2022 PUBLIC SECTOR IDENTITY INDEX REPORT — GLOBAL REPORT
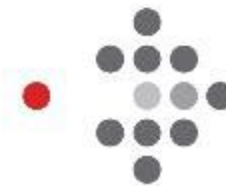
January 2022

Presented to:

okta | ★ **auth0**

Market Connections®
Research you can act on.

Table of Contents

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.

Use Cases

Legend: ■ Total ■ US ■ UK ■ ANZ

	Total	US	UK	ANZ
Employees accessing Enterprise applications	75%	80%	68%	72%
Residents/Citizens accessing applications	66%	65%	64%	68%
External users (contractors, vendors, other government entities)	48%	48%	45%	50%
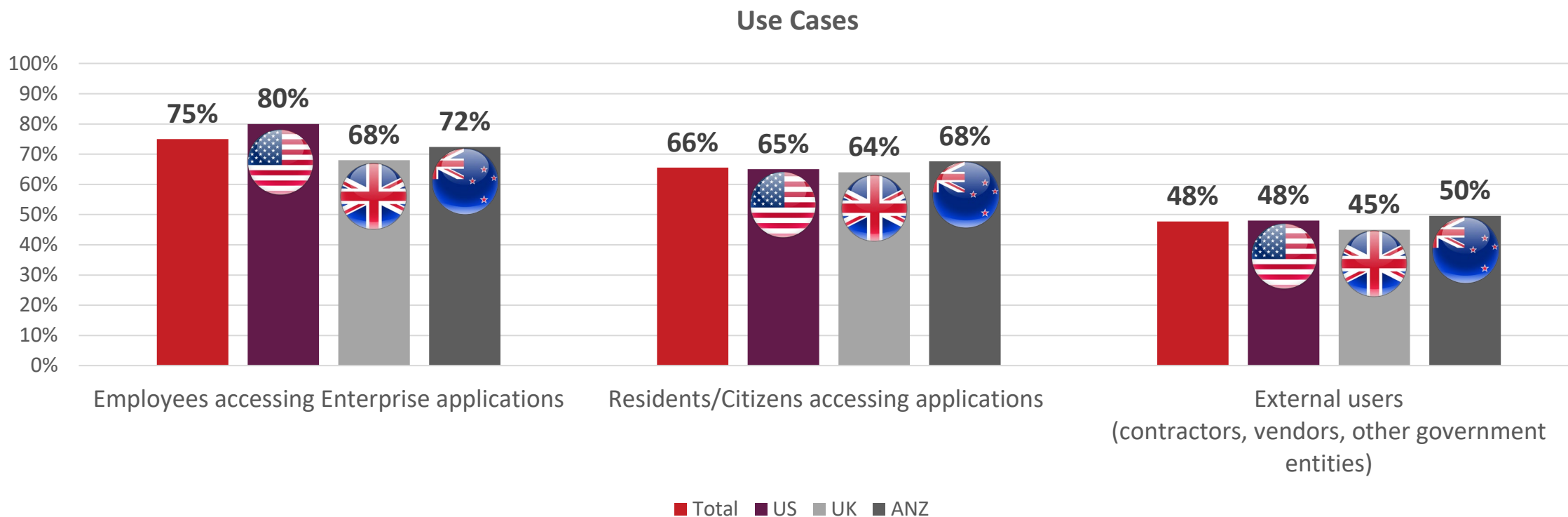
Which of the following use cases are most applicable to your role

Respondent Classifications – Job Role

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

Job Role	Global	🇺🇸 US	🇬🇧 UK	🇳🇿 NZ
Program Management/Execution	27%	23%	32%	30%
IT Administration	25%	30%	15%	26%
IT Engineering	10%	11%	12%	8%
Professional/Technical Services	10%	8%	13%	10%
Purchasing/Contracting	8%	9%	6%	10%
Executive Management	6%	9%	3%	3%
Software developer	5%	2%	8%	6%
Security operations	4%	2%	8%	3%
Information Security	4%	4%	4%	3%
Product Manager	2%	1%	2%	3%
Chief Technology Officer	1%	2%	1%	0%
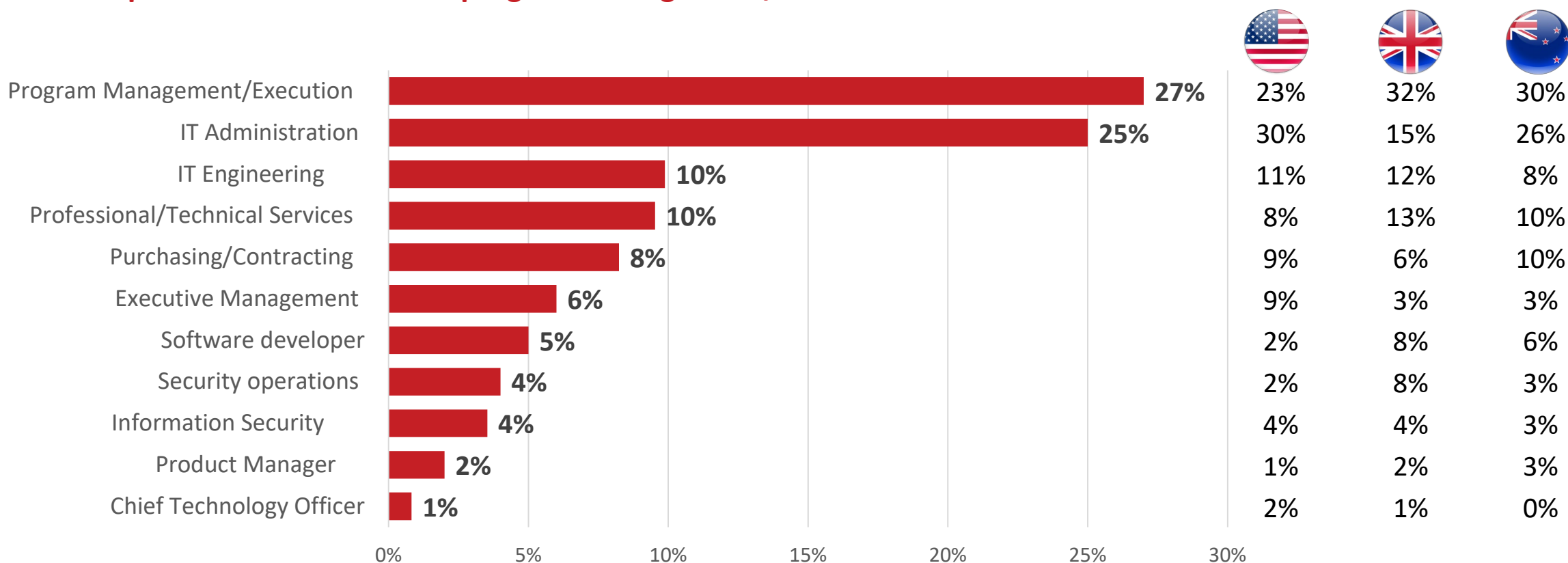
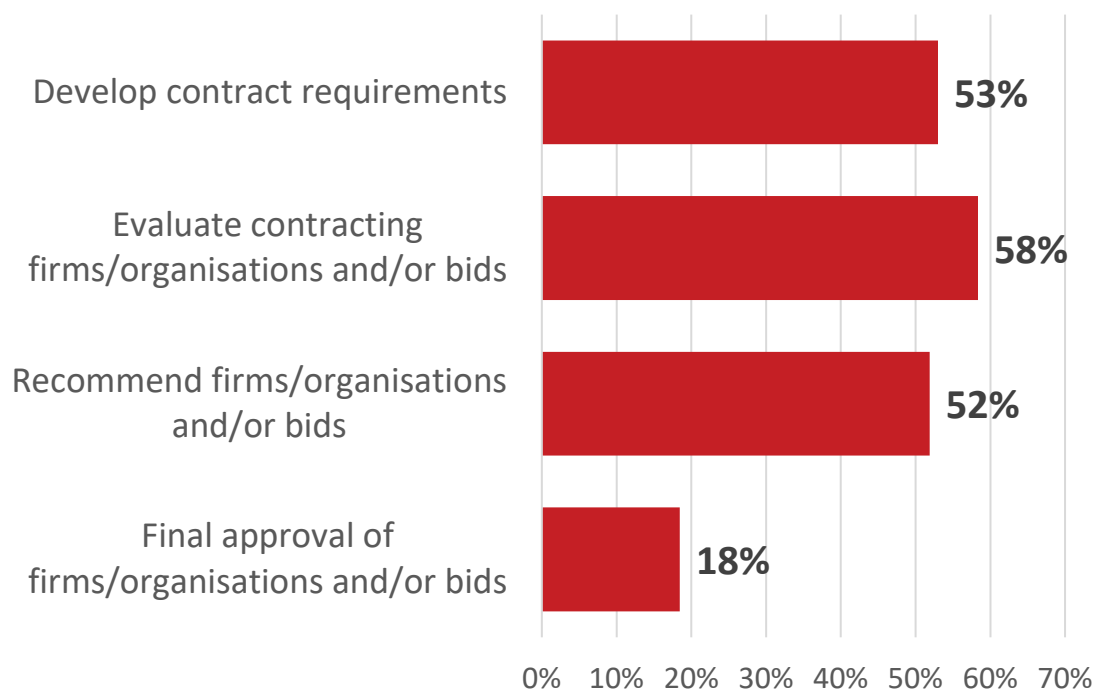*Which of the following best describes your role in your organization?*

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).

