2022 PUBLIC SECTOR IDENTITY INDEX — GLOBAL REPORT

January 2022

Presented to:

okta | auth0

Market Connections®
Research you can act on.

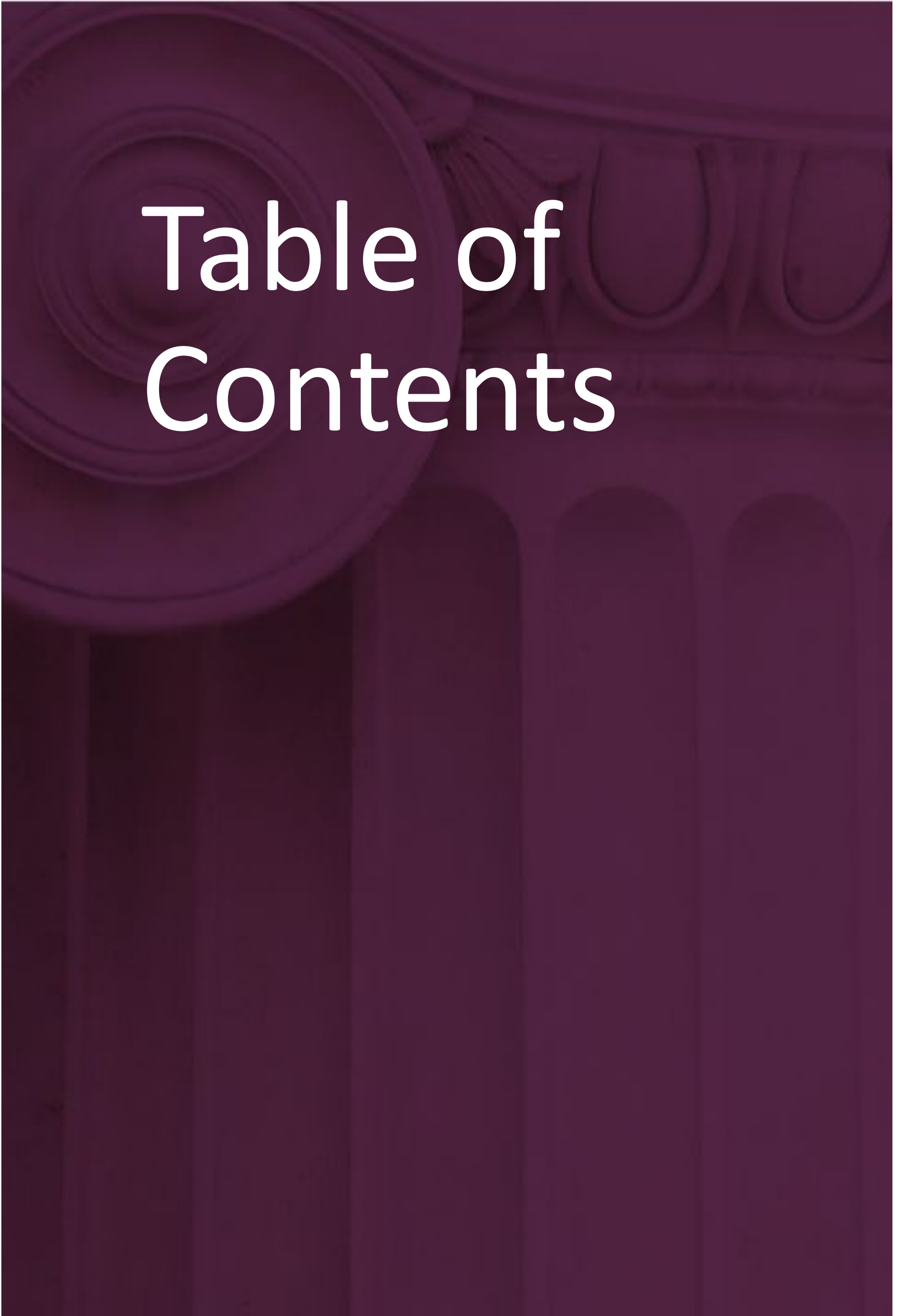


Table of Contents

Methodology 3
Respondent Classifications 4
Digital Services Landscape 11
Authentication Landscape 23
Single IAM System 28
Key Takeaways 33

Methodology

Market Connections and Auth0 partnered to design an online survey of 850 IT and line of business decision makers within national and state/local governments in the US (200 federal, 200 state & local), UK (100 federal, 100 state & local), and Australia/New Zealand (155 federal/national, 95 state & local) , fielded in September - October 2021.

PRIMARY OBJECTIVES:

To identify and quantify:

- The current state of identify authentication and security
- Challenges to current implementation
- Current pain points
- Plans and concerns over changing systems and processes

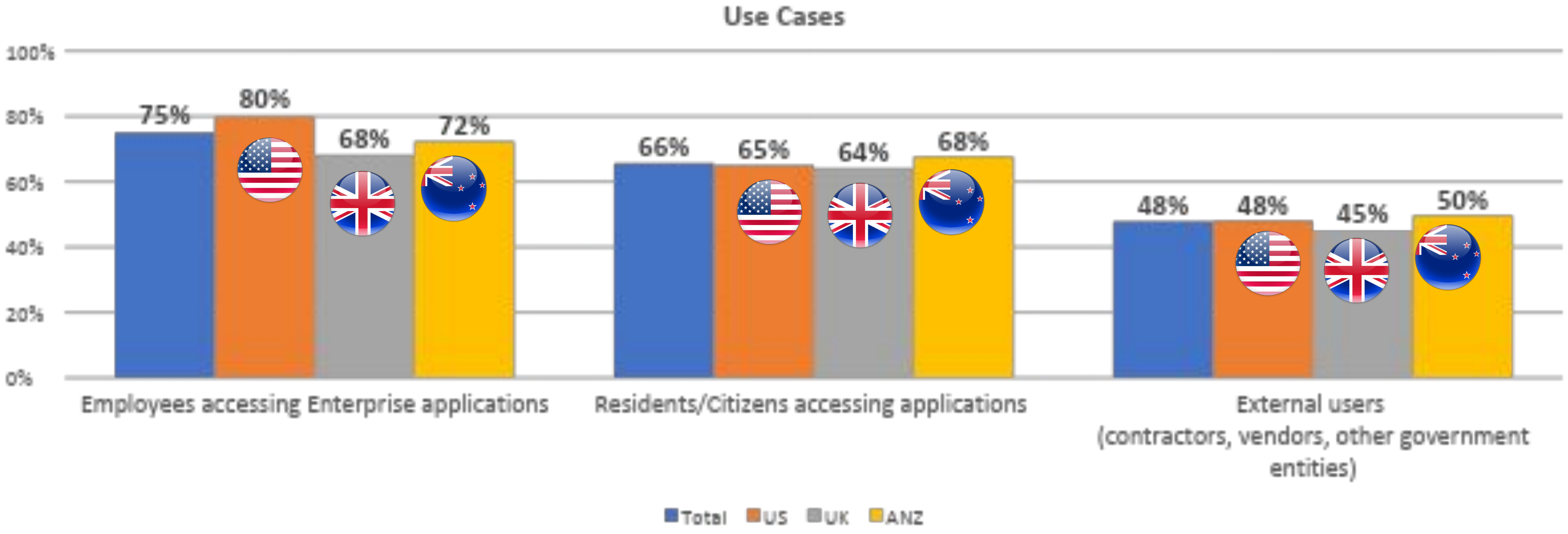
Respondent Classifications

Sample Composition

	Total	United States (US)	United Kingdom (UK)	Australia/ New Zealand (ANZ)
Federal/National Government	**455**	**200**	**100**	**155** **80 New Zealand** **75 Australia**
State and Local Government (population 250,000+)	**395**	**200**	**100**	**95 (Australia Only)**
Total	**850**	**400**	**200**	**250**

Respondent Classifications

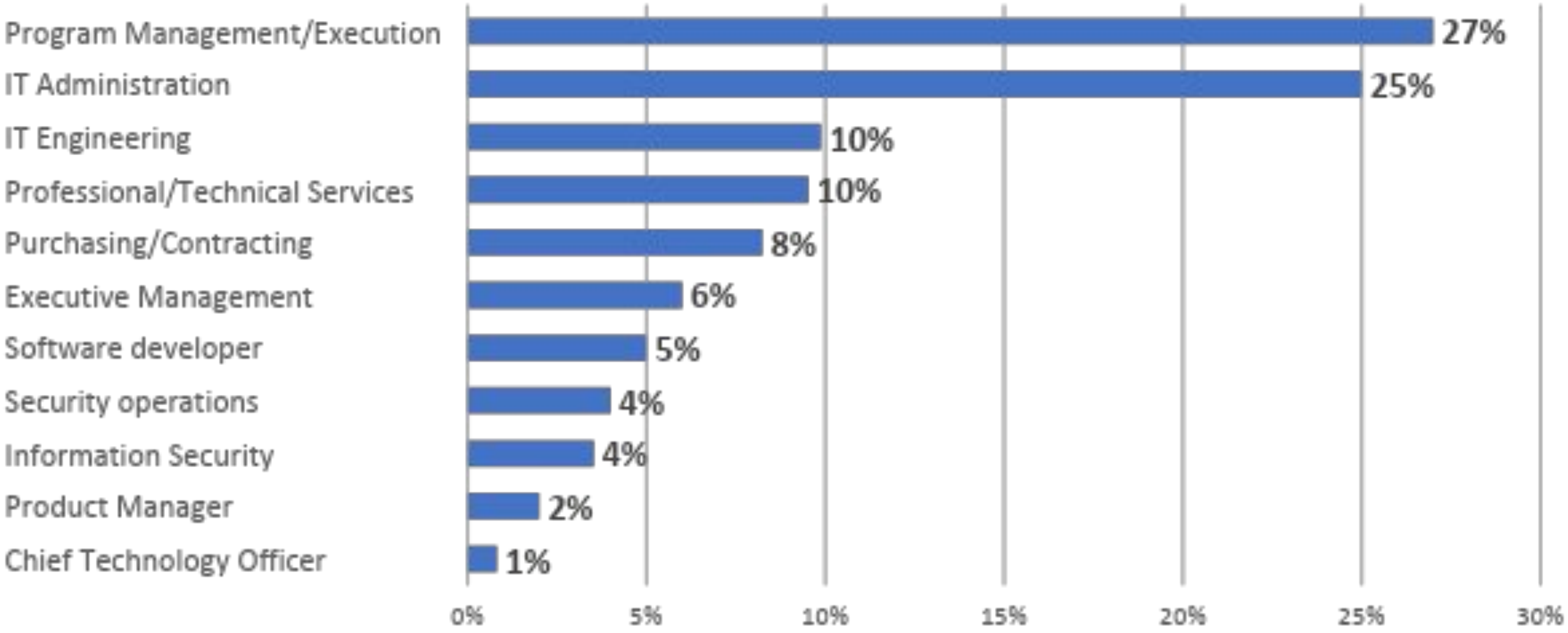
The most frequently cited use case was employees accessing Enterprise applications, but two-thirds also cited residents/citizens accessing applications and nearly half cited external users.



Which of the following use cases are most applicable to your role

Respondent Classifications – Job Role

Most respondents were either in program management/execution or IT administration.

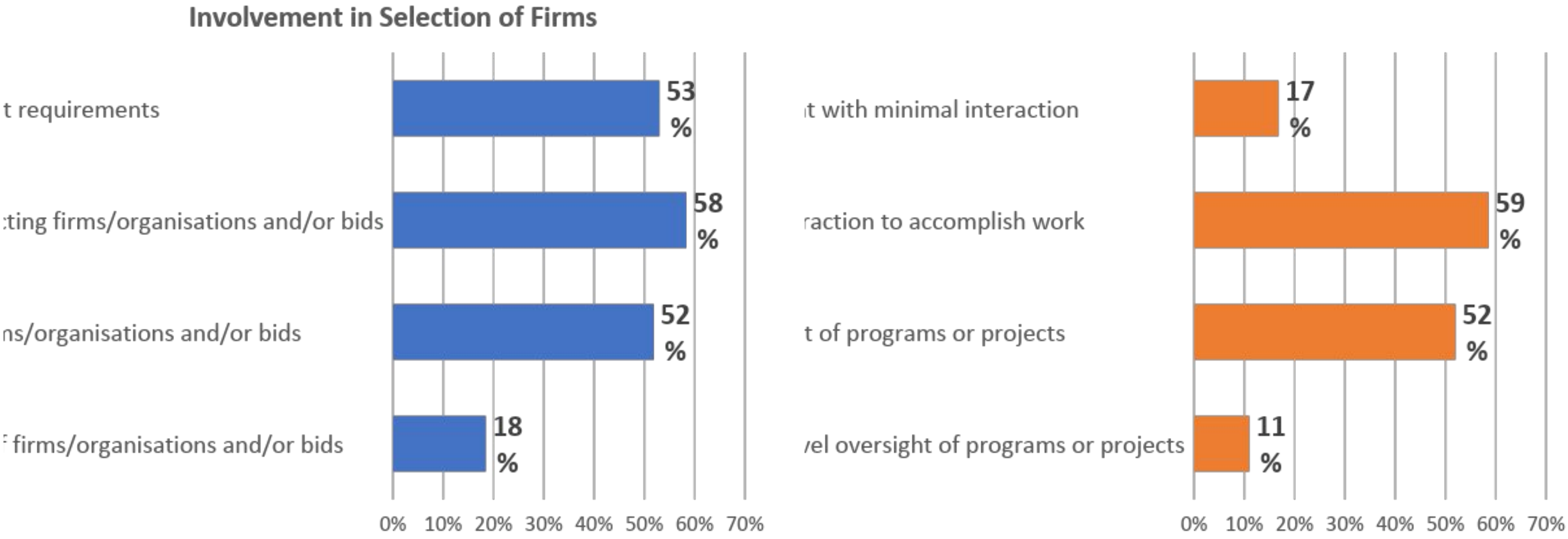


	🇺🇸	🇬🇧	🇳🇿
Program Management/Execution	23%	32%	30%
IT Administration	30%	15%	26%
IT Engineering	11%	12%	8%
Professional/Technical Services	8%	13%	10%
Purchasing/Contracting	9%	6%	10%
Executive Management	9%	3%	3%
Software developer	2%	8%	6%
Security operations	2%	8%	3%
Information Security	4%	4%	3%
Product Manager	1%	2%	3%
Chief Technology Officer	2%	1%	0%

Q *Which of the following best describes your role in your organization?*

Respondent Classifications

Respondents were screened to ensure they were involved in either their organization’s selection of or management of firms that provide Identity and Access Management (IAM).

