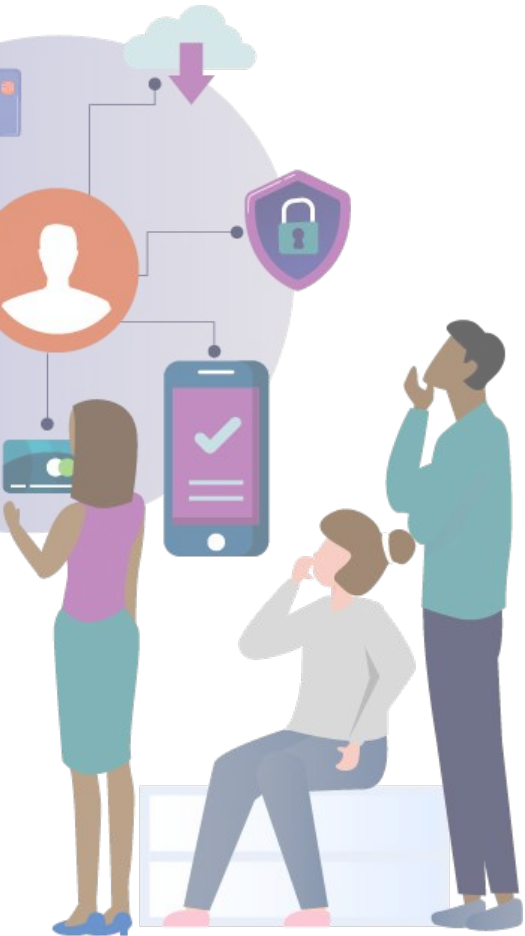
# Does your industry have certain contextual situations or regulatory requirements that require the usage of physical ID that couldn't be replaced by Digital ID?