Involvement in Selection of Firms

Develop contract requirements	**53%**
Evaluate contracting firms/organisations and/or bids	**58%**
Recommend firms/organisations and/or bids	**52%**
Final approval of firms/organisations and/or bids	**18%**

0% 10% 20% 30% 40% 50% 60% 70%

Involvement in Management of Firms
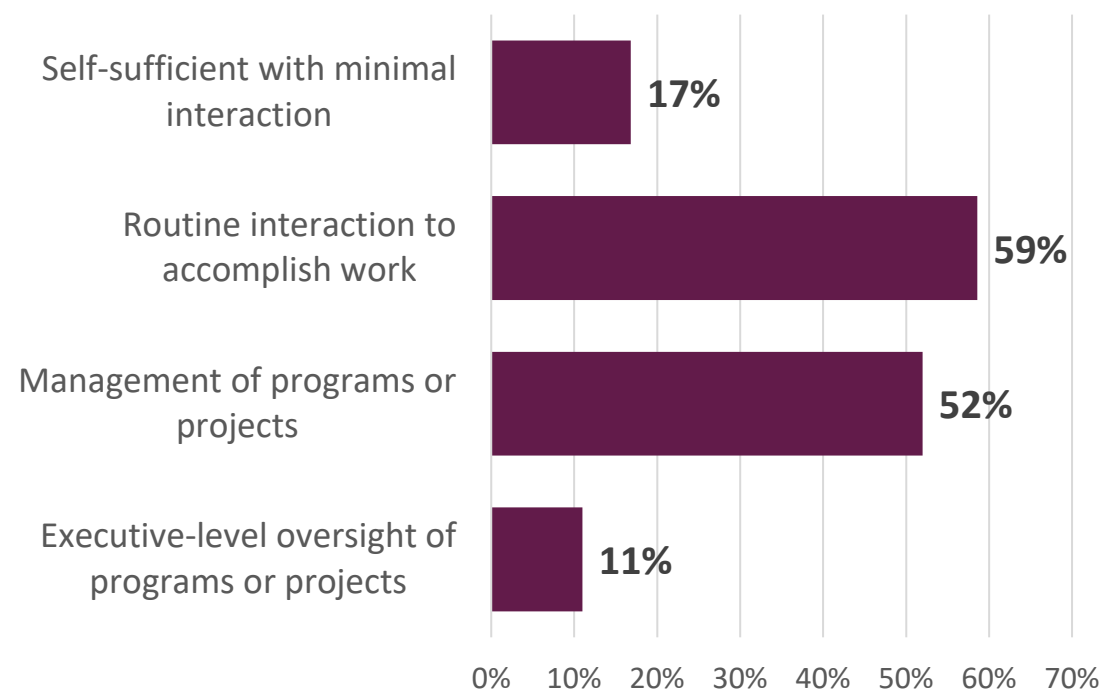
Self-sufficient with minimal interaction	**17%**
Routine interaction to accomplish work	**59%**
Management of programs or projects	**52%**
Executive-level oversight of programs or projects	**11%**

0% 10% 20% 30% 40% 50% 60% 70%

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.

	Know a little	Know quite a bit	I am the resident expert
Total	28%	51%	21%
🇺🇸	28%	51%	21%
🇬🇧	24%	53%	24%
🇳🇿	30%	51%	19%
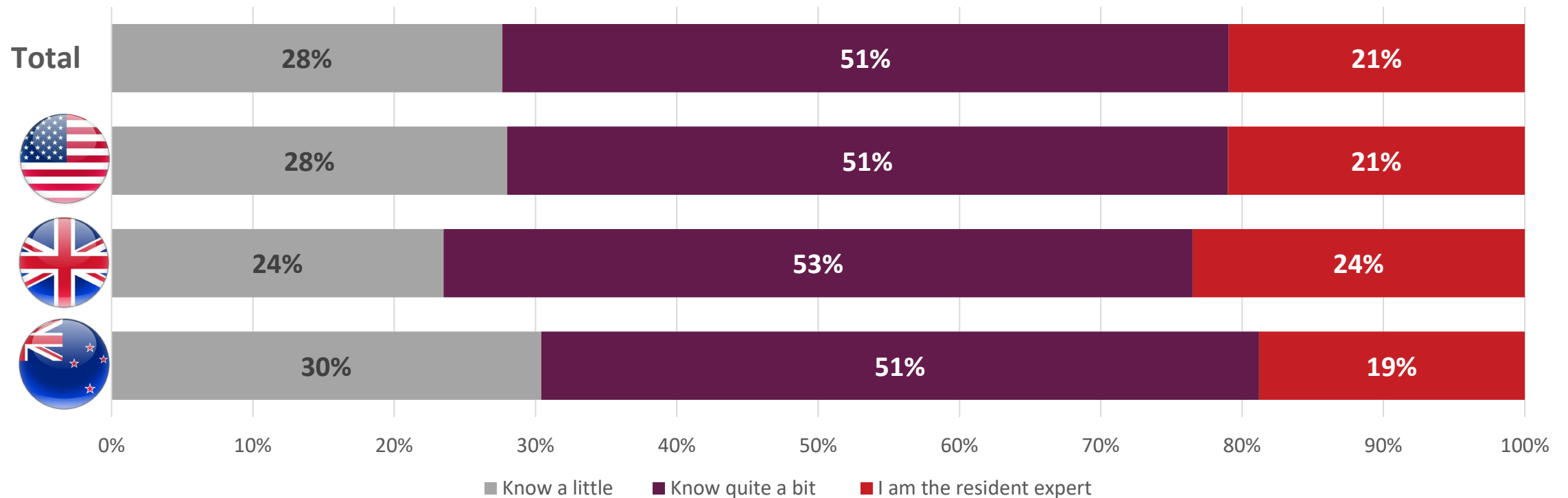
How would you describe your knowledge of your organization's processes around Identity and Access Management (IAM)?

Organization Currently Builds External-Facing Applications

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

Legend: Total | US | UK | ANZ

=statistically significant difference
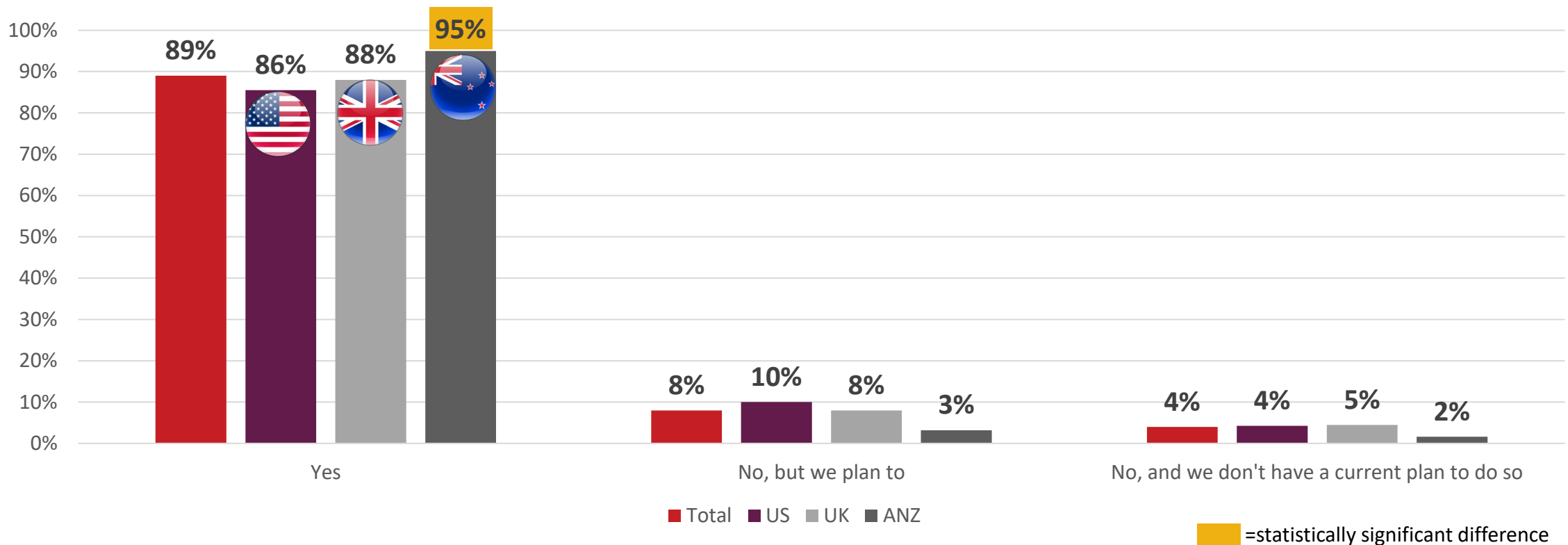
Does your [organization/organisation] currently build external-facing applications?

Digital Services Landscape

Importance of Providing Digital Applications/Services

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

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

Extremely/ Very Important

Total 3% 14% 55% 28% **83%**

🇺🇸 3% 13% 57% 27% **84%**

🇬🇧 5% 17% 52% 27% **79%**

🇳🇿 3% 12% 54% 32% **85%**

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

■ Not at all important ■ Somewhat important ■ Very important ■ Extremely important

█ =statistically significant difference
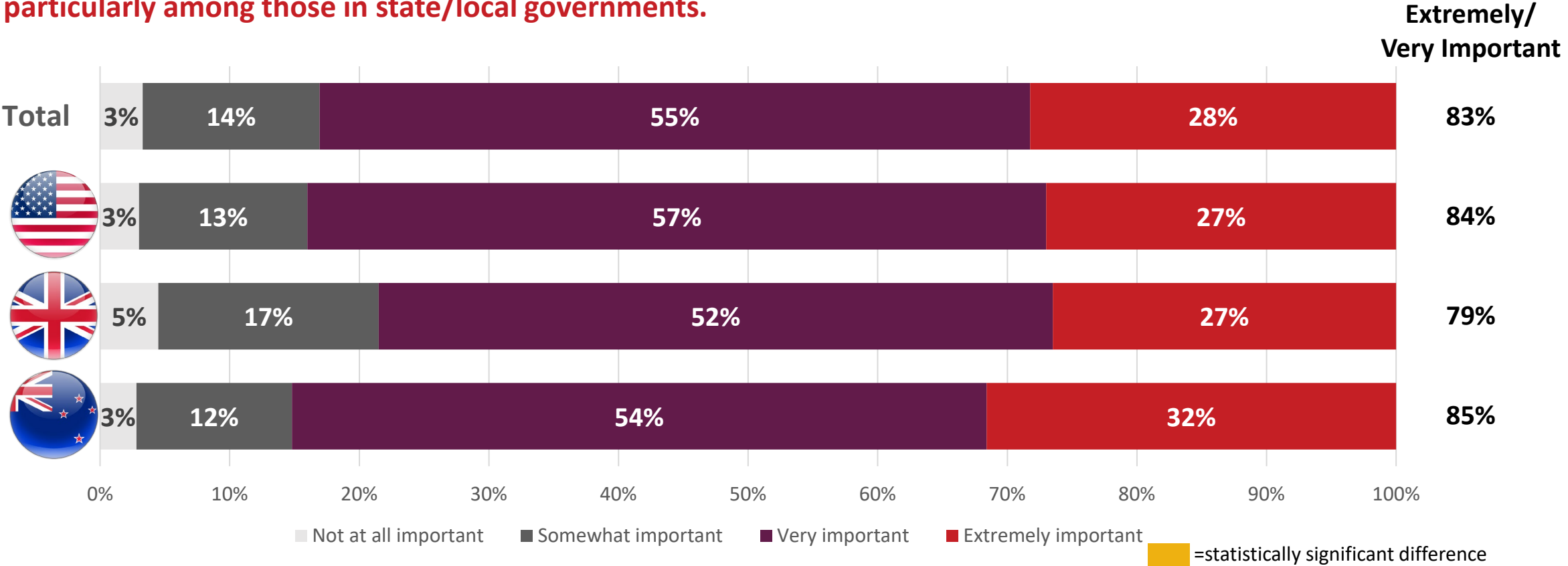
How important is it that your organization has the ability to provide digital applications or services for citizens?