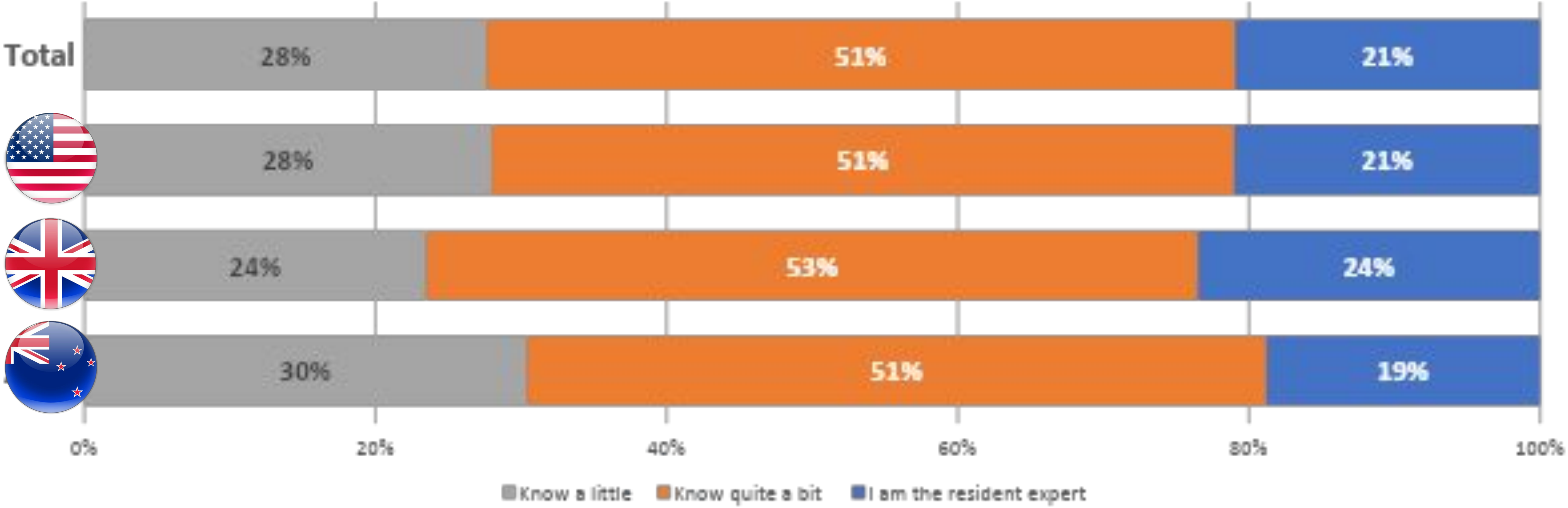


Q *In which of the following ways are you or have you been involved in your [organization's/organisation’s] selection of firms that provide Identity and Access Management (IAM)?*

In which of the following ways are you or have you been involved in your [organization's/organisation’s] management of these firms once they have been hired or selected?

Respondent Classifications – IAM Knowledge

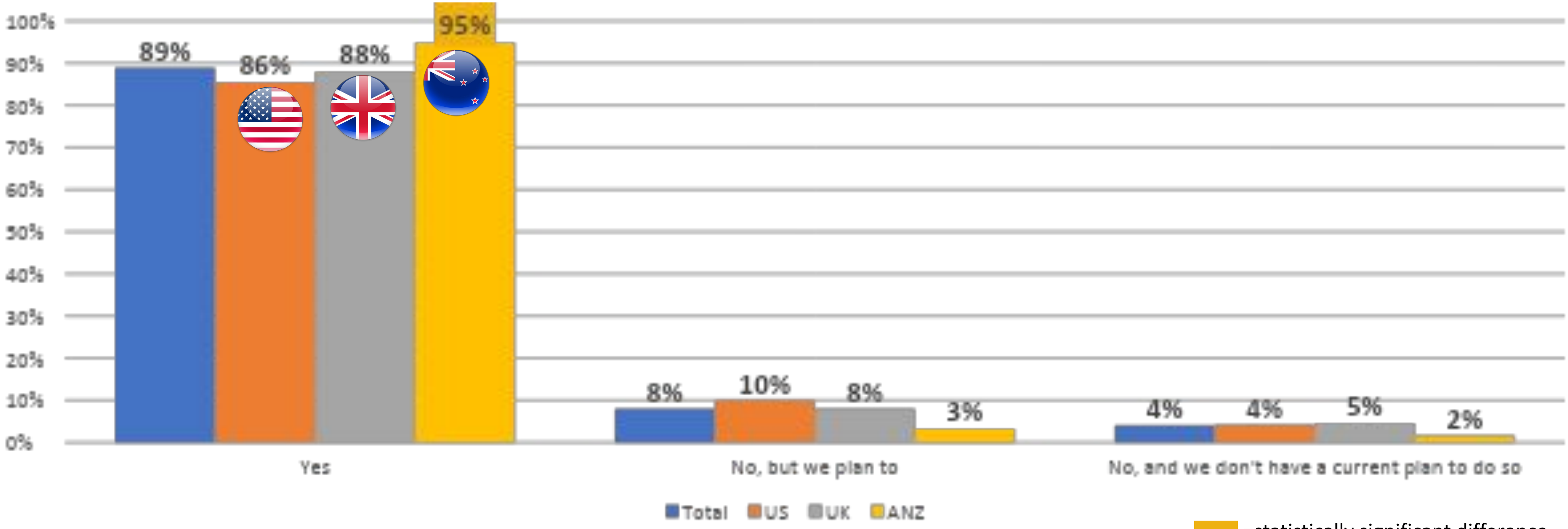
Respondents were screened to ensure they knew at least a little about their organization's processes around IAM; nearly three-quarters know quite a bit or are the resident expert in their organization.



Q *How would you describe your knowledge of your organization's processes around Identity and Access Management (IAM)?*

Organization Currently Builds External-Facing Applications

While the overwhelming majority currently build external-facing applications, those in ANZ are most likely to do so.



🟨 =statistically significant difference

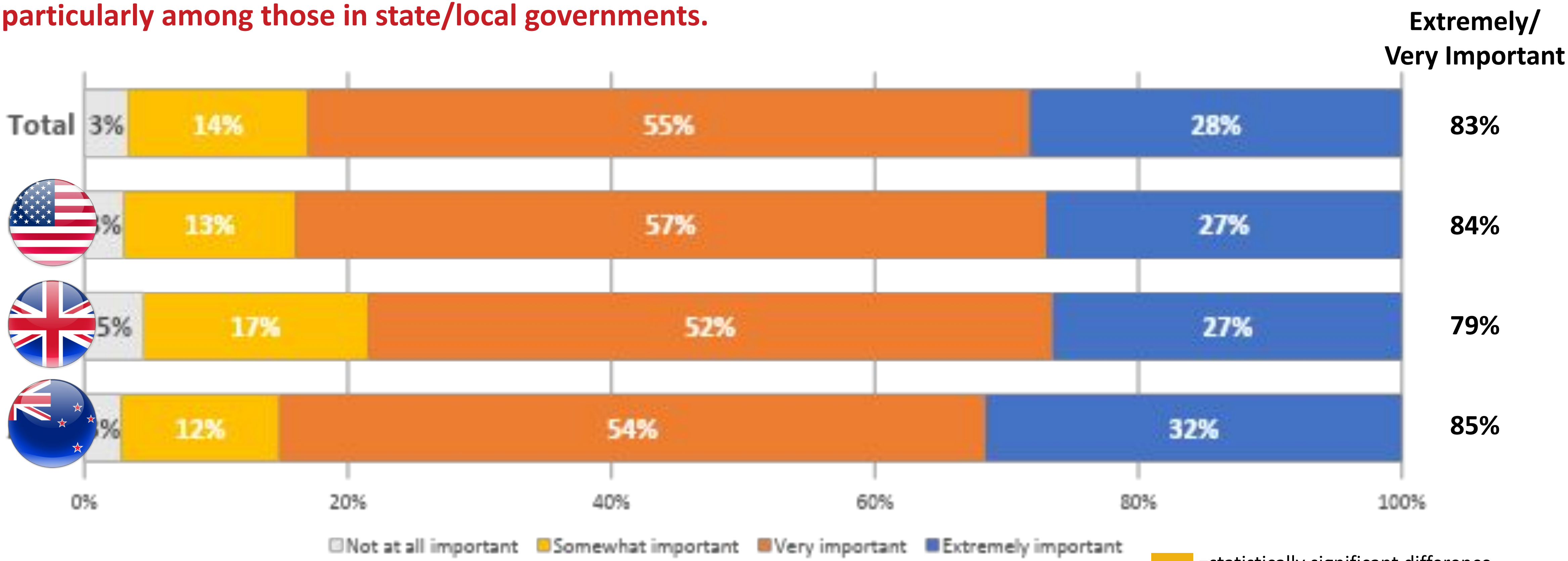
Does your [organization/organisation] currently build external-facing applications?

Digital Services Landscape

Importance of Providing Digital Applications/Service

	Extremely/Very Important
National/Federal	80%
State/Local	**87%**

Across the board providing digital applications/services to citizens is seen as important, particularly among those in state/local governments.



🟨 =statistically significant difference

How important is it that your organization has the ability to provide digital applications or services for citizens?

Importance of Providing Digital Applications/Services - Examples

Not at all important

> Applications for internal use only
>
> CENTRAL GOVERNMENT, UK

> There is little need to communicate with the public, and most of it is return of confiscated items.
>
> FEDERAL CIVILIAN OR INDEPENDENT GOVERNMENT AGENCY, US

> Access is only for education providers and stakeholders
>
> FEDERAL GOVERNMENT, NEW ZEALAND

Extremely important

> …Ensuring that the services provided are available and accessible via physical or digital means is critical to the execution of the agency mission.
>
> FEDERAL CIVILIAN OR INDEPENDENT GOVERNMENT AGENCY, US

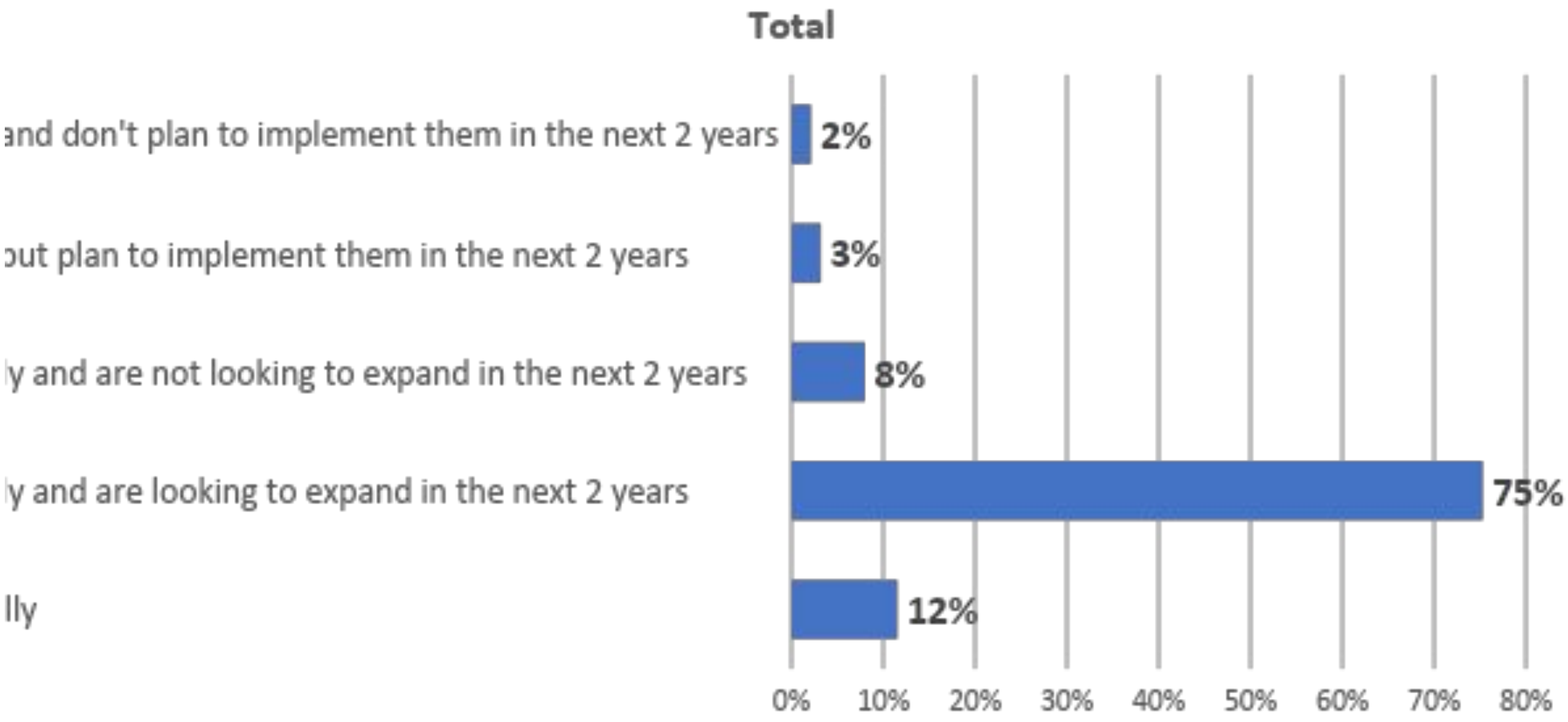
> Consumer access to online services has increased and grown extraordinarily post-COVID
>
> STATE OR TERRITORIES GOVERNMENT, AUSTRALIA

> To ensure equitable and effective access to health services for all, particularly for citizens located in remote areas.
>
> LOCAL GOVERNMENT, UK

Q *Why is it [ANSWER] that your organization has the ability to provide digital citizen services? Please be as specific and detailed as possible*

Current State of Digitizing Citizen Services

Three-quarters have at least some services digitally and are looking to expand in the next 2 years.



