

2022 Public Sector Identity Index Report — ANZ 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	20
Single IAM System	25
Key Takeaways	30
Appendix	38

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



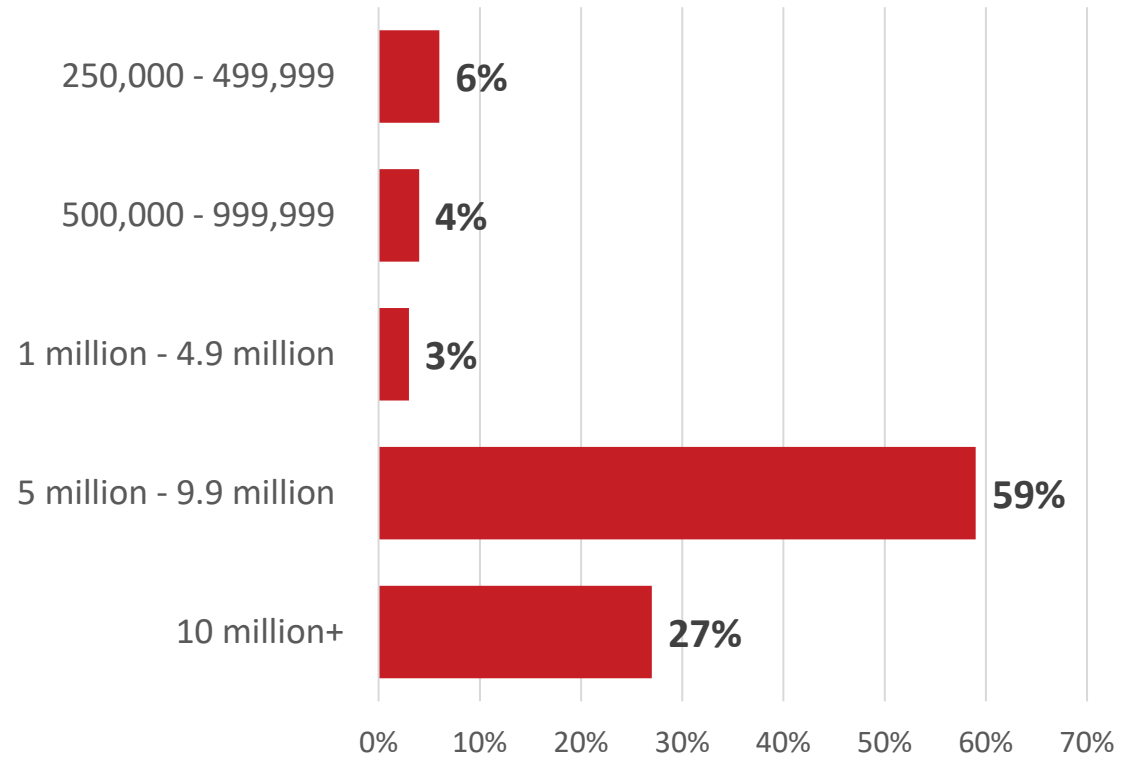
Sample Composition



Australia/ New Zealand (ANZ)

Federal Government	155 80 New Zealand 75 Australia
State and Local Government (population 250,000+)	95 (Australia Only)
Total	250