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

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.

	Total	🇺🇸	🇬🇧	🇳🇿
We do not have digital citizen services, and don't plan to implement them in the next 2 years	2%	2%	3%	2%
We do not have digital citizen services, but plan to implement them in the next 2 years	3%	3%	3%	4%
We have some services available digitally and are not looking to expand in the next 2 years	8%	10%	9%	4%
We have some services available digitally and are looking to expand in the next 2 years	75%	73%	78%	78%
We have all our services available digitally	12%	13%	8%	12%

=statistically significant difference

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

	4	5 - Extremely important	Total	🇺🇸	🇬🇧	🇳🇿
Protecting citizens' privacy and data	38%	35%	73%	72%	71%	**78%**
Abiding by specific government rules for data security	37%	35%	72%	**73%**	65%	**78%**
Overall accessibility of services	41%	30%	71%	71%	68%	74%
Securing digital citizen services	39%	32%	71%	**72%**	62%	**76%**
Ensuring citizens' trust in digital services	39%	31%	70%	**71%**	63%	**74%**
Minimizing friction for the customer	43%	28%	70%	**70%**	62%	**78%**
Accessibility of services via mobile	45%	25%	70%	67%	72%	**74%**
Balancing security with user experience	41%	28%	69%	67%	66%	**74%**
Accessibility of services via computer	37%	32%	69%	70%	67%	69%
Improving existing services	46%	23%	69%	70%	65%	70%
Improving the user experience	44%	24%	68%	68%	64%	72%
Building services that can adapt to how users change	44%	21%	66%	65%	68%	64%
Cost reduction via process automation	39%	24%	64%	65%	60%	65%
Managing partners across the entirety of a project	40%	23%	63%	62%	60%	68%
Speed in adding new services	40%	23%	63%	62%	66%	62%
Increased participation in government	41%	22%	62%	65%	62%	59%

■ 4   ■ 5 - Extremely important   ▇ =statistically significant difference

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

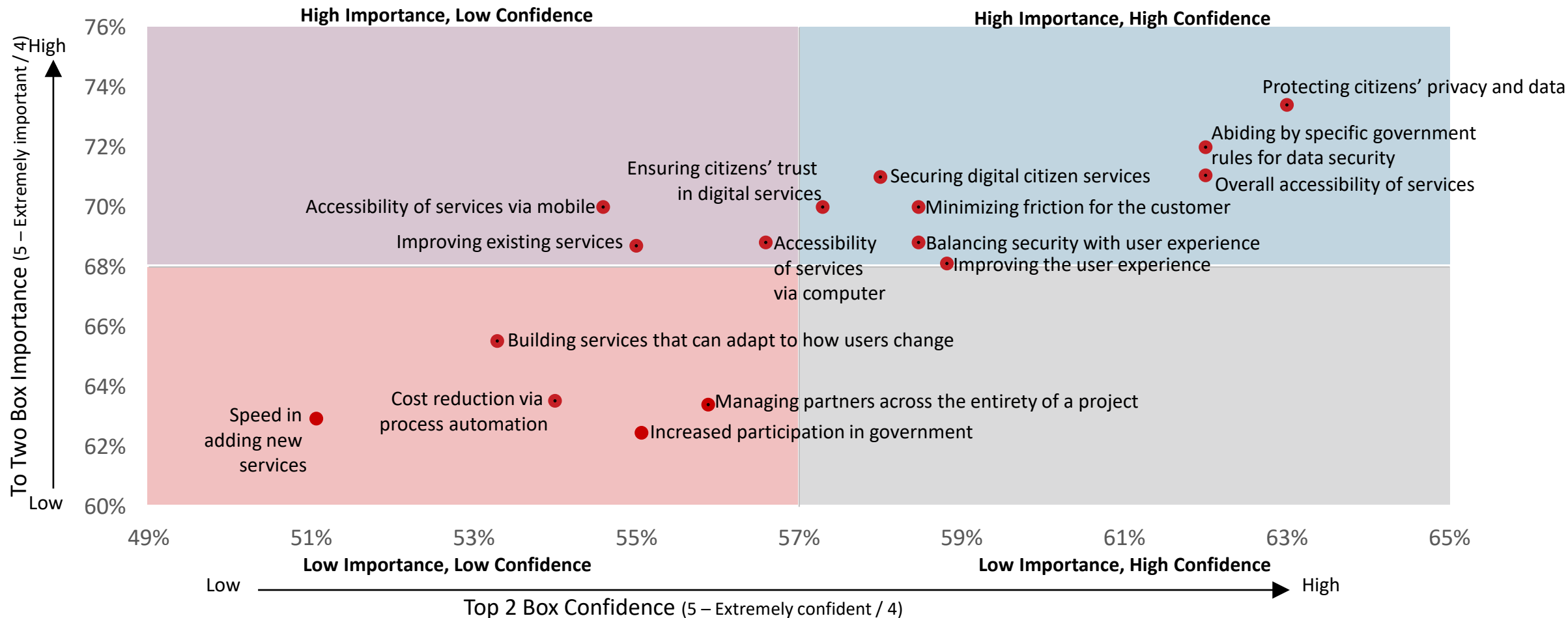|	4	5 - Extremely confident	Total	🇺🇸	🇬🇧	🇳🇿
Protecting citizens' privacy and data	43%	20%	63%	65%	54%	66%
Abiding by specific government rules for data security	39%	24%	62%	63%	56%	67%
Overall accessibility of services	43%	19%	62%	58%	60%	70%
Improving the user experience	43%	16%	59%	60%	57%	60%
Balancing security with user experience	39%	19%	58%	58%	54%	63%
Minimizing friction for the customer	40%	18%	58%	58%	54%	63%
Securing digital citizen services	39%	19%	58%	59%	52%	61%
Ensuring citizens' trust in digital services	38%	19%	57%	56%	53%	62%
Accessibility of services via computer	36%	20%	57%	57%	56%	56%
Managing partners across the entirety of a project	39%	17%	56%	54%	55%	59%
Increased participation in government	38%	17%	55%	55%	53%	58%
Improving existing services	37%	18%	55%	55%	48%	62%
Accessibility of services via mobile	38%	16%	55%	54%	53%	57%
Cost reduction via process automation	38%	16%	54%	53%	48%	60%
Building services that can adapt to how users change	37%	16%	53%	53%	54%	53%
Speed in adding new services	34%	17%	51%	54%	48%	49%

0% 10% 20% 30% 40% 50% 60% 70%

🟥 4 🟪 5 - Extremely confident

🟧 =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?
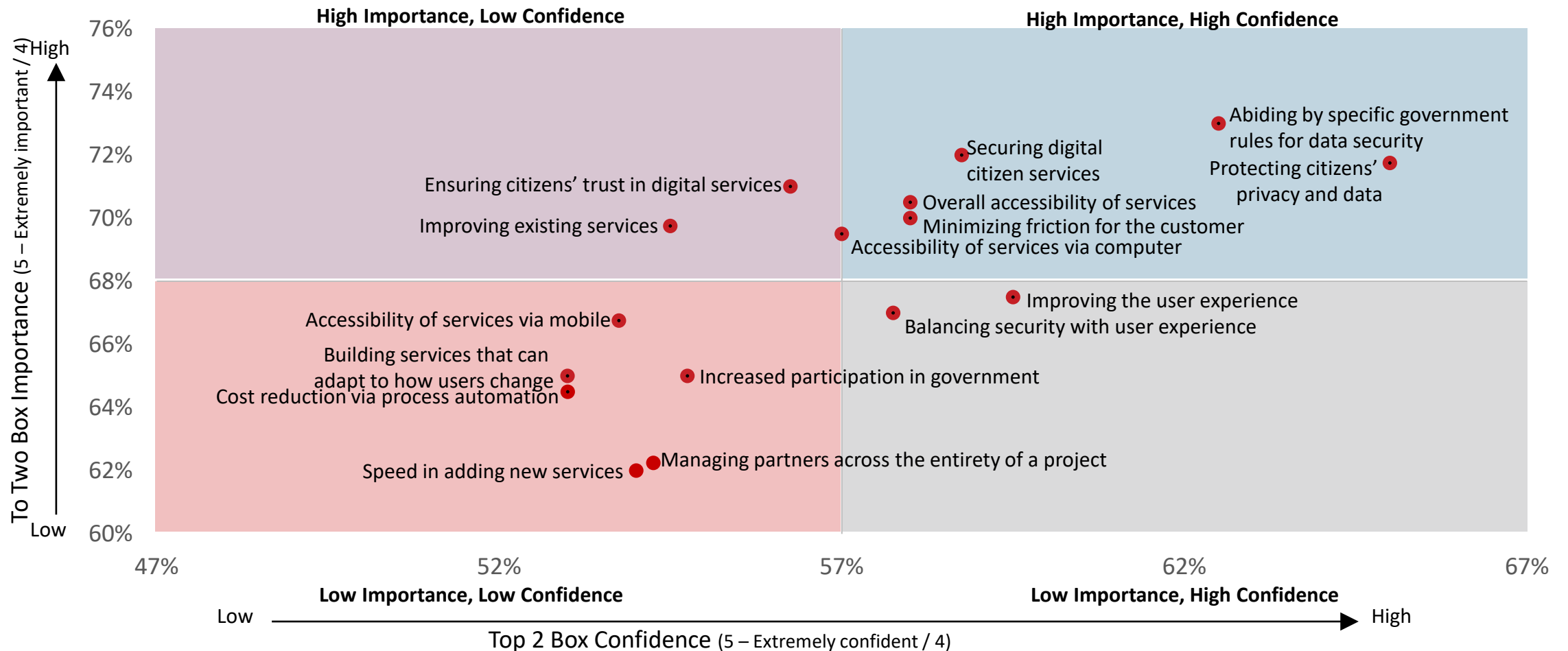
Importance/Confidence: Total

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

Chart: Scatter plot of Top 2 Box Confidence (x-axis, 49%–65%) vs. To Two Box Importance (y-axis, 60%–76%).