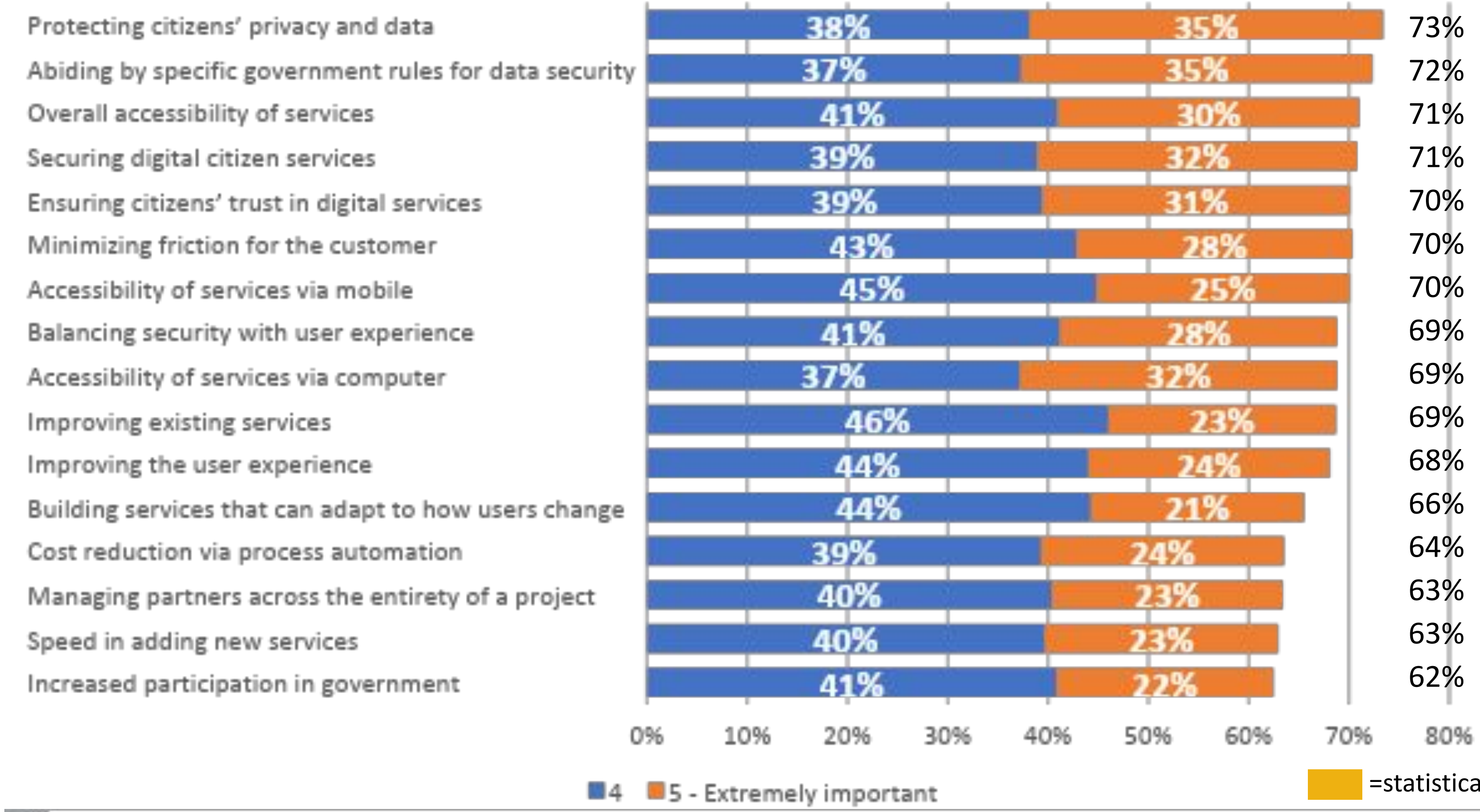
🇺🇸	🇬🇧	🇳🇿
2%	3%	2%
3%	3%	4%
10%	9%	4%
73%	78%	78%
13%	8%	12%

🟨 =statistically significant difference

Q *Currently, where is your organization in terms of digitizing its citizen services?*

Importance When Thinking About Citizen Services

- Protecting citizens' privacy and data and abiding by government data security rules are the most important to this audience.
- Those in ANZ generally view these aspects as more important, followed by those in US and then those in the UK.



5 – Extremely Important/4

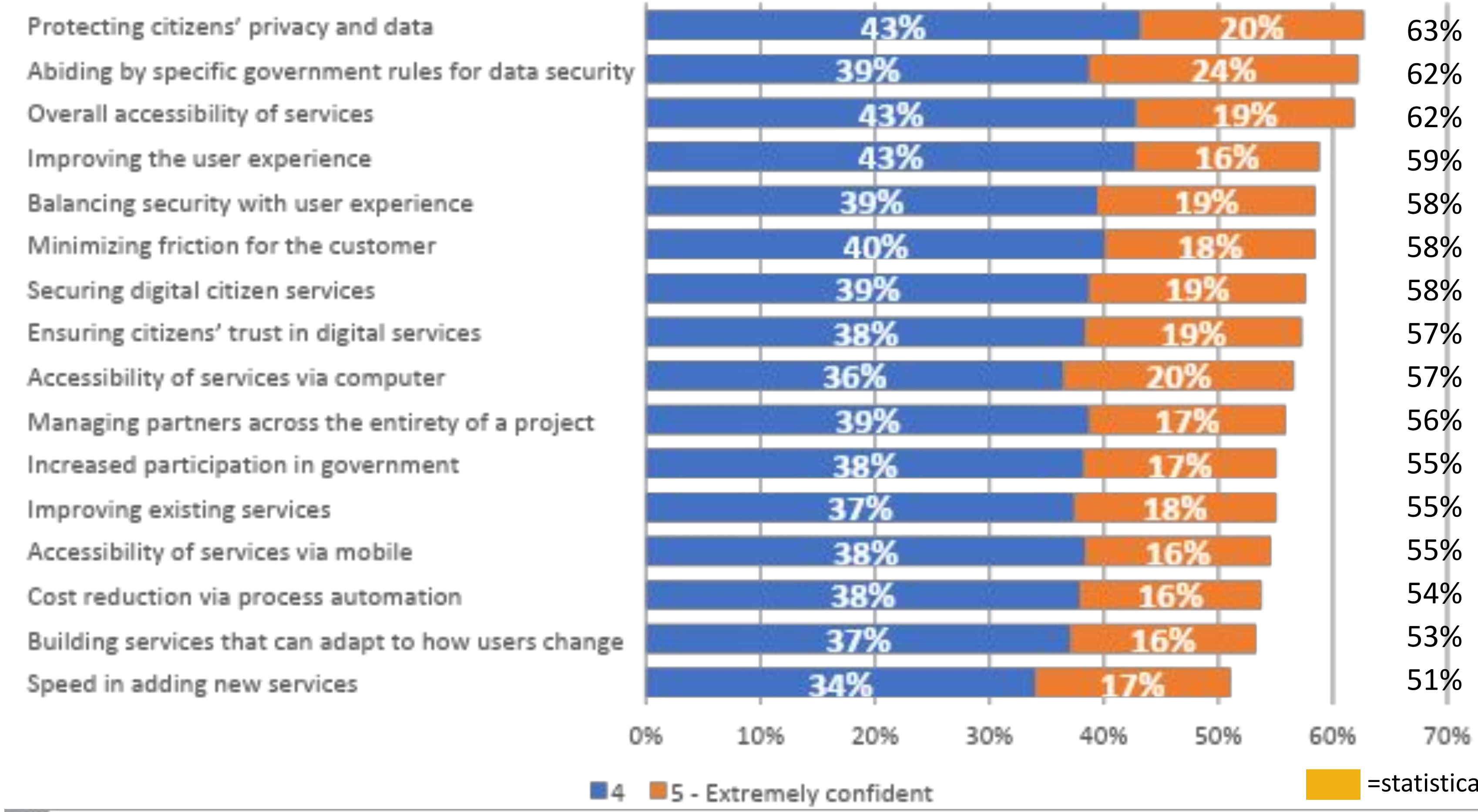
	Total	🇺🇸	🇬🇧	🇳🇿
Protecting citizens' privacy and data	73%	72%	71%	**78%**
Abiding by specific government rules for data security	72%	**73%**	65%	**78%**
Overall accessibility of services	71%	71%	68%	74%
Securing digital citizen services	71%	**72%**	62%	**76%**
Ensuring citizens' trust in digital services	70%	**71%**	63%	**74%**
Minimizing friction for the customer	70%	**70%**	62%	**78%**
Accessibility of services via mobile	70%	67%	72%	**74%**
Balancing security with user experience	69%	67%	66%	**74%**
Accessibility of services via computer	69%	70%	67%	69%
Improving existing services	69%	70%	65%	70%
Improving the user experience	68%	68%	64%	72%
Building services that can adapt to how users change	66%	65%	68%	64%
Cost reduction via process automation	64%	65%	60%	65%
Managing partners across the entirety of a project	63%	62%	60%	68%
Speed in adding new services	63%	62%	66%	62%
Increased participation in government	62%	65%	62%	59%

🟨 =statistically significant difference

Q *How important are each of the following to your ${custom25} when thinking about its citizen services?*

Confidence in Delivering

- These respondents are the most confident in their ability to deliver on the things of most importance to them – protecting privacy/data and abiding by data security rules.
- Those in ANZ generally view themselves as more confident than those in the US and the UK.



5 – Extremely Confident/4

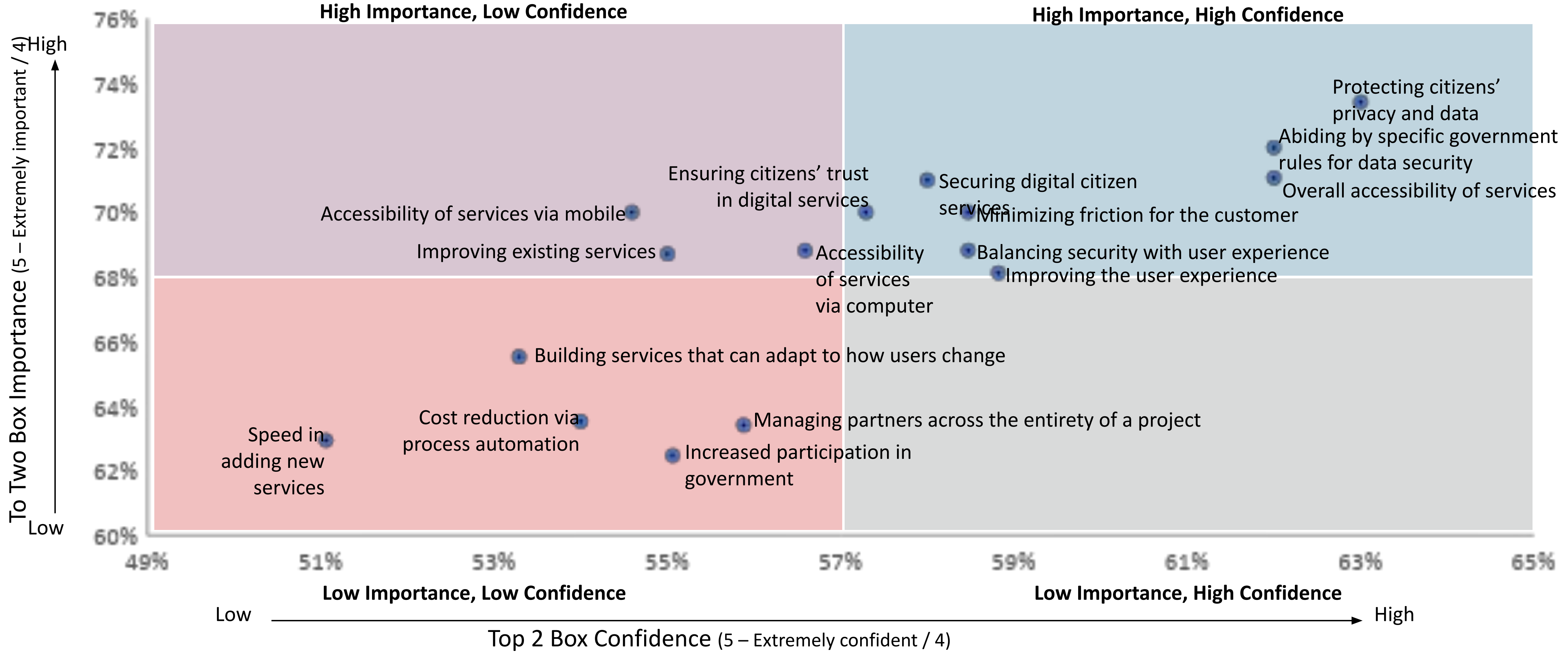
Total	🇺🇸	🇬🇧	🇳🇿
63%	65%	54%	66%
62%	63%	56%	67%
62%	58%	60%	70%
59%	60%	57%	60%
58%	58%	54%	63%
58%	58%	54%	63%
58%	59%	52%	61%
57%	56%	53%	62%
57%	57%	56%	56%
56%	54%	55%	59%
55%	55%	53%	58%
55%	55%	48%	62%
55%	54%	53%	57%
54%	53%	48%	60%
53%	53%	54%	53%
51%	54%	48%	49%

🟨 =statistically significant difference

How confident are you in your [organization's/organisation's] current ability to deliver on each of the following aspects of citizen services?