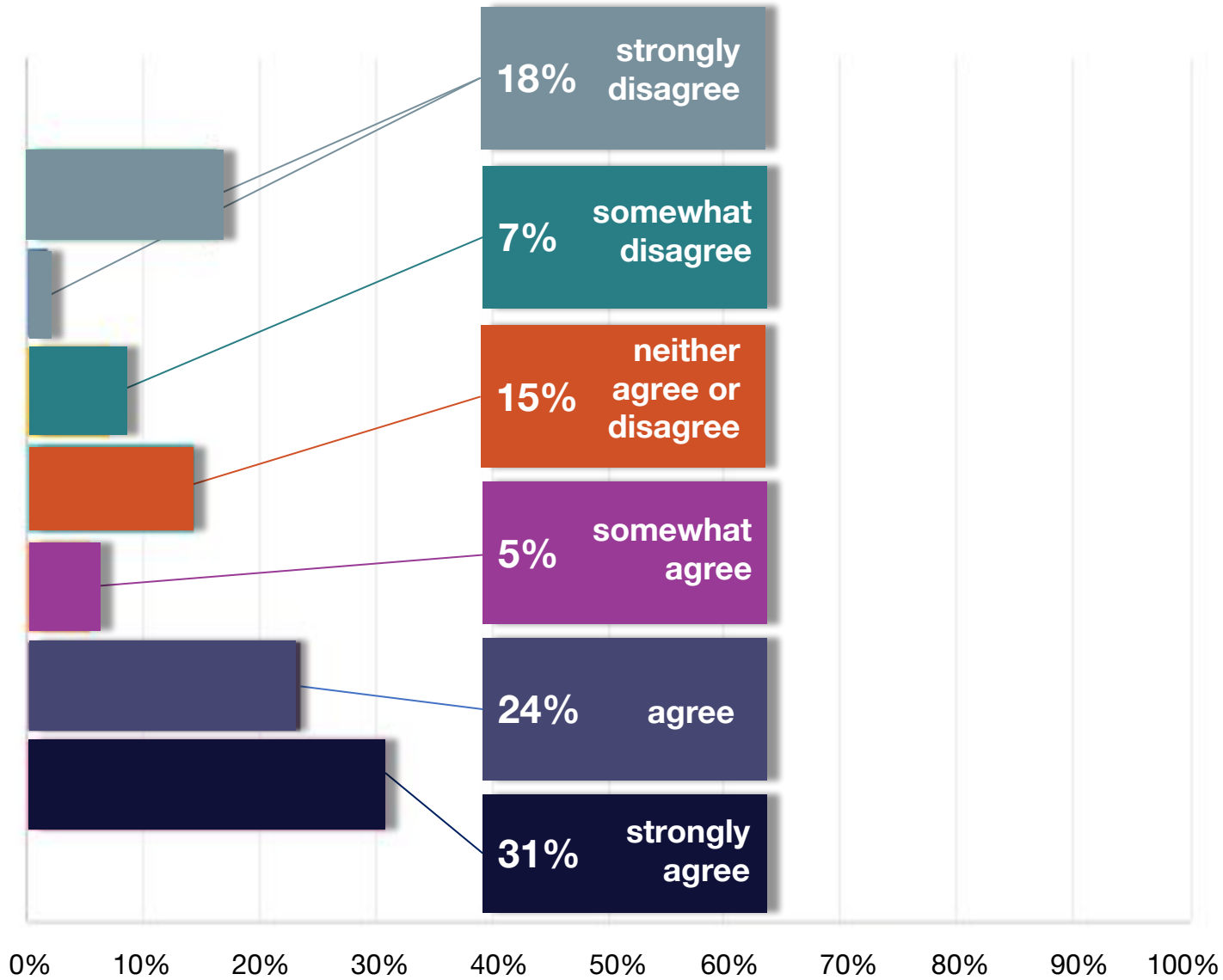


# Do you see any barriers or blockers that would prevent your clients, end-users, members, and/or customers from using Digital ID instead of physical ID?



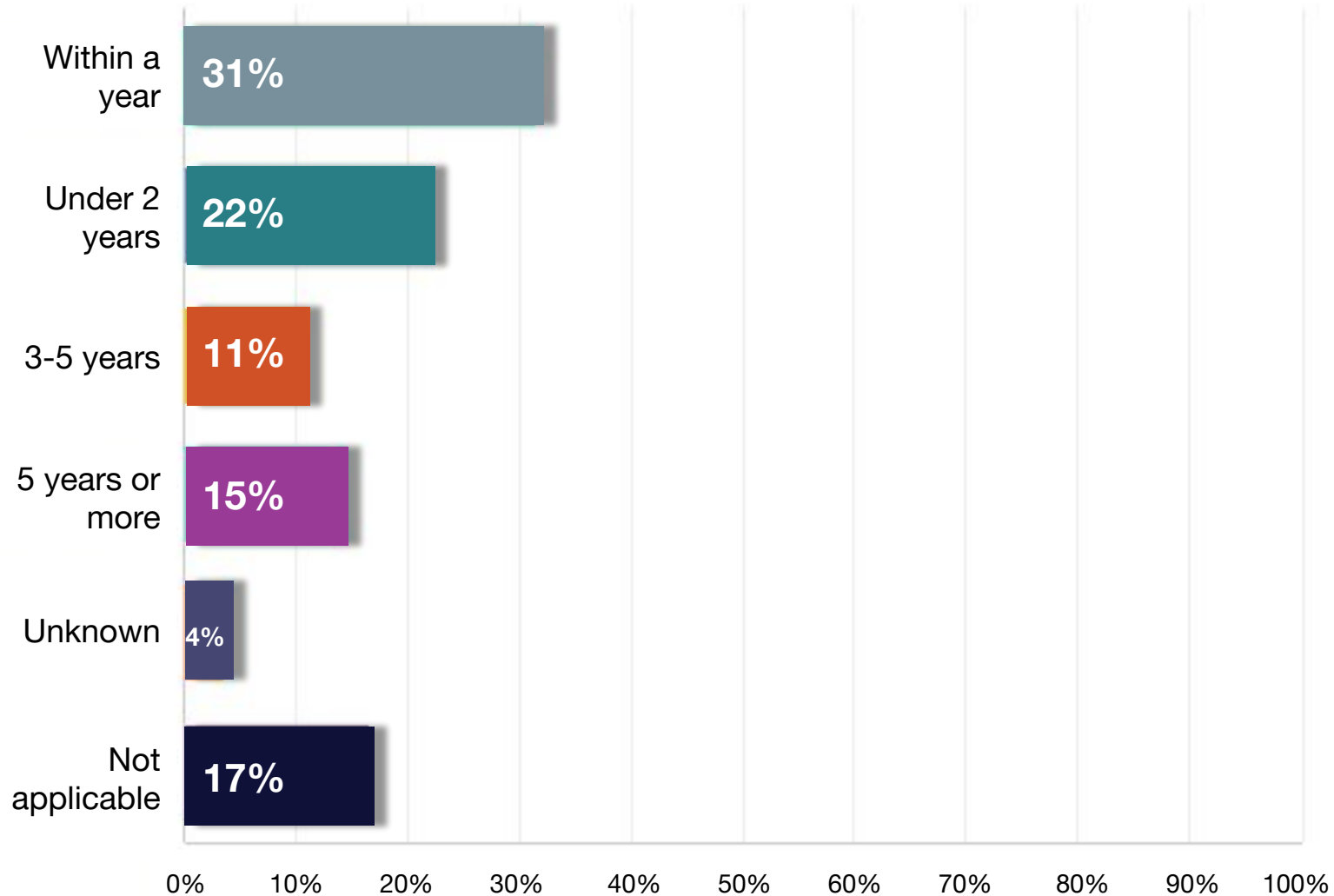
# Would having a Digital ID as the primary provider of authentication in your industry be discriminatory to your users from an inclusion standpoint?