Quadrant labels:
- High Importance, Low Confidence (top-left)
- High Importance, High Confidence (top-right)
- Low Importance, Low Confidence (bottom-left)
- Low Importance, High Confidence (bottom-right)

Data points:
- Protecting citizens' privacy and data
- Abiding by specific government rules for data security
- Overall accessibility of services
- Securing digital citizen services
- Ensuring citizens' trust in digital services
- Minimizing friction for the customer
- Accessibility of services via mobile
- Balancing security with user experience
- Improving existing services
- Accessibility of services via computer
- Improving the user experience
- Building services that can adapt to how users change
- Cost reduction via process automation
- Managing partners across the entirety of a project
- Speed in adding new services
- Increased participation in government

Y-axis label: To Two Box Importance (5 – Extremely important / 4); High at top, Low at bottom

X-axis label: Top 2 Box Confidence (5 – Extremely confident / 4); Low at left, High at right
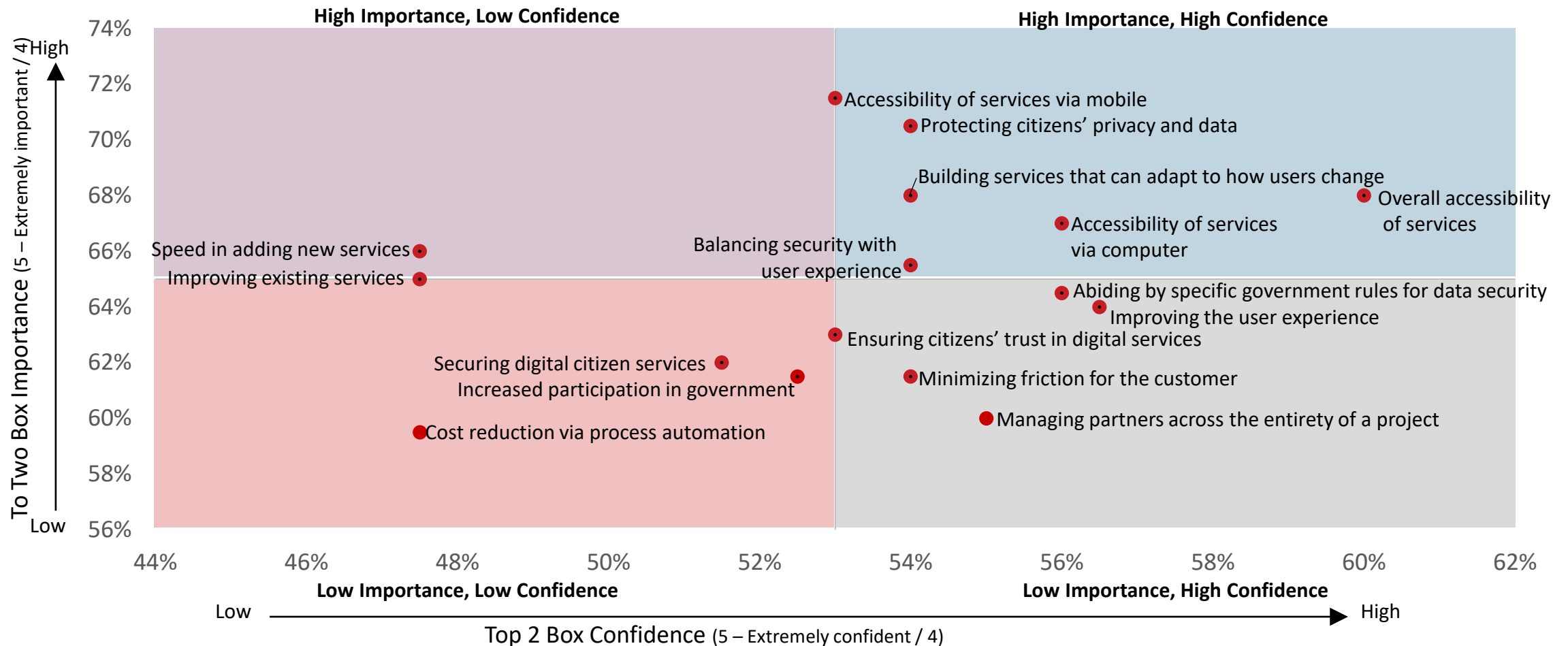
Importance/Confidence: US 🇺🇸

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

High Importance, Low Confidence   **High Importance, High Confidence**

- Abiding by specific government rules for data security
- Protecting citizens' privacy and data
- Securing digital citizen services
- Ensuring citizens' trust in digital services
- Overall accessibility of services
- Minimizing friction for the customer
- Improving existing services
- Accessibility of services via computer
- Improving the user experience
- Balancing security with user experience
- Accessibility of services via mobile
- Building services that can adapt to how users change
- Cost reduction via process automation
- Increased participation in government
- Speed in adding new services
- Managing partners across the entirety of a project

Low Importance, Low Confidence   **Low Importance, High Confidence**

Y-axis: To Two Box Importance (5 – Extremely important / 4) — 60%, 62%, 64%, 66%, 68%, 70%, 72%, 74%, 76% — Low to High

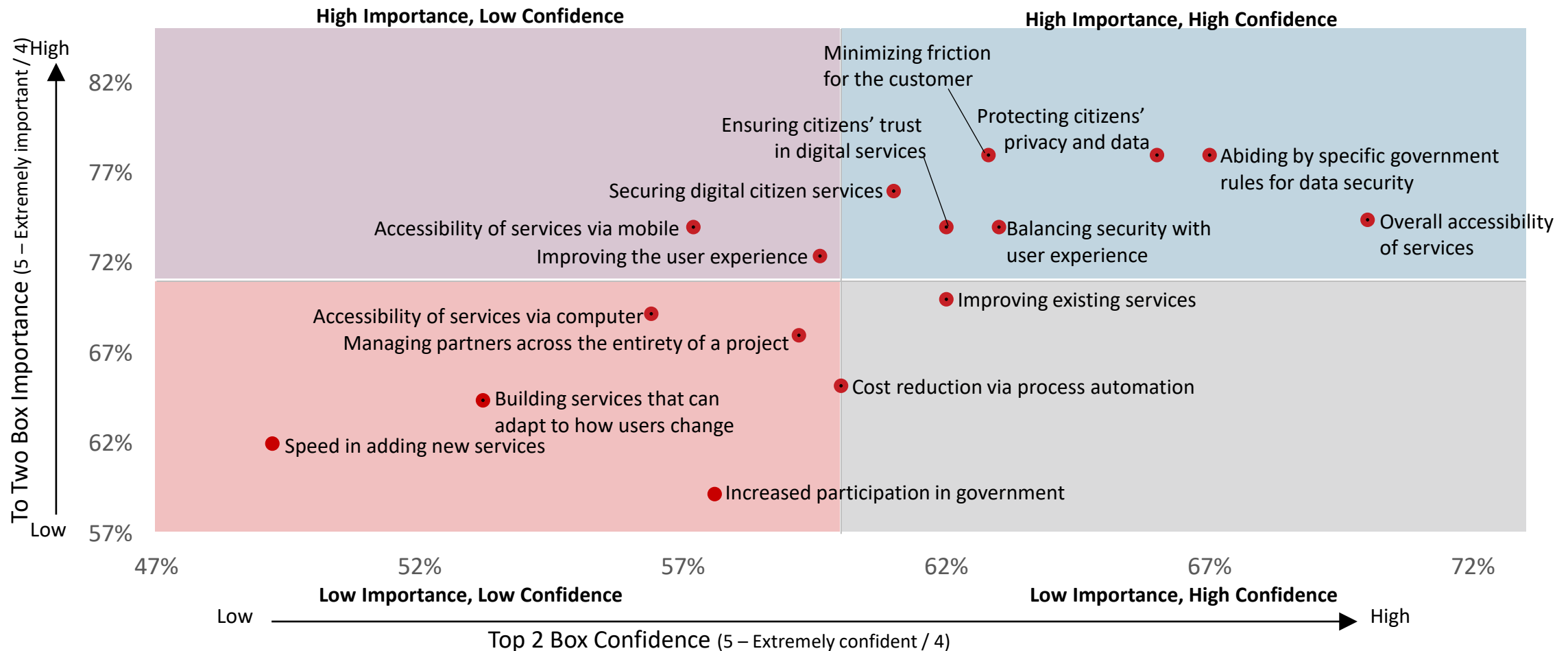X-axis: Top 2 Box Confidence (5 – Extremely confident / 4) — 47%, 52%, 57%, 62%, 67% — Low to High