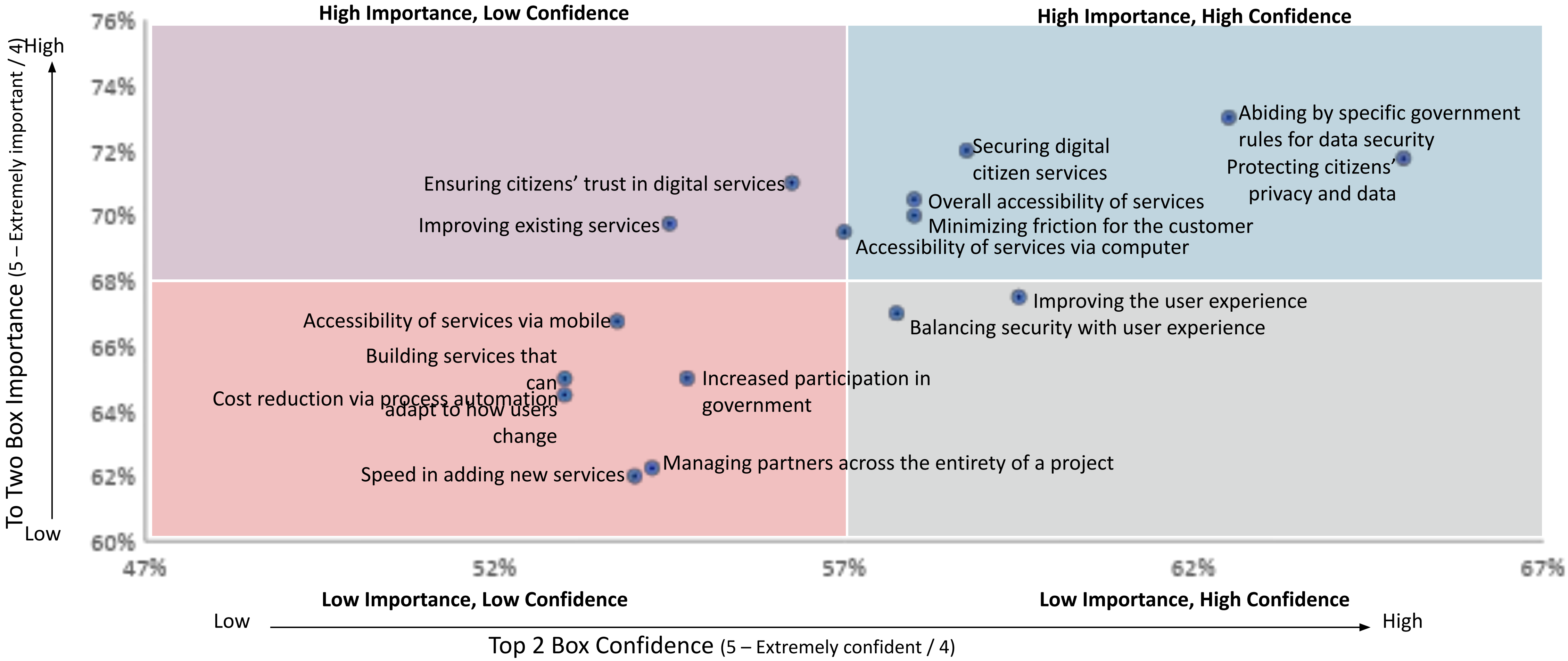
Importance/Confidence: Total

In total, these respondents have key perceived weaknesses in accessibility of services via mobile and via computer, as well as in improving existing services.



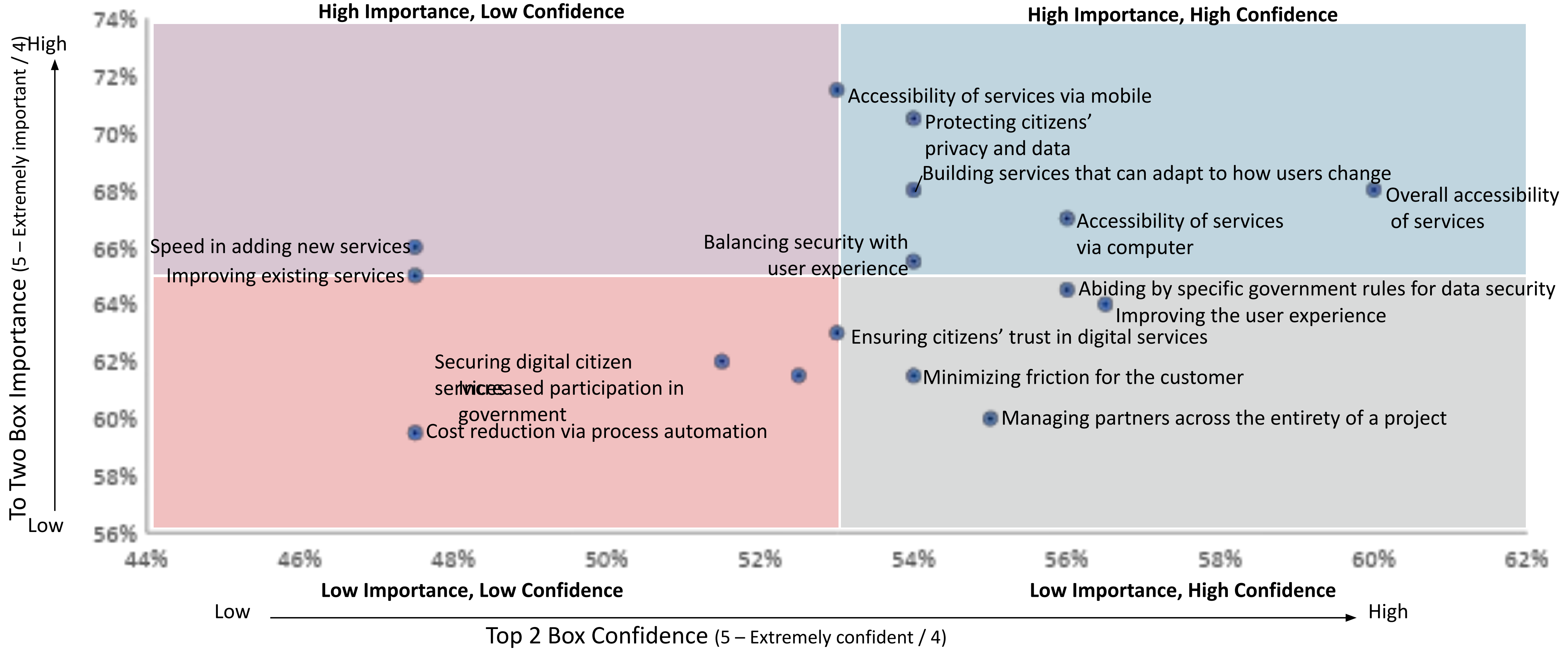
Importance/Confidence: S

In the US, these respondents have key perceived weaknesses in ensuring citizens' trust in digital services and improving existing services.



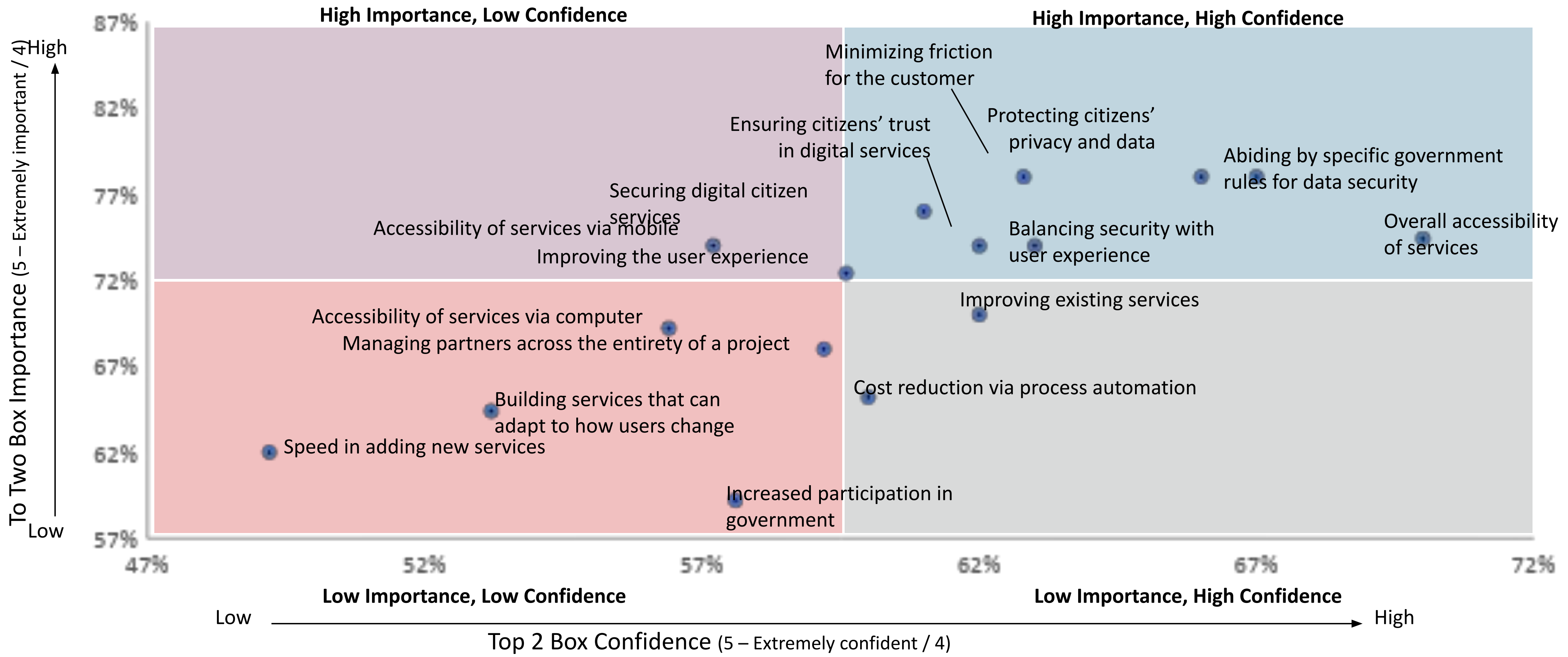
Importance/Confidence: UK

In the UK, these respondents have key perceived weaknesses in accessibility of services via mobile, speed in adding new services and improving existing services.



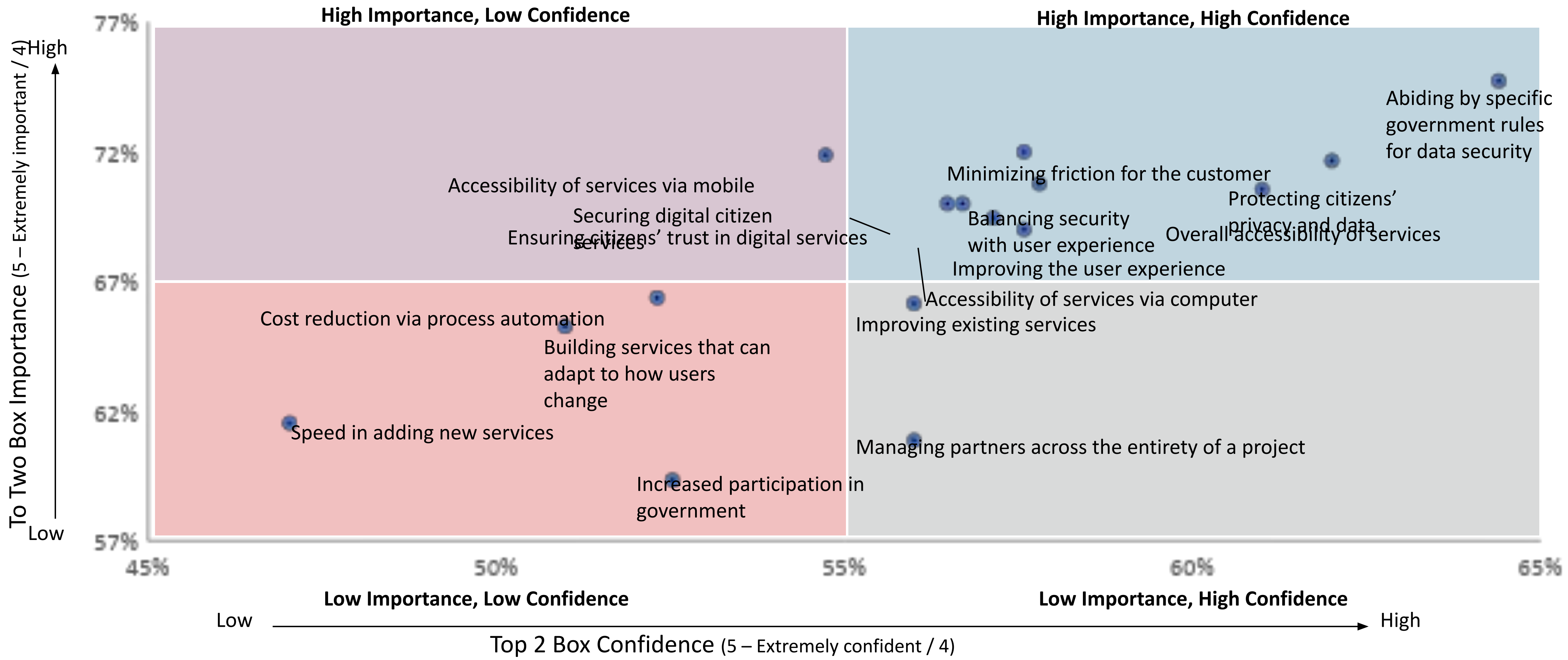
Importance/Confidence: ANZ

In ANZ, these respondents have key perceived weaknesses in the accessibility of services via mobile and improving the user experience.