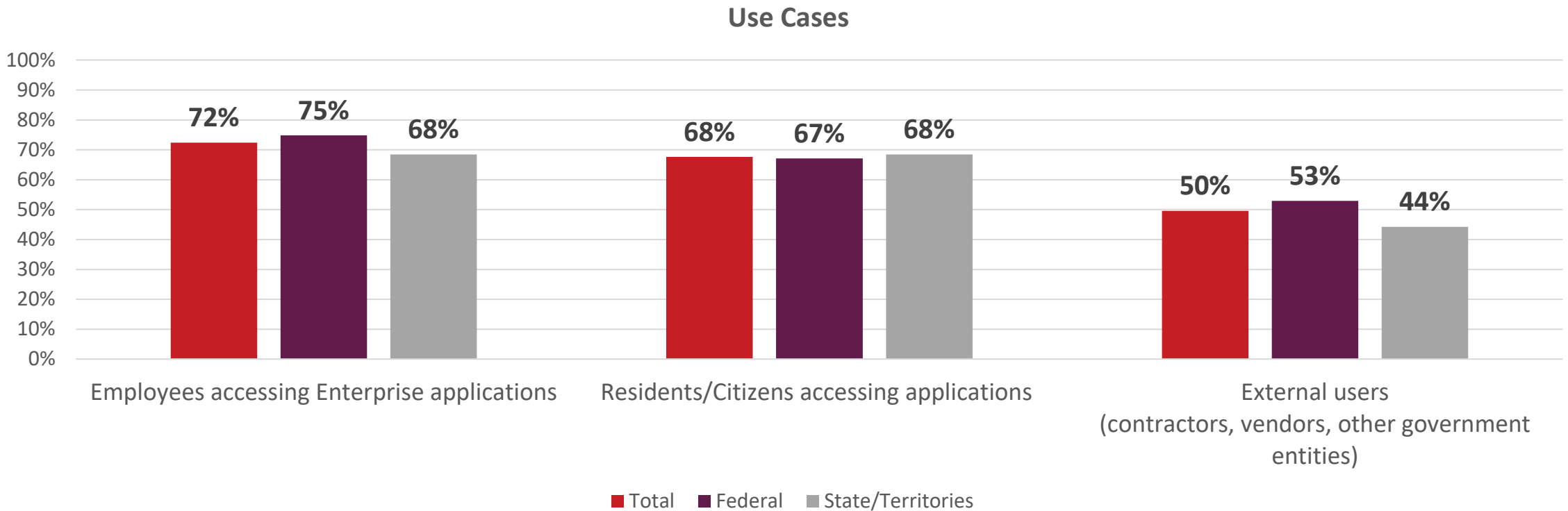
Local Government Population





Respondent Classifications

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

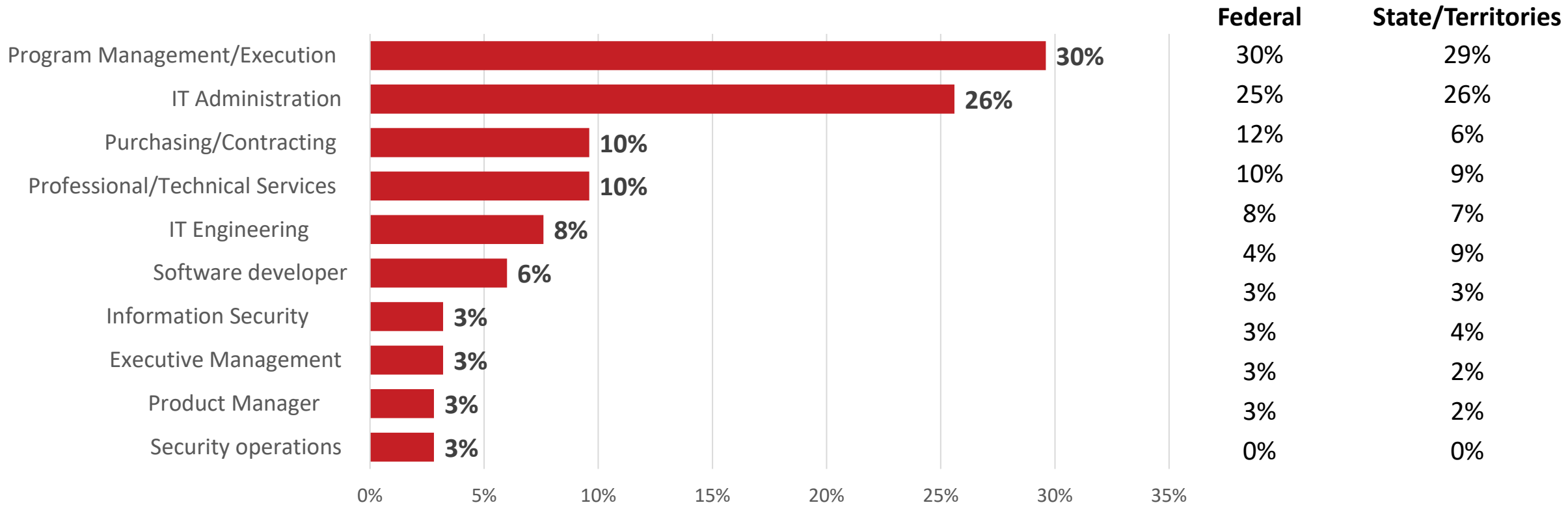


Q Which of the following use cases are most applicable to your role