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.
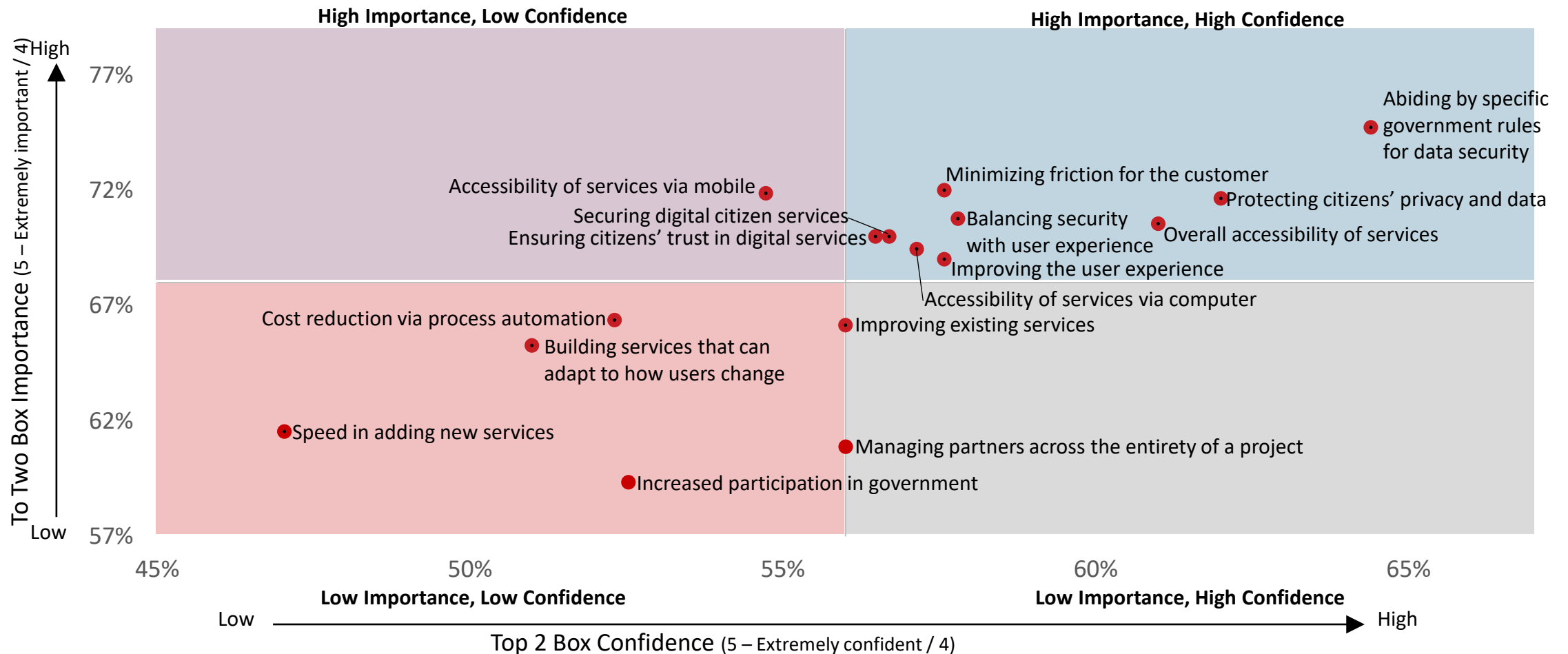

High Importance, Low Confidence

High Importance, High Confidence

- Accessibility of services via mobile
- Protecting citizens' privacy and data
- Building services that can adapt to how users change
- Overall accessibility of services
- Accessibility of services via computer
- Speed in adding new services
- Improving existing services
- Balancing security with user experience
- Abiding by specific government rules for data security
- Improving the user experience
- Ensuring citizens' trust in digital services
- Securing digital citizen services
- Increased participation in government
- Minimizing friction for the customer
- Cost reduction via process automation
- Managing partners across the entirety of a project

To Two Box Importance (5 – Extremely important / 4)

Low Importance, Low Confidence

Low Importance, High Confidence

Top 2 Box Confidence (5 – Extremely confident / 4)

Importance/Confidence: ANZ

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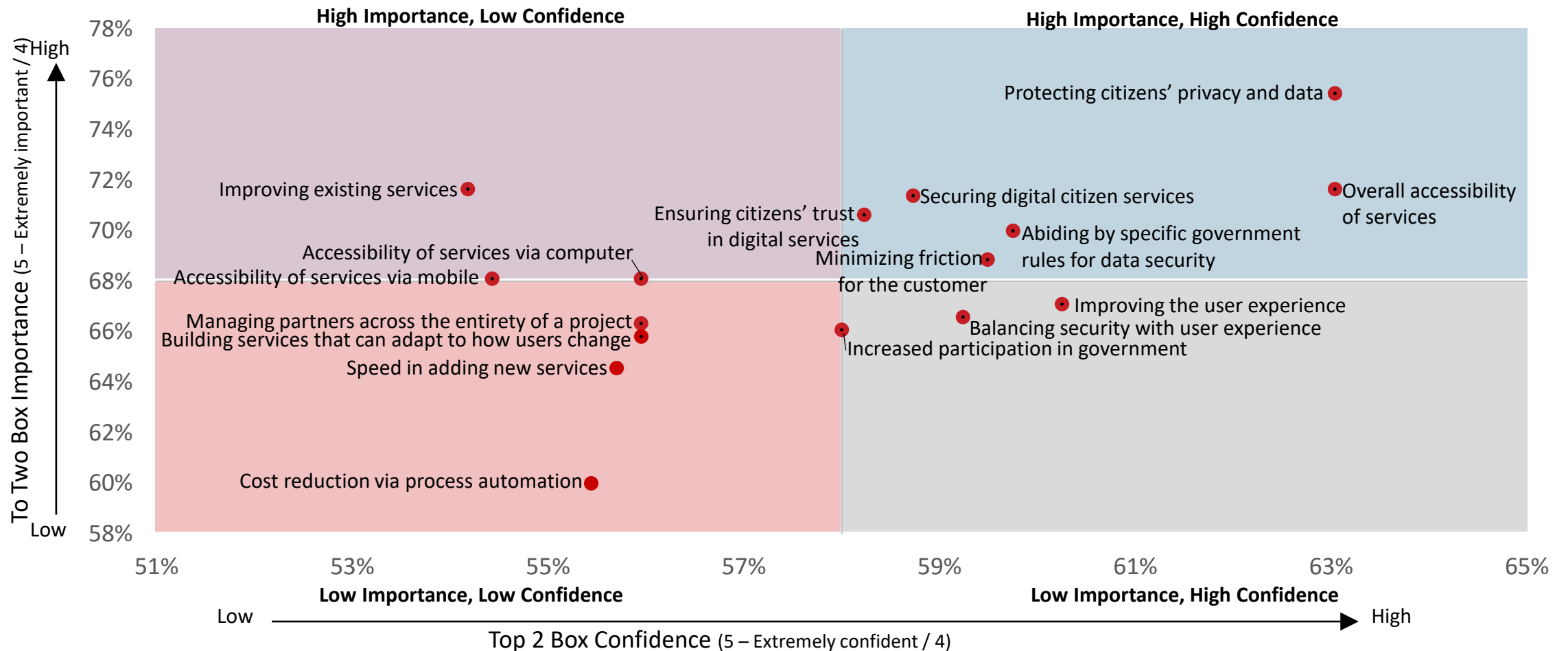

High Importance, Low Confidence

High Importance, High Confidence

To Two Box Importance (5 – Extremely important / 4)

- Minimizing friction for the customer
- Ensuring citizens' trust in digital services
- Protecting citizens' privacy and data
- Abiding by specific government rules for data security
- Securing digital citizen services
- Accessibility of services via mobile
- Balancing security with user experience
- Overall accessibility of services
- Improving the user experience
- Accessibility of services via computer
- Improving existing services
- Managing partners across the entirety of a project
- Cost reduction via process automation
- Building services that can adapt to how users change
- Speed in adding new services
- Increased participation in government

Low Importance, Low Confidence

Low Importance, High Confidence

Top 2 Box Confidence (5 – Extremely confident / 4)

Importance/Confidence: National/Federal

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

Scatter plot titled with axes: Y-axis "To Two Box Importance (5 – Extremely important / 4)" ranging from Low (57%) to High; X-axis "Top 2 Box Confidence (5 – Extremely confident / 4)" ranging from Low (45%) to High (65%).

Quadrant labels:
- High Importance, Low Confidence
- High Importance, High Confidence
- Low Importance, Low Confidence
- Low Importance, High Confidence

Y-axis gridlines: 77%, 72%, 67%, 62%, 57%
X-axis gridlines: 45%, 50%, 55%, 60%, 65%

Data points:
- Abiding by specific government rules for data security
- Minimizing friction for the customer
- Accessibility of services via mobile
- Protecting citizens' privacy and data
- Securing digital citizen services
- Balancing security with user experience
- Ensuring citizens' trust in digital services
- Overall accessibility of services
- Improving the user experience
- Accessibility of services via computer
- Cost reduction via process automation
- Improving existing services
- Building services that can adapt to how users change
- Speed in adding new services
- Managing partners across the entirety of a project
- Increased participation in government

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.

Scatter plot titled with axes "Top 2 Box Confidence (5 – Extremely confident / 4)" on the x-axis (Low 51% to High 65%) and "To Two Box Importance (5 – Extremely important / 4)" on the y-axis (Low 58% to High 78%).

Quadrant labels:
- High Importance, Low Confidence
- High Importance, High Confidence
- Low Importance, Low Confidence
- Low Importance, High Confidence

Data points:
- Protecting citizens' privacy and data
- Overall accessibility of services
- Improving existing services
- Securing digital citizen services
- Ensuring citizens' trust in digital services
- Abiding by specific government rules for data security
- Accessibility of services via computer
- Accessibility of services via mobile
- Minimizing friction for the customer
- Improving the user experience
- Managing partners across the entirety of a project
- Building services that can adapt to how users change
- Balancing security with user experience
- Increased participation in government
- Speed in adding new services
- Cost reduction via process automation

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.