**Do you see Digital ID increasing accessibility and inclusion for your users?**






**When do you feel your organization or industry would be ready to overcome any barriers to implement Digital ID solutions?**

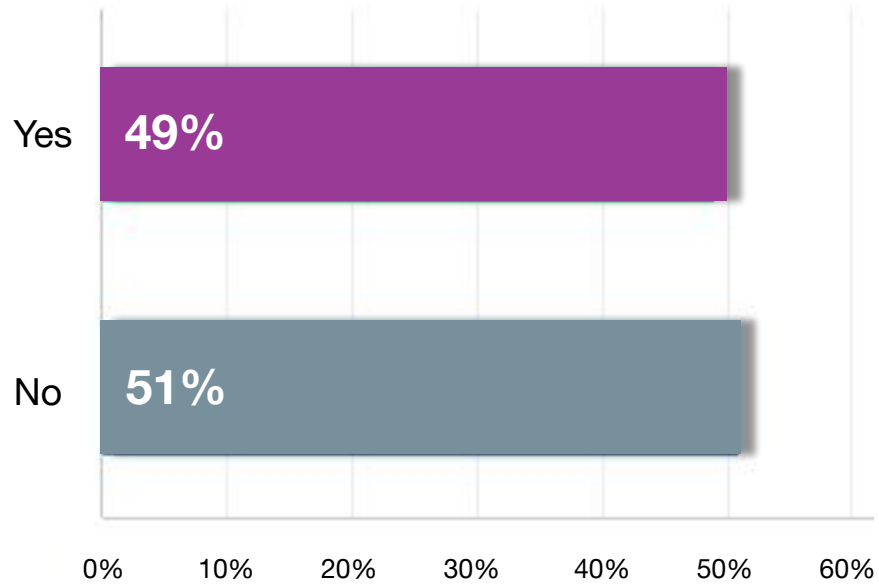


# What sort of training within your organization do you feel is needed to accomplish this new digital service and adoption of Digital ID?