Respondent Classifications – Job Role

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



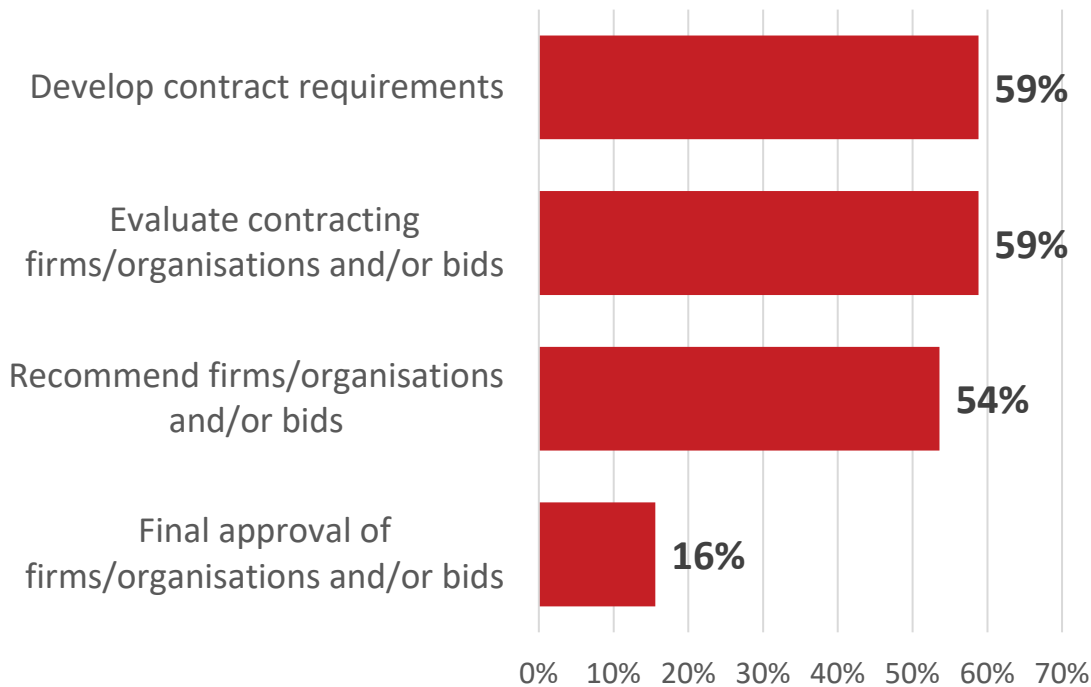
Q Which of the following best describes your role in your organization?