Legend: ■ Total ■ US ■ UK ■ ANZ   🟨 =statistically significant difference
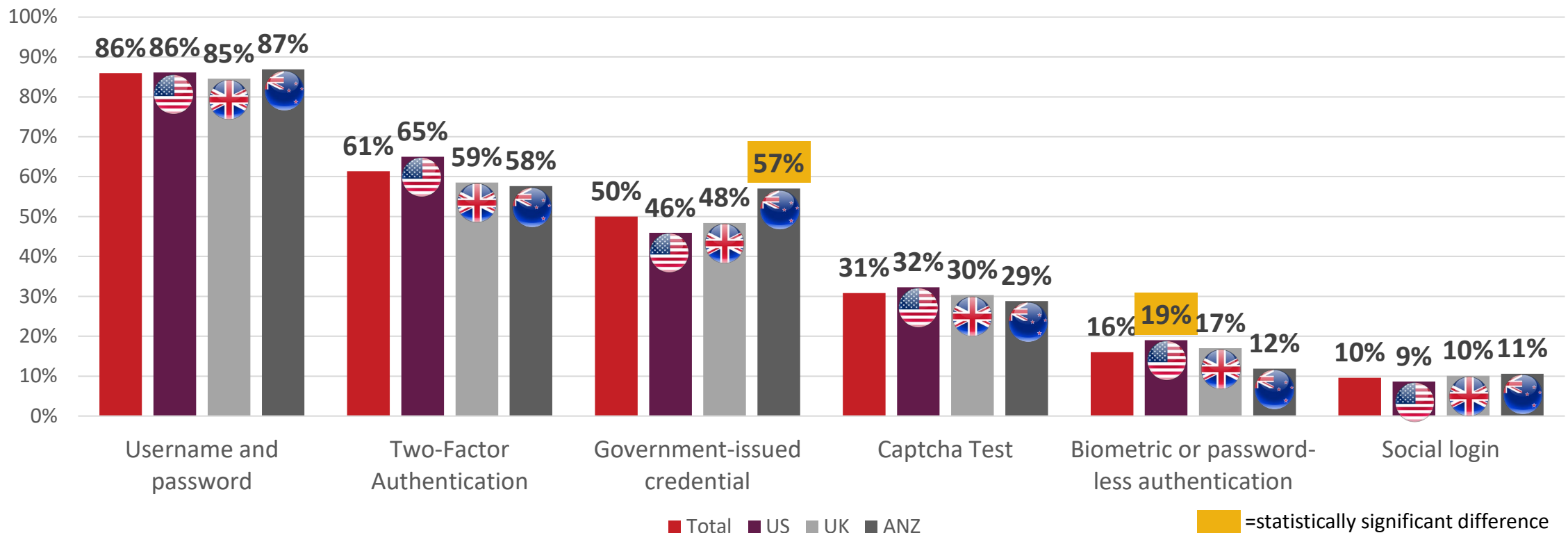
Which authentication method are citizens currently using to access your digital applications or services? Select all that apply

Method	Total	US	UK	ANZ
Username and password	86%	86%	85%	87%
Two-Factor Authentication	61%	65%	59%	58%
Government-issued credential	50%	46%	48%	57%
Captcha Test	31%	32%	30%	29%
Biometric or password-less authentication	16%	19%	17%	12%
Social login	10%	9%	10%	11%

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.

Total   US   UK   ANZ   =statistically significant difference
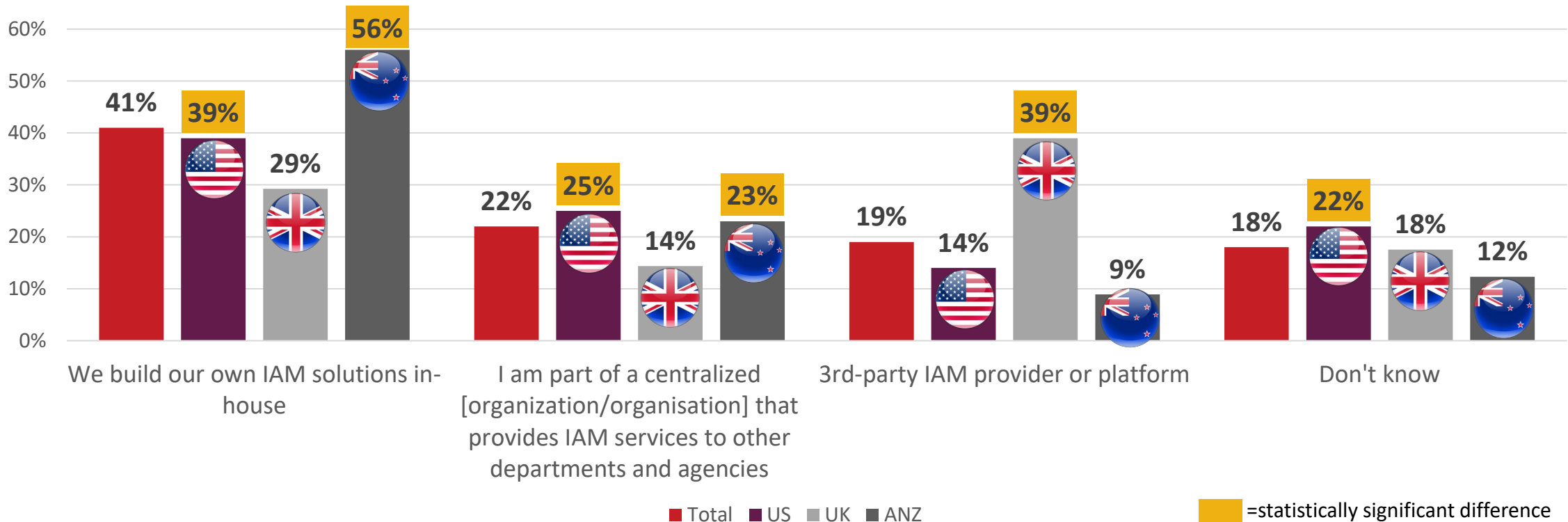
Who currently provides Identity and Access Management (IAM) services for your [organization's/organisation's]?

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

	4	5 - A very big problem	Total	🇺🇸	🇬🇧	🇳🇿
It is costly to tie up our IT resources with IAM	35%	11%	46%	47%	40%	52%
Speed to implementation has been very slow	31%	15%	46%	45%	40%	52%
We don't have enough staff/resources to manage this internally	28%	18%	45%	46%	41%	48%
The solutions we have are not compatible with all our…	32%	10%	43%	41%	35%	51%
We don't have the resources to adapt to each of our…	32%	10%	42%	41%	45%	40%
Our current solutions are not scalable	31%	10%	41%	44%	32%	44%
We don't have the expertise to manage this internally	27%	11%	39%	37%	35%	44%

■ 4 ■ 5 - A very big problem

=statistically significant difference

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 Solution

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	🇺🇸	🇬🇧	🇳🇿
Security	64%	63%	59%	69%
Ease of use	60%	58%	50%	70%

Security: 5% | 31% | 46% | 17%

Ease of use: 8% | 32% | 41% | 19%

Legend:
- 1 - Not at all confident/2
- 3
- 4
- 5 - Extremely confident

=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%

5 – Extremely important/4

	1 - Not at all important/2	3	4	5 - Extremely important	
Total	4%	32%	42%	22%	64%
🇺🇸	5%	32%	43%	21%	64%
🇬🇧	4%	35%	41%	21%	62%
🇳🇿	2%	31%	43%	24%	67%

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

■ 1 - Not at all important/2   ■ 3   ■ 4   ■ 5 - Extremely important
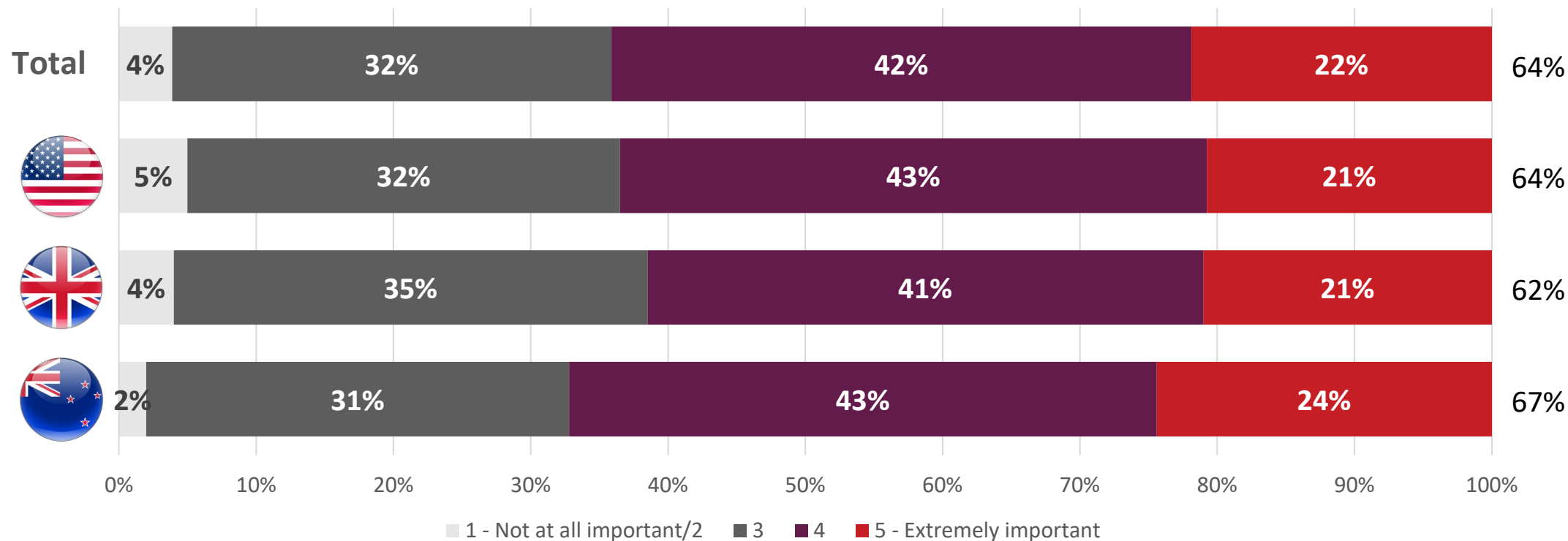
How important is it to your [organization/organisation] to have one digital credential for authentication and authorization across all your services? By this we mean enabling users to securely authenticate with multiple applications using a single set of credentials (username and password)

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.

53%	**53%**	**55%**	**53%**
0% **Total** 100%	0% 🇺🇸 100%	0% 🇬🇧 100%	0% 🇳🇿 100%
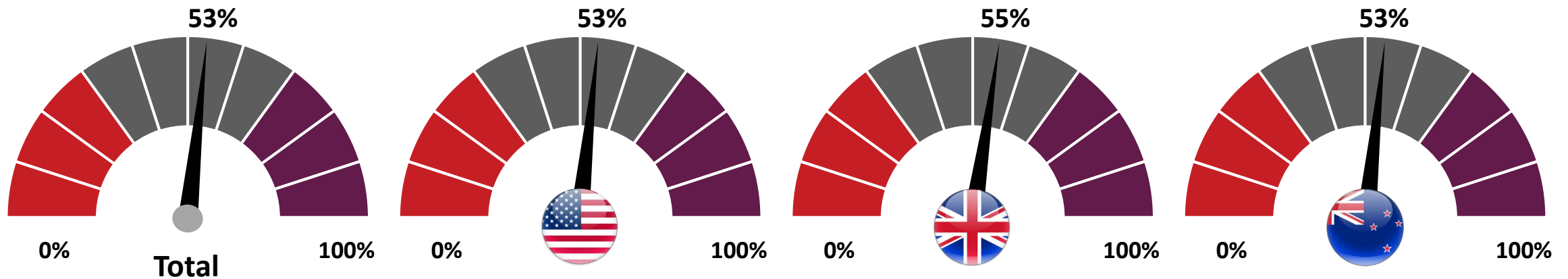
Across what percentage of your services do you currently have a single digital credential for access?