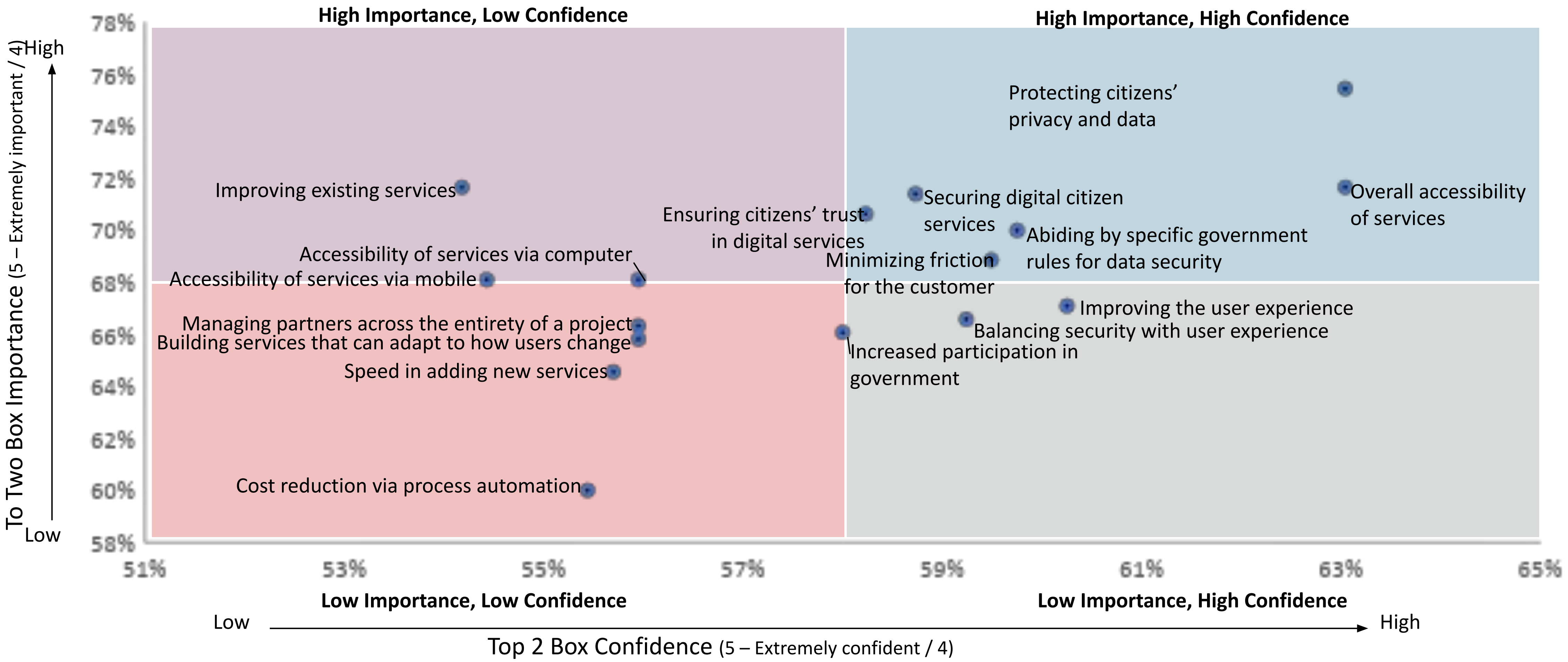
Importance/Confidence: National/Federal

National/Federal respondents have a key perceived weakness in the accessibility of services via mobile.



Importance/Confidence: State/Local

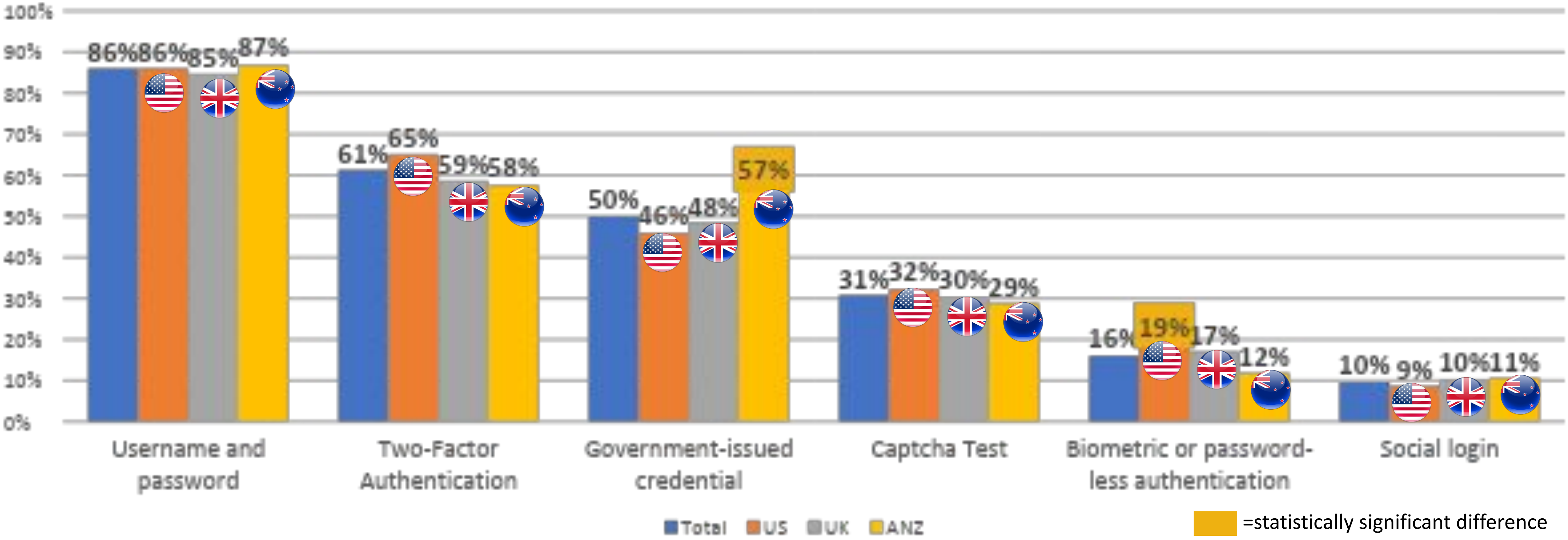
State/Local respondents have key perceived weaknesses in improving existing services and in the accessibility of services via mobile and computer.



Authentication Landscape

Current Authentication Methods Used by Citizens

- Overall, username and password is the most frequently used, following by two-factor authentication.
- ANZ are the most likely to use a government-issued credential, and the US are more likely than ANZ to use biometric or password-less authentication.

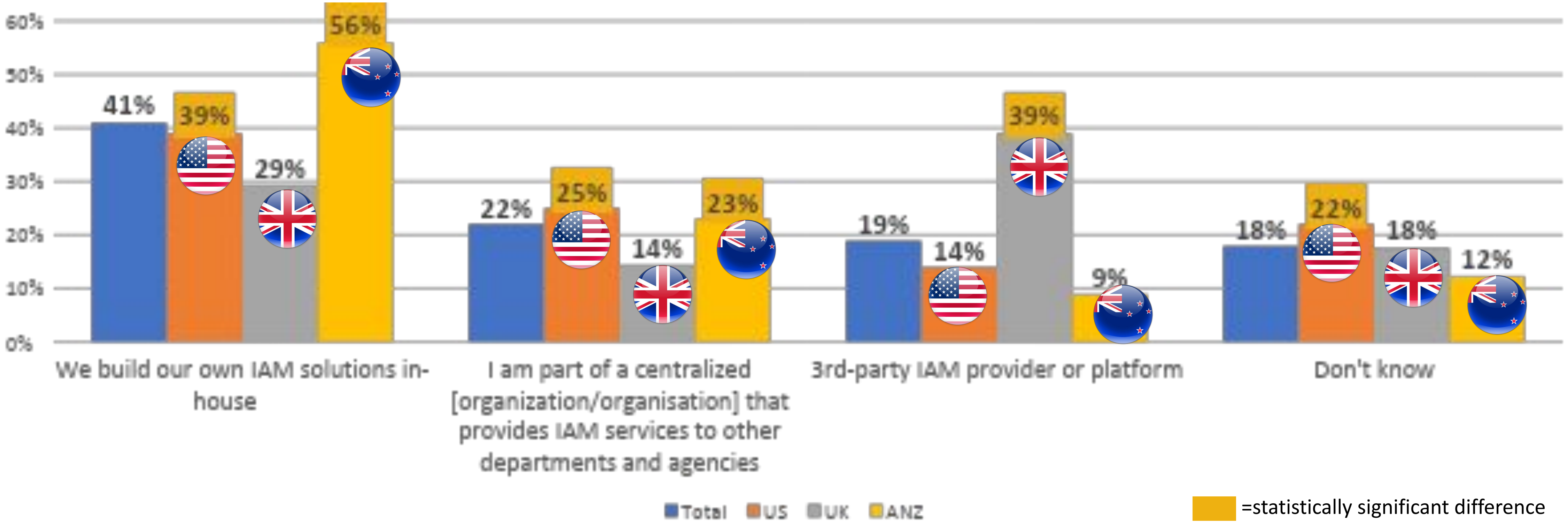


🟨 =statistically significant difference

Which authentication method are citizens currently using to access your digital applications or services? Select all that apply

Current Providers of IAM

- Four in ten currently build their own IAM solutions in-house – most in ANZ, followed by US and then UK.
- Those in the UK are the most likely to be using a 3rd party IAM provider or platform.

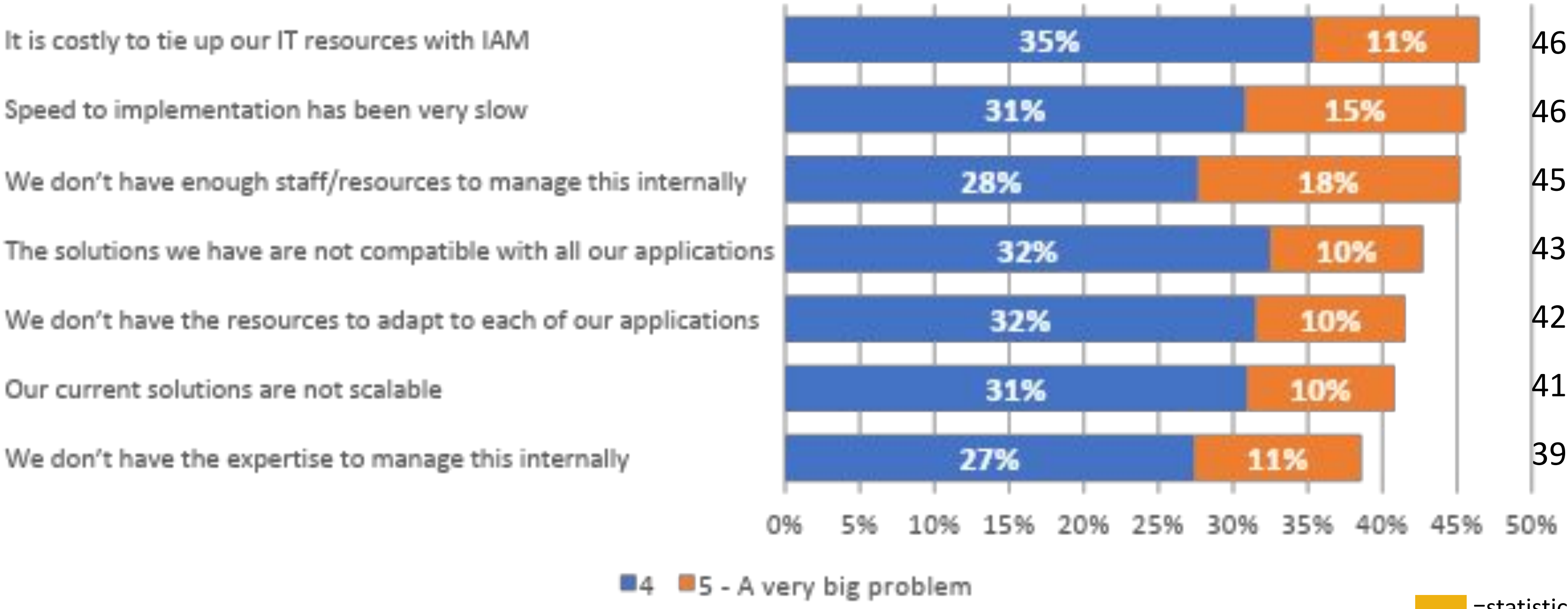


🟨=statistically significant difference

Who currently provides Identity and Access Management (IAM) services for your [organization's/organisation's]?