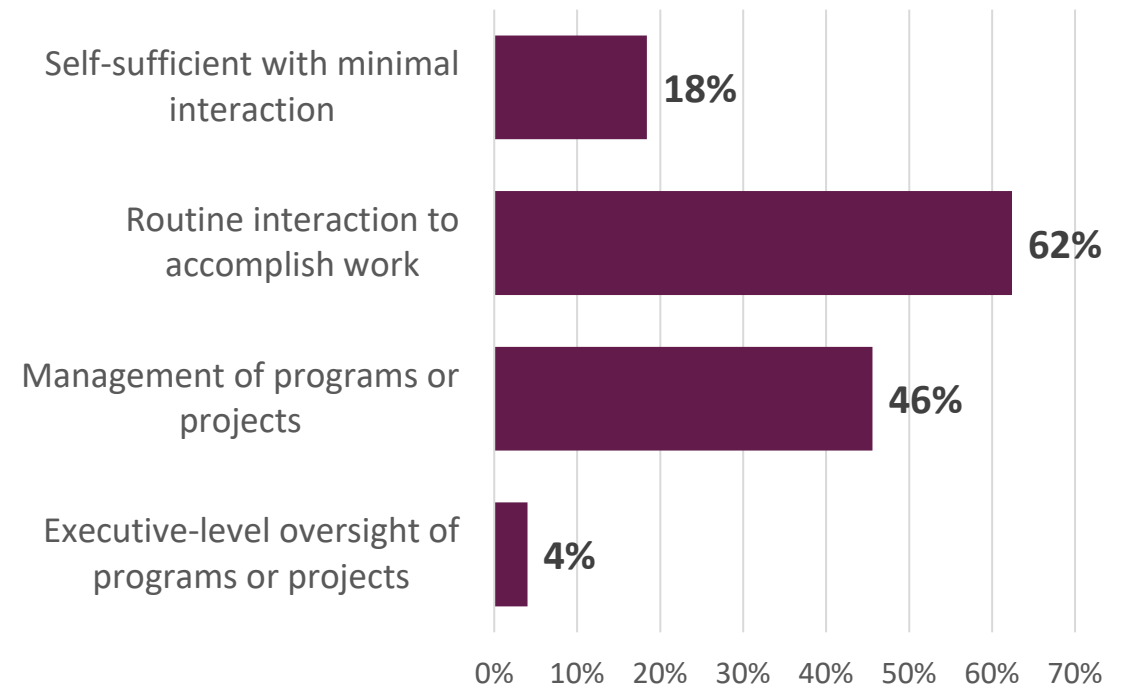
Respondent Classifications

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).

Involvement in Selection of Firms



Involvement in Management of Firms

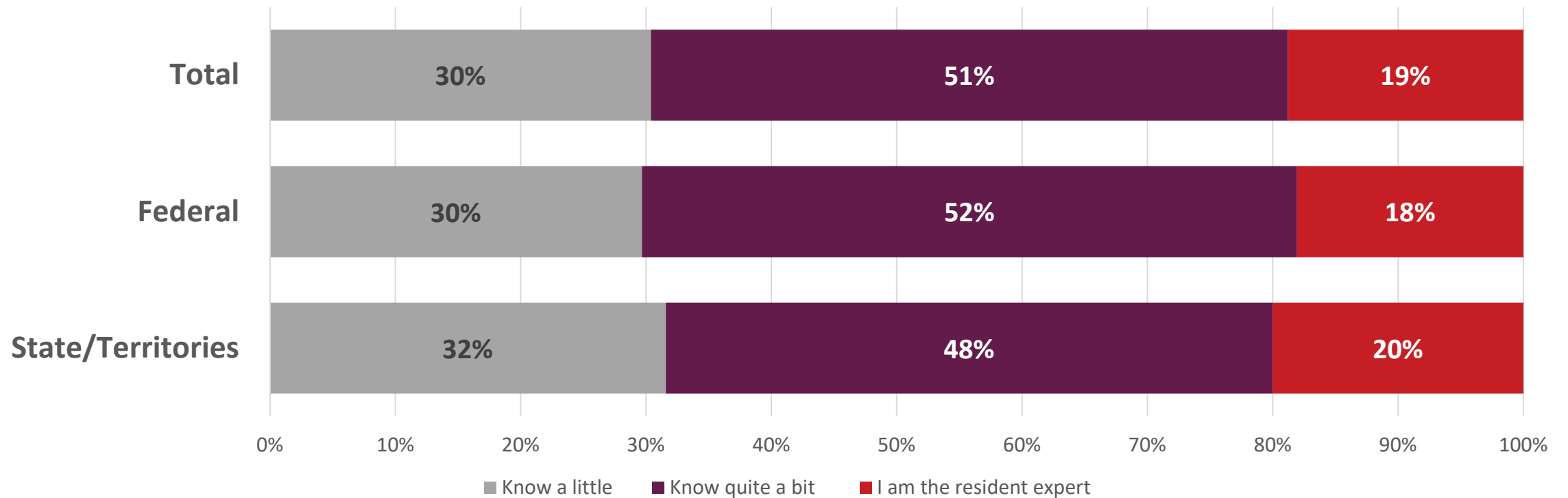


Q In which of the following ways are you or have you been involved in your [organization's/organisation's] selection of firms that provide Identity and Access Management (IAM)?
 In which of the following ways are you or have you been involved in your [organization's/organisation's] management of these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