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	🇺🇸	🇬🇧	🇳🇿
Adhering to government compliance rules and regulations	73%	74%	65%	78%
Having consistent login/sign-up experience across all apps	73%	73%	68%	76%
Ensuring data security and privacy	72%	71%	68%	78%
Maintaining user exp. while ensuring data privacy and…	72%	72%	73%	71%
Maintaining centralized control over user authorization	72%	74%	67%	73%
Interoperability with all our systems	72%	71%	69%	74%
Allowing users to interact with govt services similarly to retail	70%	70%	67%	74%
Interoperability with legacy systems	70%	70%	63%	76%
Framework that allows adapting solutions in stages	69%	73%	65%	66%
Using existing databases rather than migrating	69%	67%	65%	76%
Solutions having no negative impact on the end-user	69%	72%	61%	72%
Customizable to different applications	69%	70%	63%	71%
Ease of integration with legacy systems	69%	72%	58%	74%
Simple user experience	69%	70%	64%	71%
Solutions that work with any app and any environment	68%	66%	68%	72%
Reducing vendor lock-in	66%	67%	66%	65%
Having a single view of the customer	66%	67%	60%	71%
Speed of implementation	66%	65%	63%	71%
Pre-built solutions	58%	62%	58%	51%

Chart (stacked bars, 4 / 5 - Extremely important):
- Adhering to government compliance rules and regulations: 39% | 34%
- Having consistent login/sign-up experience across all apps: 47% | 26%
- Ensuring data security and privacy: 38% | 34%
- Maintaining user exp. while ensuring data privacy and…: 39% | 33%
- Maintaining centralized control over user authorization: 46% | 26%
- Interoperability with all our systems: 42% | 30%
- Allowing users to interact with govt services similarly to retail: 47% | 23%
- Interoperability with legacy systems: 42% | 28%
- Framework that allows adapting solutions in stages: 45% | 24%
- Using existing databases rather than migrating: 45% | 24%
- Solutions having no negative impact on the end-user: 44% | 24%
- Customizable to different applications: 46% | 23%
- Ease of integration with legacy systems: 46% | 23%
- Simple user experience: 41% | 28%
- Solutions that work with any app and any environment: 45% | 23%
- Reducing vendor lock-in: 44% | 22%
- Having a single view of the customer: 42% | 24%
- Speed of implementation: 42% | 24%
- Pre-built solutions: 38% | 20%

0% 10% 20% 30% 40% 50% 60% 70% 80%

■ 4   ■ 5 - Extremely important

■ =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?

2022 PUBLIC SECTOR IDENTITY INDEX REPORT — GLOBAL REPORT | MARKET CONNECTIONS, INC. | 703.378.2025

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%

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

Method	Percentage
Username and password	86%
Two-Factor Authentication	61%
Government-issued credential	50%
Captcha Test	31%
Biometric or password-less authentication	16%
Social login	10%
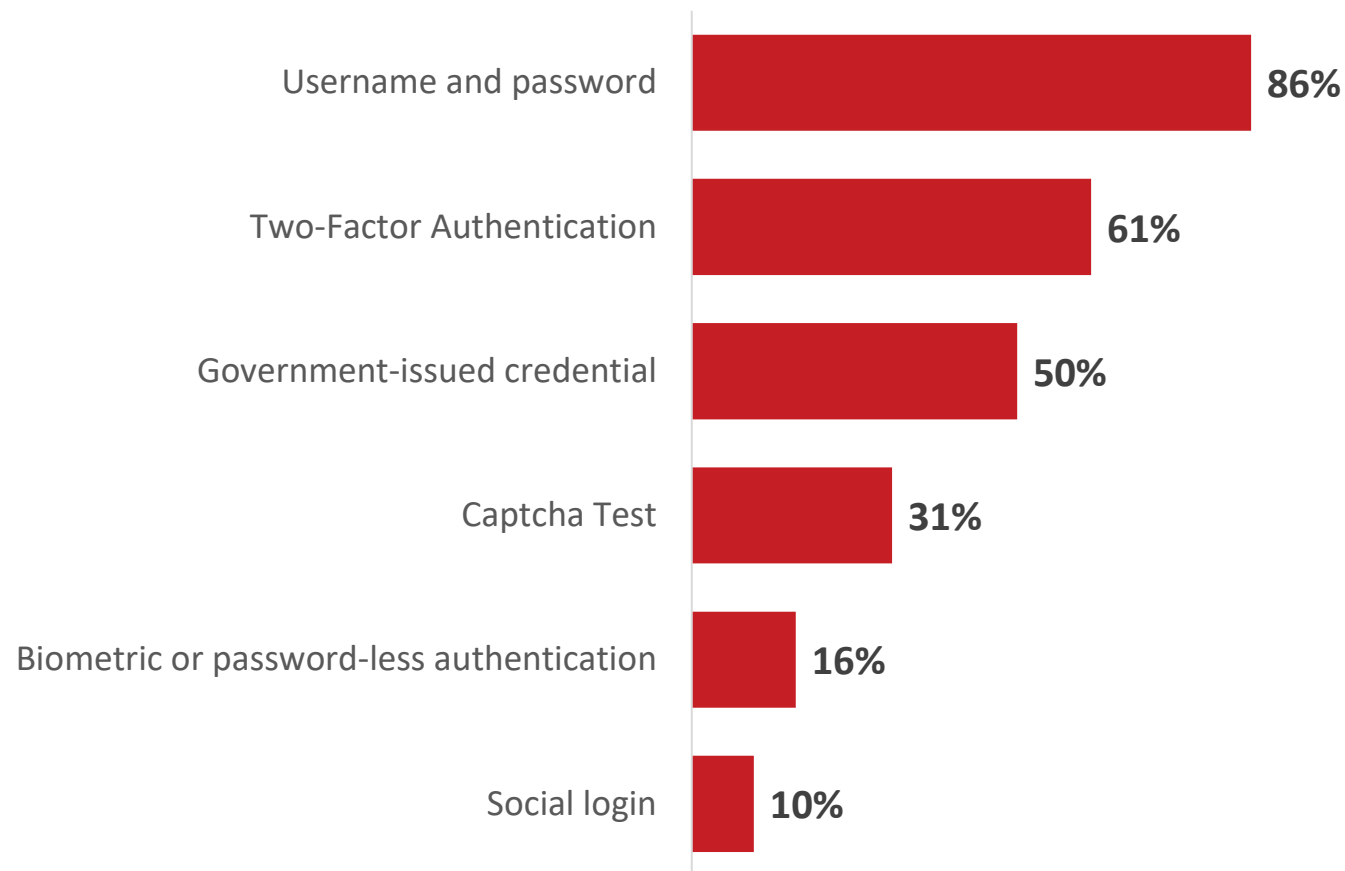
KEY TAKEAWAY

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

We have some services available digitally and are looking to expand in the next 2 years	75%
We have all our services available digitally	12%

Who Provides IAM Services

We build our own IAM solutions in-house	41%
Centralized organization that provides IAM services to other departments and agencies	22%
3rd-party IAM provider or platform	19%
Don't know	18%
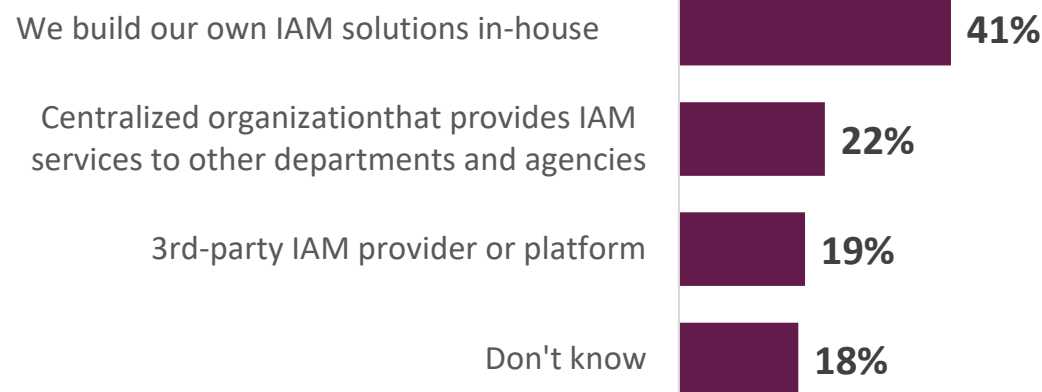
KEY TAKEAWAY

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

5 - A very big problem/4/3

Pain Point	%
Speed to implementation has been very slow	83%
We don't have enough staff/resources to manage this internally	82%
The solutions we have are not compatible with all our applications	82%
We don't have the resources to adapt to each of our applications	81%
It is costly to tie up our IT resources with IAM	80%
Our current solutions are not scalable	78%
We don't have the expertise to manage this internally	78%