Pain Points in Building IAM In-House

The biggest pain points of building IAM in-house are tying up internal IT resources, slow speed to implementation and not having enough staff/resources to manage it internally.



5 - A very big problem/4

Total	🇺🇸	🇬🇧	🇳🇿
46%	47%	40%	🟨 52%
46%	45%	40%	🟨 52%
45%	46%	41%	48%
43%	41%	35%	🟨 51%
42%	41%	45%	40%
41%	🟨 44%	32%	🟨 44%
39%	37%	35%	44%

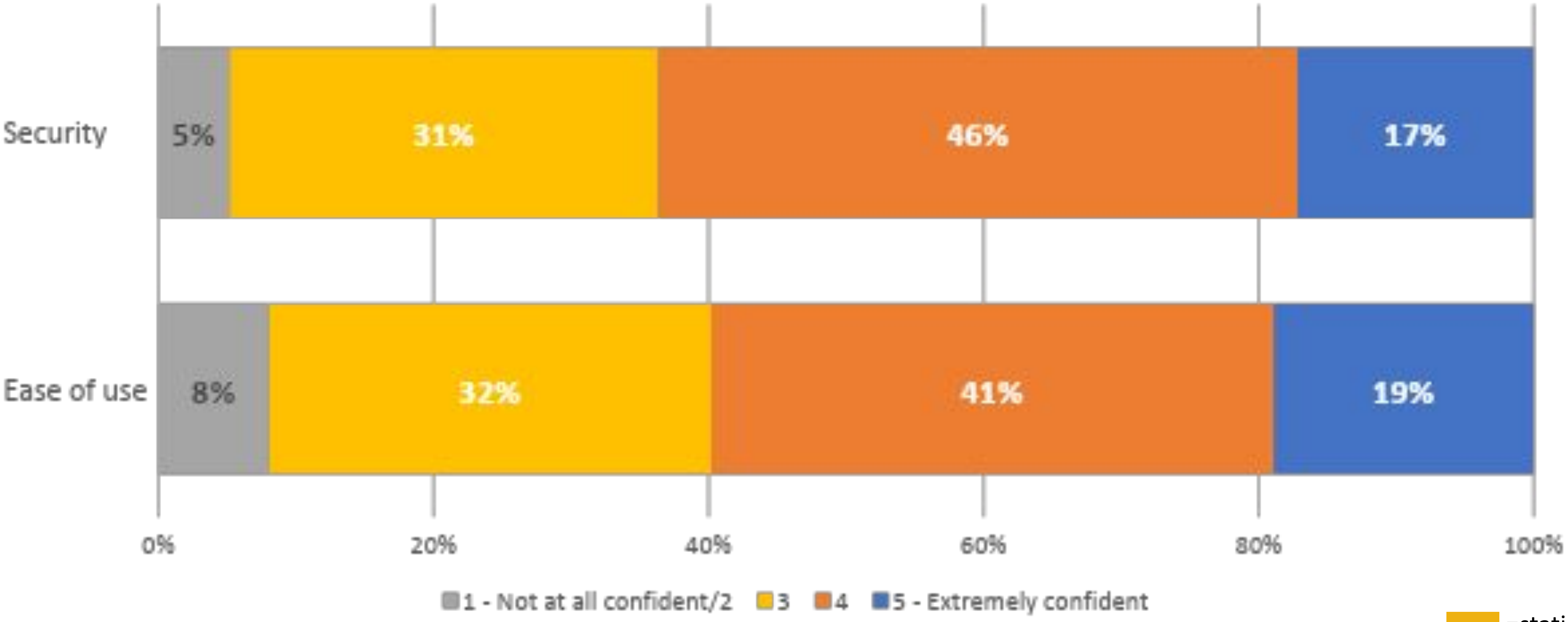
🟨 =statistically significant difference

Q *How much of a problem are each of these potential pain points in building Identity and Access Management (IAM) in-house for your [organization/organisation]?*

Confidence Regarding Current Authentication Solu

5 – Extremely confident/4	Ease of use
National/Federal	56%
State/Local	63%

- Less than one in five are extremely confident in either the security or the ease of use of their current authentication solutions.
- Those in ANZ and State/Local are the most confident.



5 - Extremely confident/4

Total	🇺🇸	🇬🇧	🇳🇿
64%	63%	59%	69% 🟨
60%	58%	50%	70% 🟨

🟨 =statistically significant difference

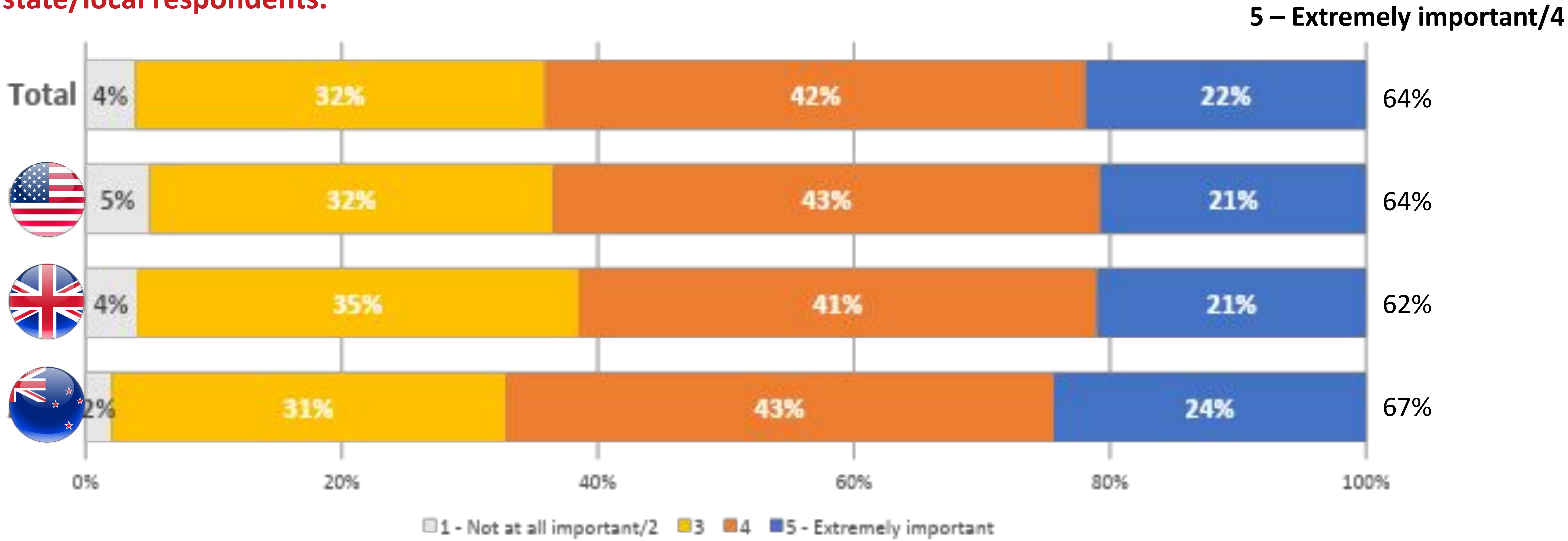
How confident are you in each of the following regarding your current authentication solution?

Single IAM System

Importance in Having One Digital Credential Across Services

Overall, having one digital credential for authentication and authorization across all services is seen as very important across the board, particularly among state/local respondents.

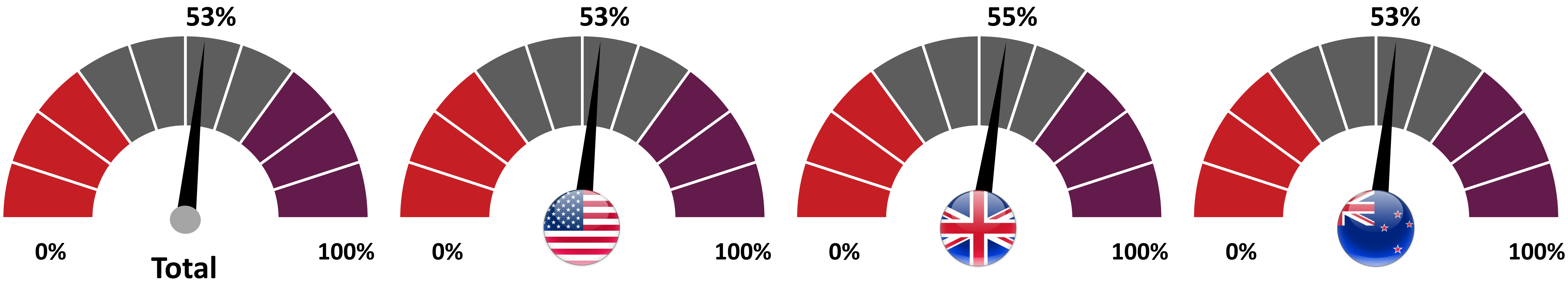
5 – Extremely important/4	
National/Federal	61%
State/Local	68%



How important is it to your [organization/organisation] to have one digital credential for authentication and authorization across all your services? By this we mean enabling users to securely authenticate with multiple applications using a single set of credentials (username and password)

Percentage of Services Having a Single Digital Credential for Access

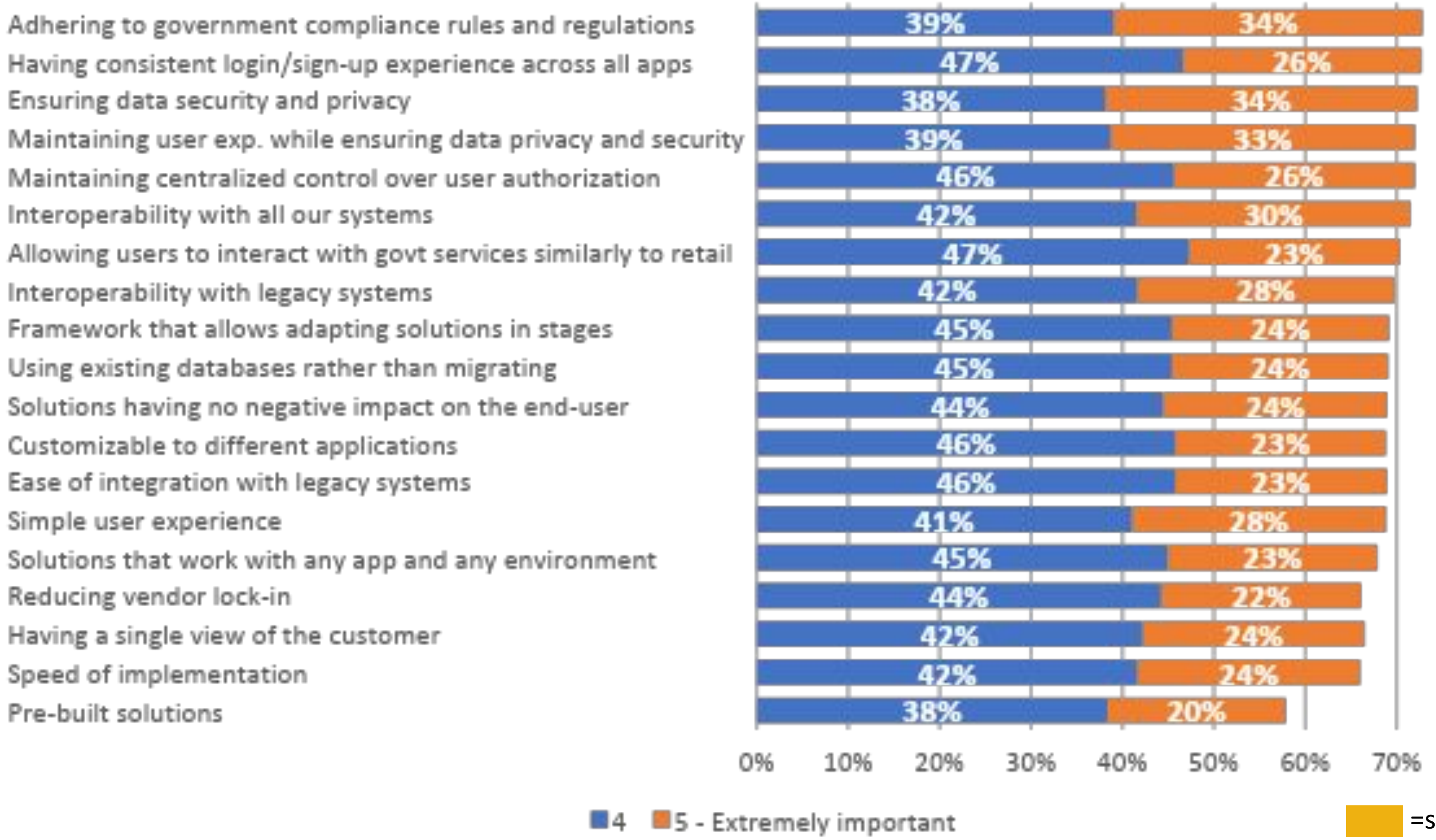
While having a single digital credential for access is seen as important, just over half of services currently have one.



Q *Across what percentage of your services do you currently have a single digital credential for access?*

Importance of Aspects of Implementing Single IAM System

Adhering to compliance rules and having a consistent experience across all applications are the most important overall, though differences exist across countries.