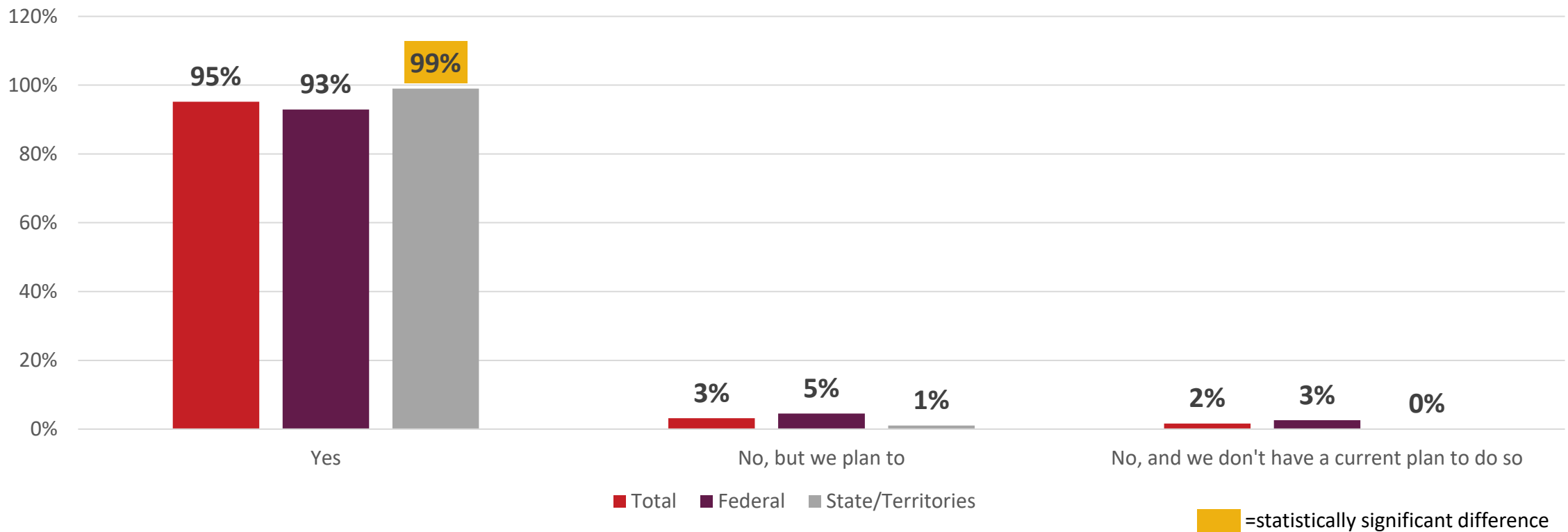


How would you describe your knowledge of your organization’s processes around Identity and Access Management (IAM)?



Organization Currently Builds External-Facing Applications

Build external-facing applications is nearly universal, particularly among state/territory government.