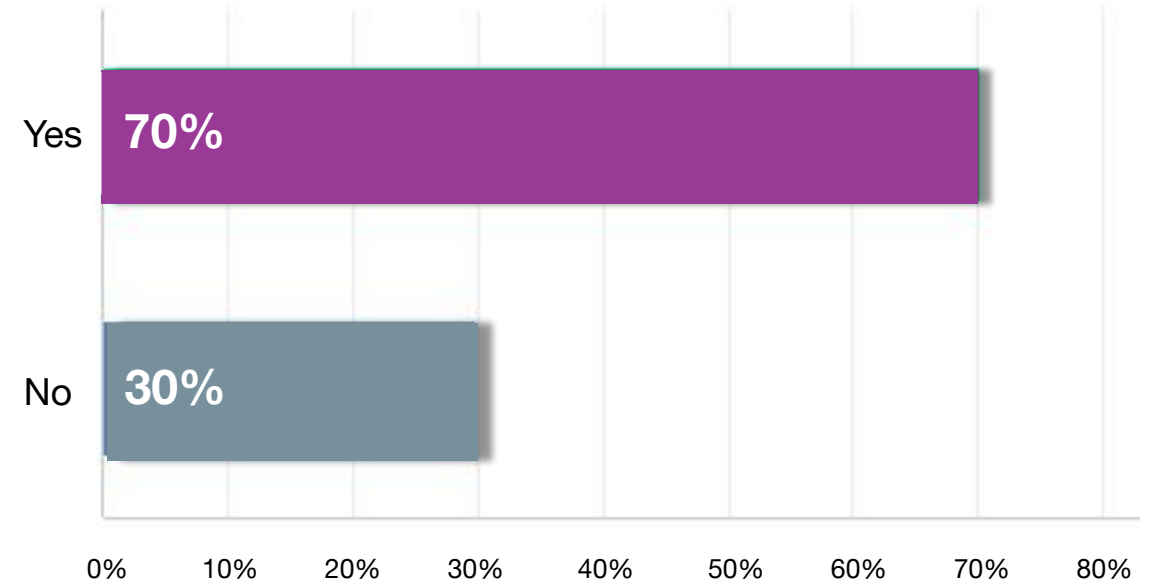
<i>PEOPLE</i>	<i>PROCESS</i>	<i>SYSTEMS</i>
<ul style="list-style-type: none"> <li>• HR, Security and Identity teams should learn more about Digital ID and how it can bring value</li> <li>• Top down and bottom-up training on the benefits, security, costs and ease of use of digital ID</li> <li>• Pacify people's fears of abuse of their Digital ID by rogue elements around the world</li> <li>• Training and opportunities need to be provided to senior leadership, so they are comfortable leading the process</li> <li>• General awareness training of the public is required to enable digital ID to be adopted. With improved knowledge will come use and accelerated rollout</li> <li>• Educate municipal decision-makers on the importance of digital transformation and the resulting efficiencies</li> <li>• Standard cybersecurity training</li> </ul>	<ul style="list-style-type: none"> <li>• DIACC's trust framework would be key to providing some level of comfort that digital identification technology/companies met a minimum level of compliance/security</li> <li>• Clear rules and guidelines on what is acceptable as a digital ID verification solution Canada for financial services</li> <li>• Guidelines and accessibility</li> <li>• Best practices, fraud prevention, integration, proof of identity able to be passed on to funding partners</li> <li>• Non-technical guidelines into the elements of authentication for senior leaders who will need to sign-off - what's required to replace in-person processes</li> <li>• Technical, legal and operational, mostly for the end user. Accessibility to all users should not be ignored.</li> </ul>	<ul style="list-style-type: none"> <li>• Self-Sovereign Identity integration</li> <li>• Common work on shared code and infrastructures to build skills</li> <li>• Blockchain technology</li> </ul> 



## Interest in an information session by DIACC for your industry or organization?



## Do you think your industry would benefit from a proof of concept of a Digital ID solution?



# Join the DIACC

Be part of the world-leading community unlocking economic and social opportunities for all by building a robust, secure, interoperable, and privacy-enhancing digital identification and authentication ecosystem.

## Contact

The Digital ID and Authentication Council of Canada



[diacc.ca](https://diacc.ca)

[in /company/mydiacc](https://www.linkedin.com/company/mydiacc)



[@mydiacc](https://twitter.com/mydiacc)

[f /mydiacc](https://www.facebook.com/mydiacc)