5 – Extremely Important/4

Total	🇺🇸	🇬🇧	🇳🇿
73%	74%	65%	78%
73%	73%	68%	76%
72%	71%	68%	78%
72%	72%	73%	71%
72%	74%	67%	73%
72%	71%	69%	74%
70%	70%	67%	74%
70%	70%	63%	76%
69%	73%	65%	66%
69%	67%	65%	76%
69%	72%	61%	72%
69%	70%	63%	71%
69%	72%	58%	74%
69%	70%	64%	71%
68%	66%	68%	72%
66%	67%	66%	65%
66%	67%	60%	71%
66%	65%	63%	71%
58%	62%	58%	51%

🟨 =statistically significant difference

How important are each of the following when thinking about implementing/maintaining a single system for identity and access management across all your services?

Statement Agreement

In general, these respondents don't feel it's too difficult to get citizens on board or to justify the cost, it's a matter of control and speed to implementation.

	Total	🇺🇸	🇬🇧	🇳🇿
It is imperative that my org. be able to continue to control user authorization	77%	76%	77%	77%
Digital identity is about more than authorization and authentication	72%	71%	75%	73%
It is important for our devs. and engrs. to be able to implement digital identity solutions quickly	70%	67%	71%	74%
Implementing a single service hub for identity systems will simplify work for core dev. Teams	68%	66%	72%	69%
Our end goal is to have a single sign-on to be able to access services from the govt at all levels	60%	63%	55%	60%
The internal developer community should be part of the process of determining how identity authentication and security is managed, and by whom	60%	58%	60%	62%
Having a 3rd-party solution to identity authentication and security would free up internal resources	58%	57%	63%	57%
My org. has enough internal expertise to implement/maintain single sign-on authentication	56%	55%	62%	55%
My org. does not currently have the time and resources to adapt a single sign-on authentication to all our applications	55%	53%	57%	57%
Outsourcing identity authentication to a third-party vendor is too expensive	53%	55%	51%	52%
My org. has enough manpower to implement/maintain single sign-on authentication	51%	51%	48%	56%
It is difficult to get internal stakeholders on board with single sign-on authentication	51%	51%	49%	52%
It's difficult to justify the cost of having identity authentication via a 3rd party	50%	49%	50%	51%
It is difficult to get citizens on board with single sign-on authentication	47%	49%	44%	49%

Q *How important are each of the following when thinking about implementing/maintaining a single system for identity and access management across all your services?*

Key Takeaways

KEY TAKEAWAY

Overall, citizens are largely relying on username and password as their current authentication method.

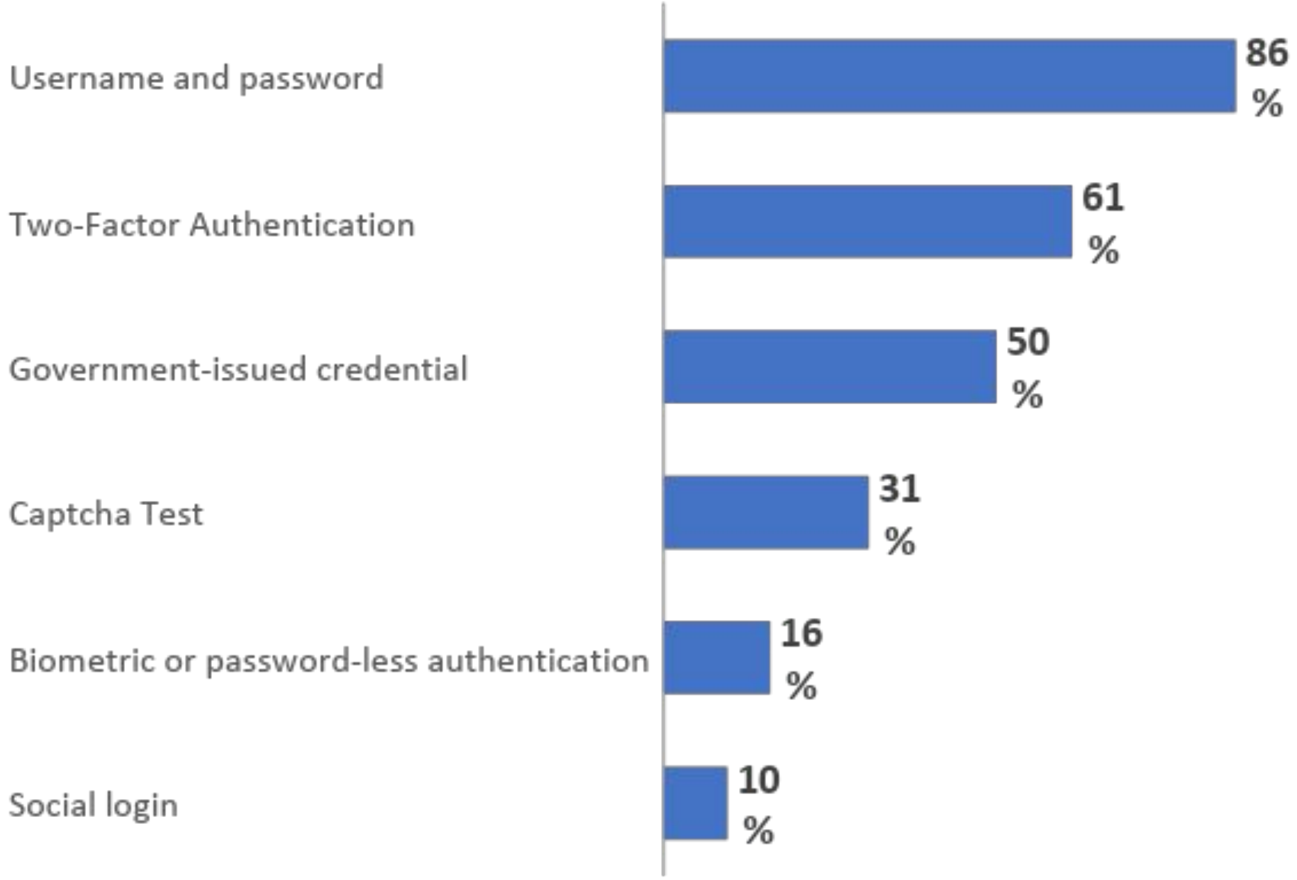
INSIGHT

- Nearly nine in ten say that citizens use username and password as their current authentication method, while only half use a government-issued credential

ACTION

- To broaden adoption of more secure authentication methods, citizens will need to be shown the risks of username and password and benefits of alternative authentication methods.

Current Authentication Methods Used by Citizens



KEY TAKEAWAY

Most are looking to expand their digital services in the next two years, but IAM providers are varied, with four in ten building them in-house.

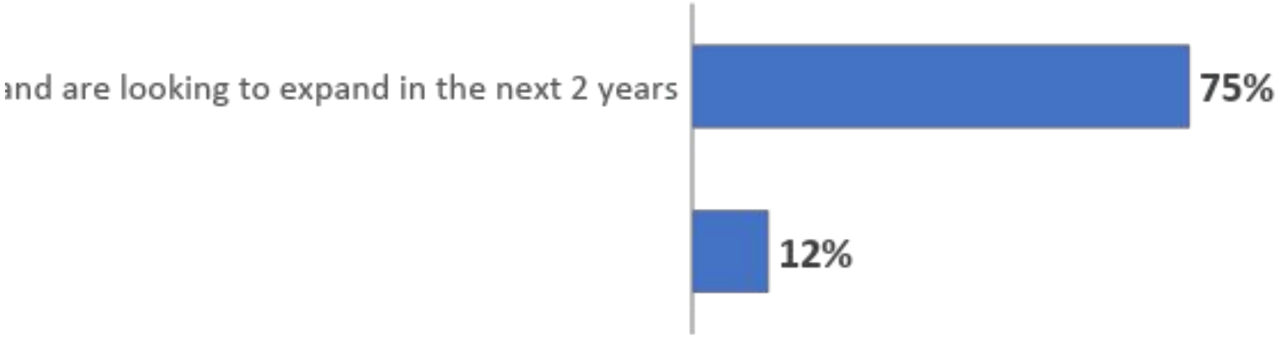
INSIGHT

- While one in ten have all their services currently available digitally, three-quarters have some available digitally and are looking to expand.
- Four in ten currently build their own IAM solutions in-house, with one in five currently outsourcing.

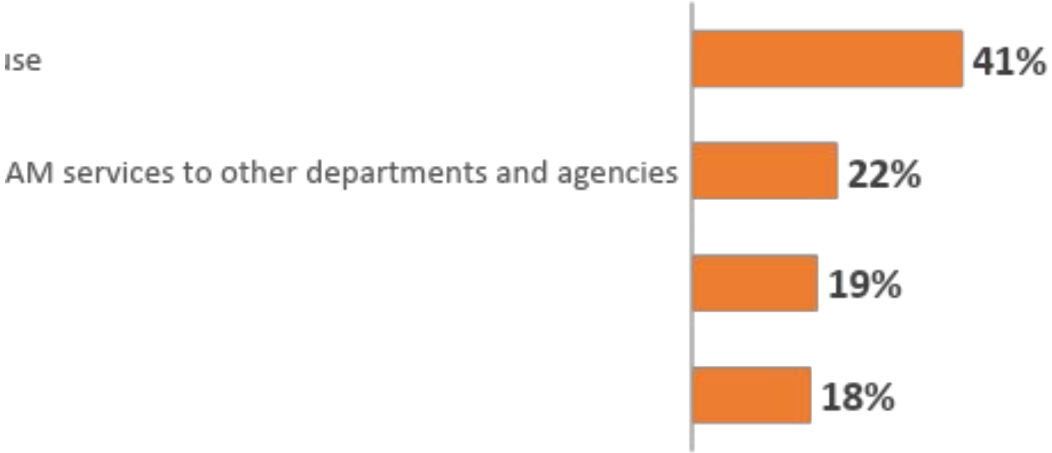
ACTION

- Identifying areas of opportunity for attaching IAM services to expanding digital services, focus marketing and messaging that shows clear benefits and value of outsourcing.

Current State of Digitizing Citizen Services



Who Provides IAM Services



KEY TAKEAWAY

Speed and using internal resources are two of the biggest pain points in building IAM solutions in-house, but many pain points are seen.

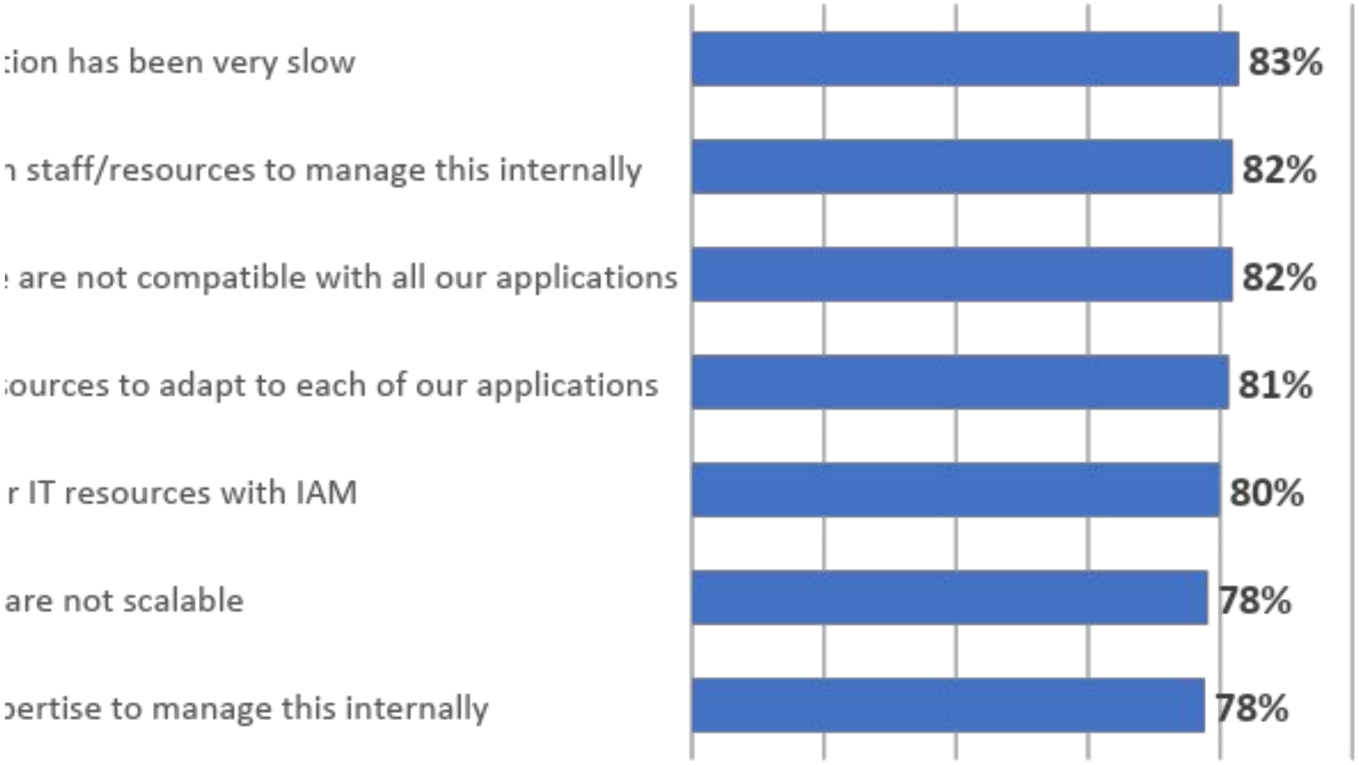
INSIGHT

- Three-quarters or more cited each potential pain point as at least a 3 on a 5-point scale.
- More than eight in ten cite speed to implementation as a pain point, as well as not having enough staff to manage IAM internally.