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
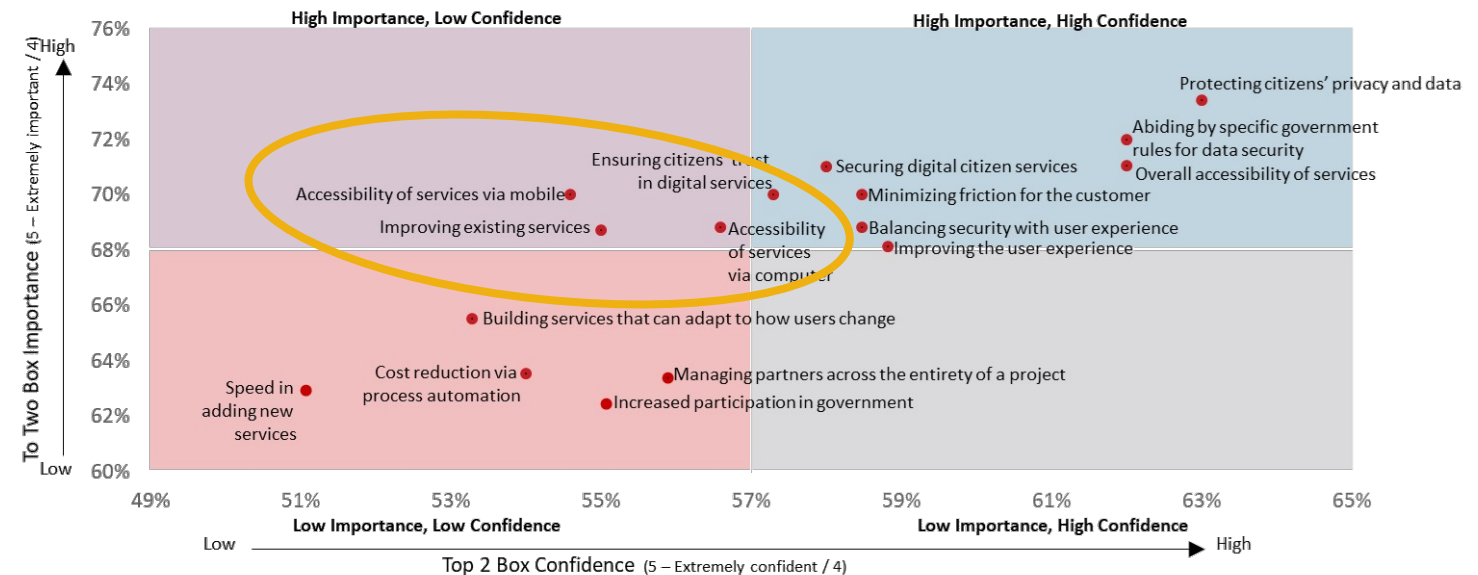
KEY TAKEAWAY

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

Total	4%	32%	42%	22%

Legend: ▢ 1 - Not at all important/2 ▪ 3 ▪ 4 ▪ 5 - Extremely important

% of Services Having a Single Digital Credential

53%

0%   Total   100%
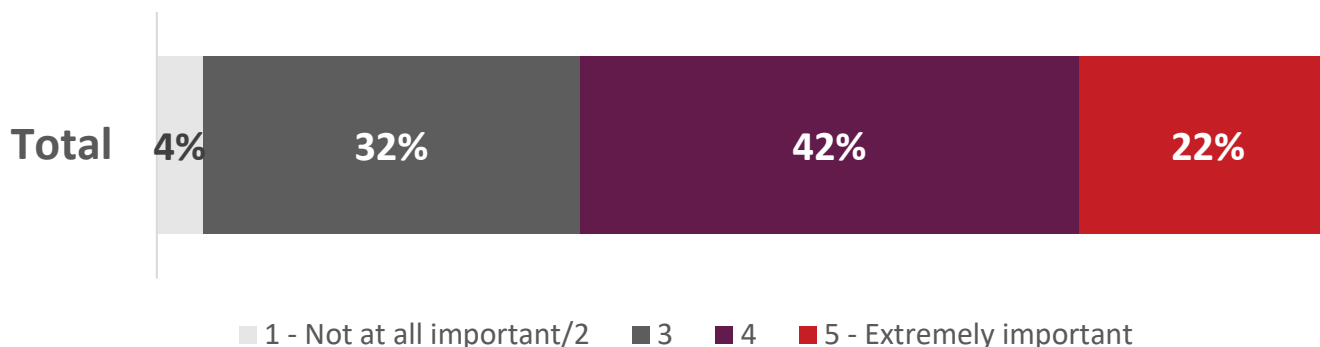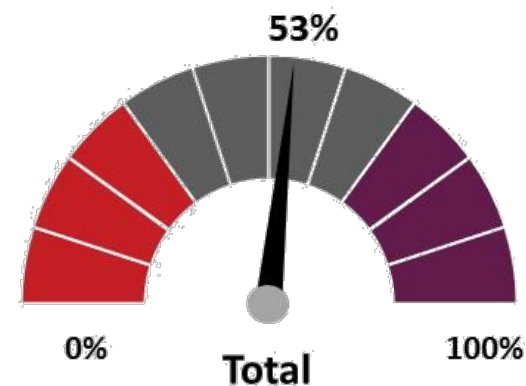
KEY TAKEAWAY

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

Adhering to govt compliance rules and regulations	73%
Having consistent experience across all apps	73%
Ensuring data security and privacy	72%
Maintaining exp. while ensuring privacy/security	72%
Maintaining centralized control	72%
Interoperability with all our systems	72%
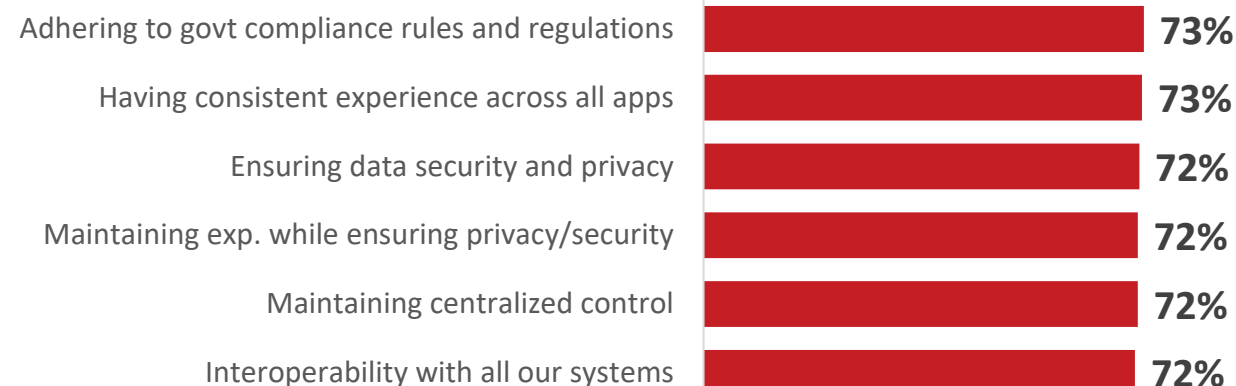
Strongly/Somewhat Agree

It is imperative that my org. be able to continue to control user authorization	77%
Digital identity is about more than authorization and authentication	72%
It is important for our devs. and engrs. to be able to implement digital identity solutions quickly	70%
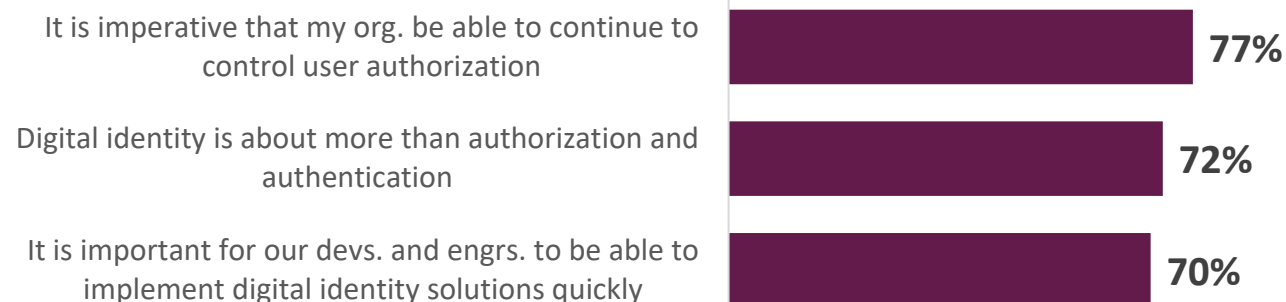
Contact Information

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%

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

Pay Grade/Level: US 🇺🇸

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

Bar chart showing pay grade/level distribution:

Pay Grade/Level	Percentage
SES (ES 1-6)/ O-7 - O-10 (1)	2%
GS 15/ O-6 (2)	8%
GS 14/ O-5 (3)	11%
GS 13/ O-4 (4)	25%
GS 11-12/ O-3 (5)	40%
GS 10/ O-2 or below	13%
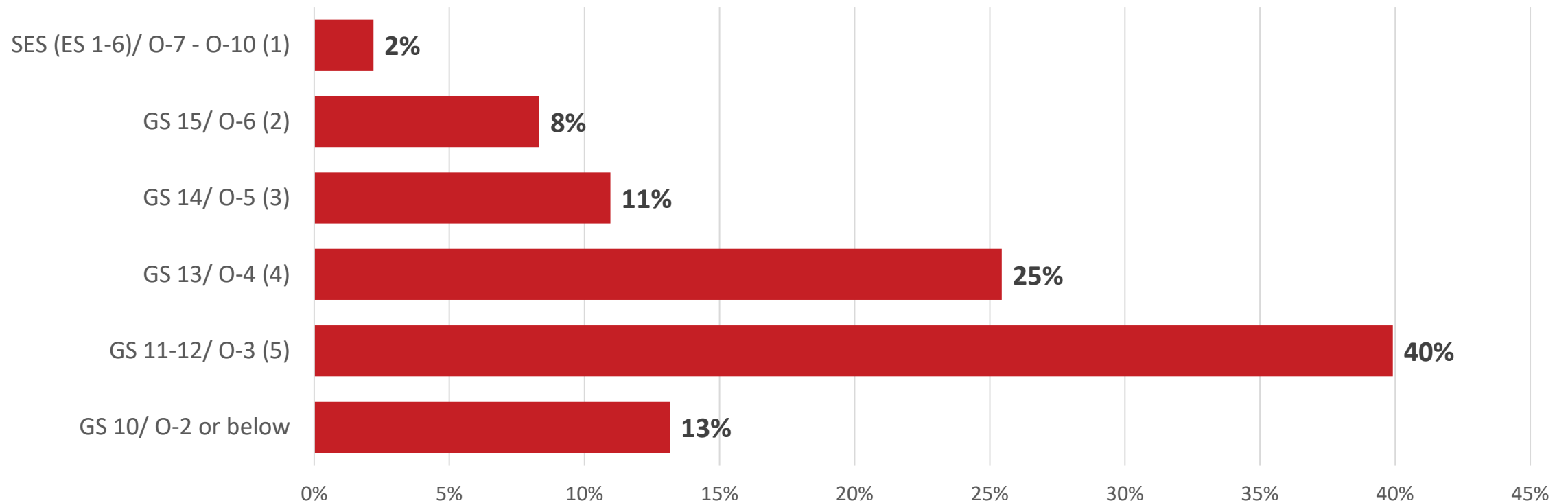
Please indicate your equivalent federal civilian or military pay grade/level.