ACTION

- Marketing and messaging that can speak to how these pain points can be addressed via solutions will resonate with this audience.

Pain Points of Building IAM In-House



KEY TAKEAWAY

Respondents saw key weaknesses of improving existing services and the accessibility of services via mobile and computer.

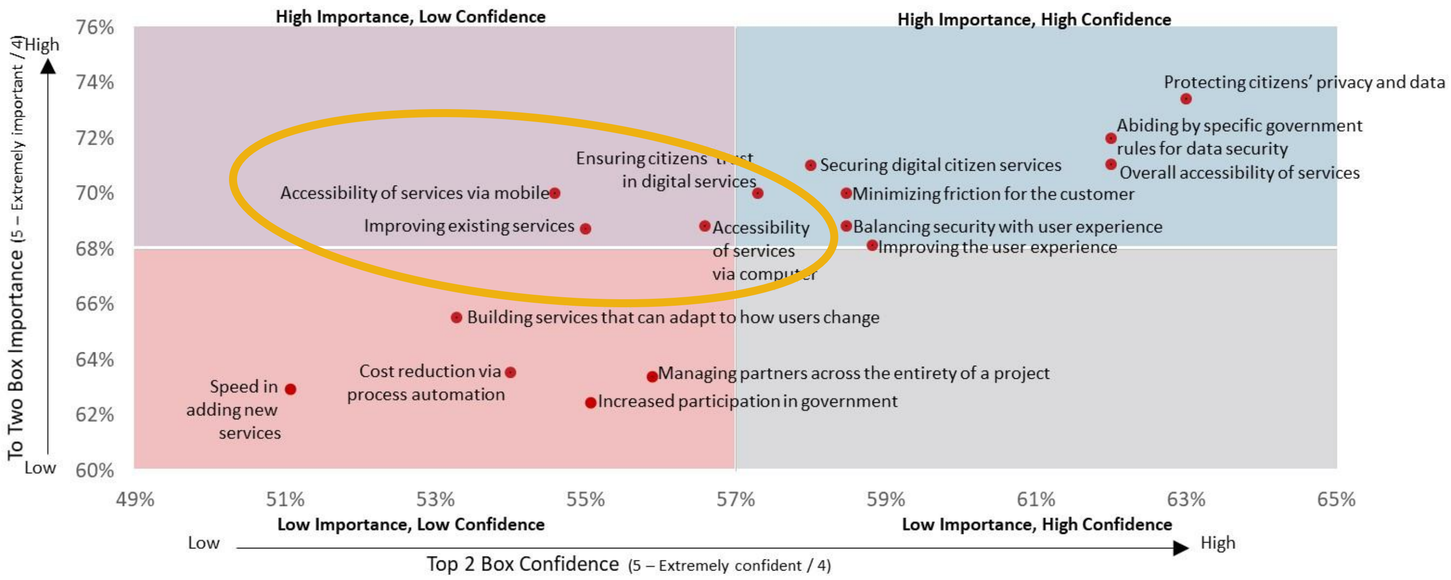
INSIGHT

- These aspects of citizen services are areas that are of high importance, but respondents had less confidence in their organization's ability to deliver.

ACTION

- Solutions that can help with accessibility and improving existing services would be of value to this audience.

Areas of Perceived Weakness



KEY TAKEAWAY

While having a single credential across services is seen as largely important, only a little over half have a single digital credential.

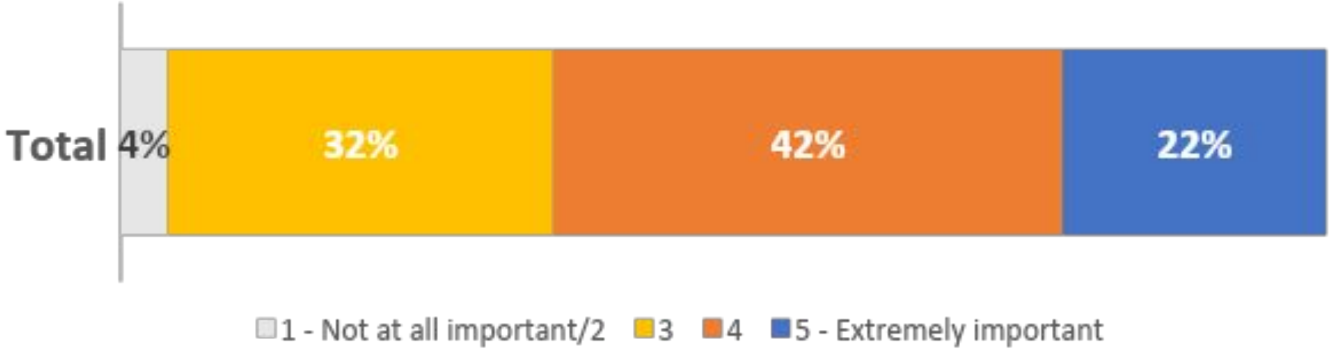
INSIGHT

- The importance is near universal – less than 5% view having one credential across services as a 1 or 2.
- However, just over half of services have a single credential – a significant opportunity.

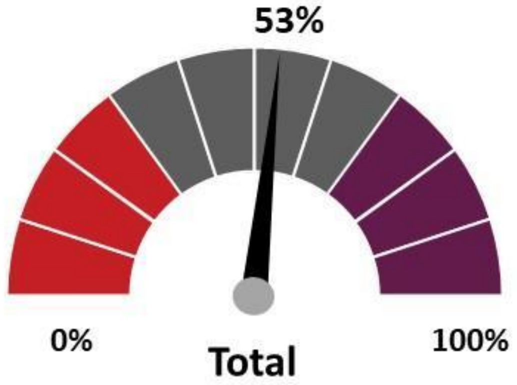
ACTION

- There's an opportunity to expand services using a single digital credential, if stakeholder see the value and benefits.

Importance Having One Credential Across Services



% of Services Having a Single Digital Credential



KEY TAKEAWAY

While value is seen in implementing a single IAM system, key issues of compliance, data privacy and a consistent user experience must be addressed.

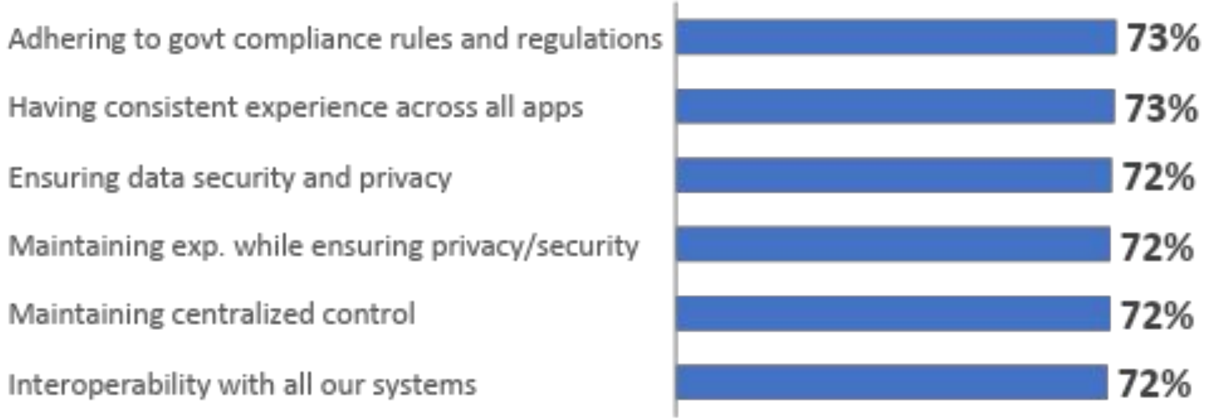
INSIGHT

- Compliance, consistency in experience, ensuring data privacy/security, maintaining centralized control and interoperability are of top importance in implementing a single IAM system.
- Three-quarters say they must be able to continue control over authorization, while many are concerned with implementing solutions quickly.

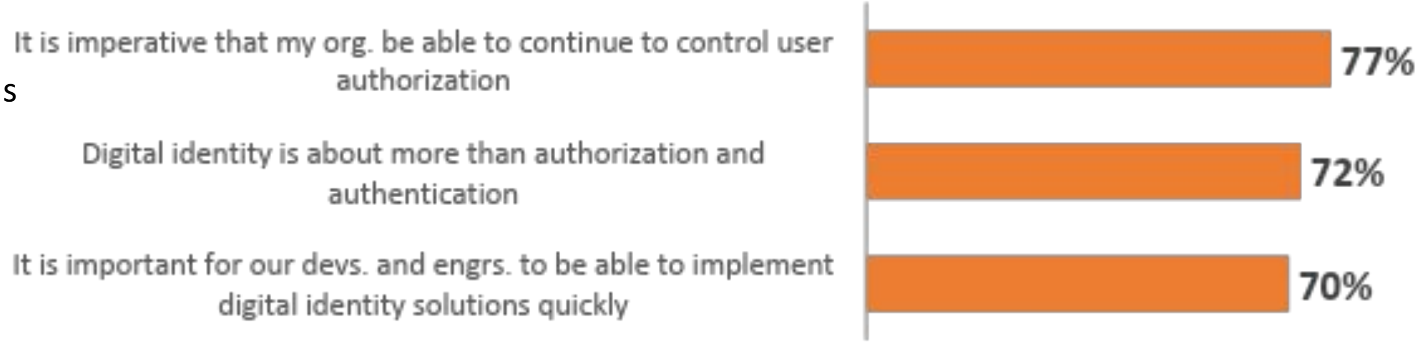
ACTION

- Any marketing and messaging around IAM solutions must address these key areas of concern.

Top Aspects of Implementing Single IAM System



Strongly/Somewhat Agree



Contact Information

Jared Shellaway, *Assistant Vice President, Research Services*

11350 Random Hills Road, Suite 800 Fairfax, VA 22030
jshellaway@govexec.com

Laurie Morrow, *Vice President, Research Strategy*

11350 Random Hills Road, Suite 800 Fairfax, VA 22030
lmorrow@govexec.com

Aaron Heffron, *Executive Vice President*

11350 Random Hills Road, Suite 800 Fairfax, VA 22030
aheffron@govexec.com

Market Connections®
Research you can act on.

Appendix

Respondent Classifications: Years Served

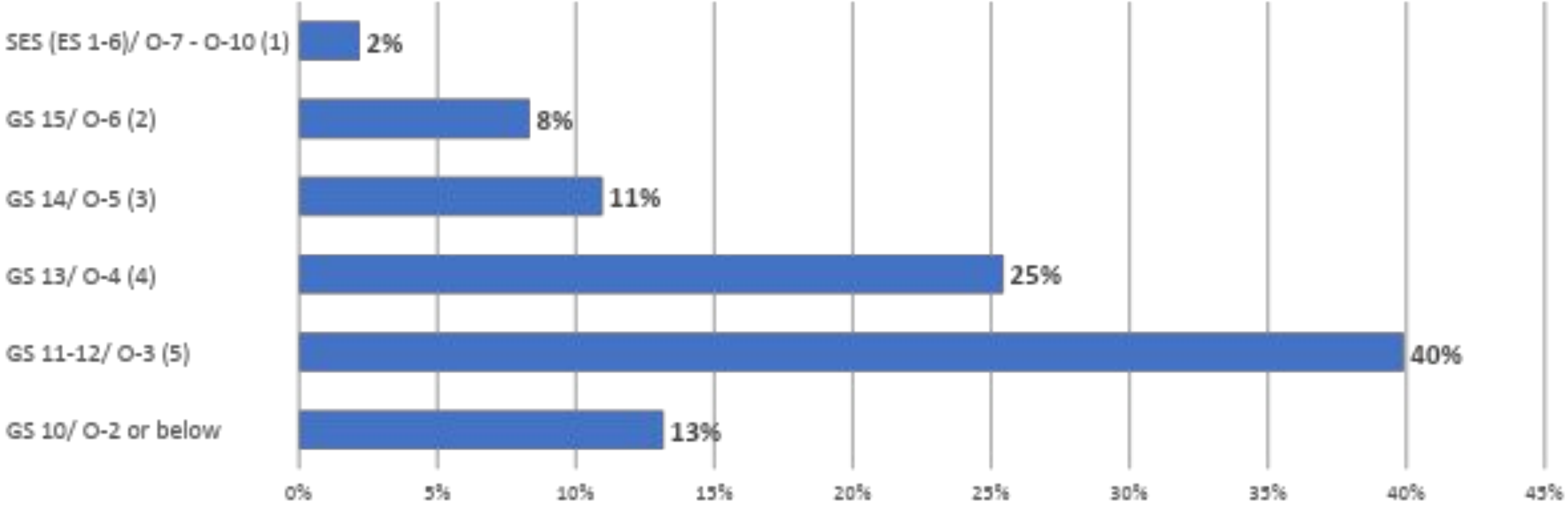
Six in ten respondents have served at least six years.

	Total	🇺🇸	🇬🇧	🇳🇿
Less than 1 year	4%	5%	3%	4%
1-5 years	34%	30%	40%	36%
6-10 years	36%	31%	40%	40%
11-15 years	15%	15%	15%	15%
16-19 years	6%	8%	3%	4%
20+ years	5%	11%	1%	1%

Q *How many years in total have you served as a government employee? (Include military service, if applicable.)*

Pay Grade/Level: U

Nearly half of US Federal respondents are GS 13 and above.



Q *Please indicate your equivalent federal civilian or military pay grade/level.*