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

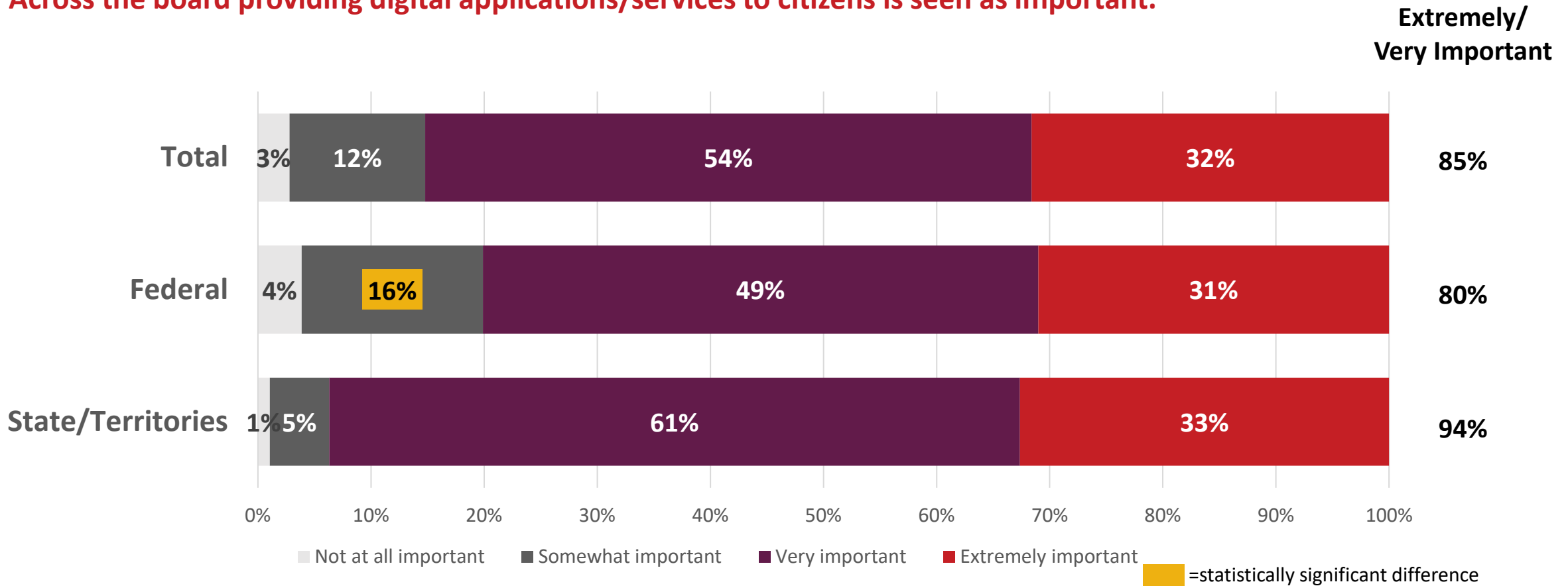


Digital Services
Landscape



Importance of Providing Digital Applications/Services

Across the board providing digital applications/services to citizens is seen as important.



Q 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

“ Not applicable
FEDERAL GOVERNMENT,
AUSTRALIA

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

Extremely important

“ Its very important as
citizens need to have
uninterrupted access to our
services
FEDERAL GOVERNMENT, NEW ZEALAND

“ Diversifying from traditional
service and embracing digital
innovation
STATE OR TERRITORIES GOVERNMENT,
AUSTRALIA

“ There has been an immense
shift in Digital Government, as
multiple departments have joined
together to become a unified
public body.
STATE OR TERRITORIES GOVERNMENT,
AUSTRALIA

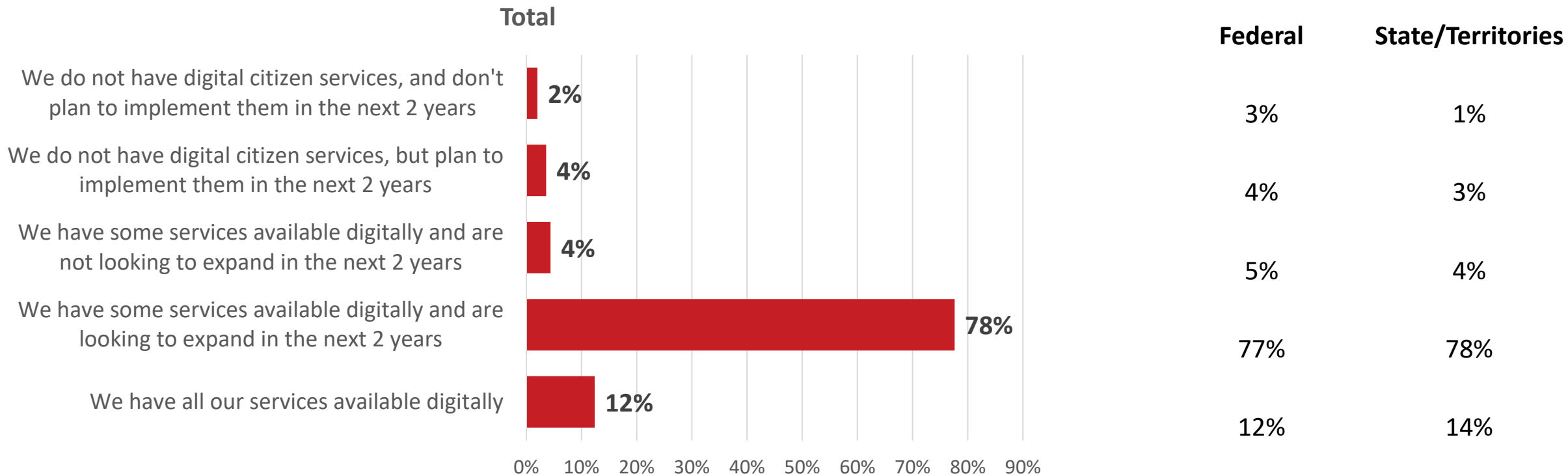


Why is it [ANSWER] that your organization has the ability to provide digital citizen services? Please be as specific and detailed as possible



Current State of Digitizing Citizen Services

Nearly eight in ten have at least some services digitally and are looking to expand in the next 2 years.

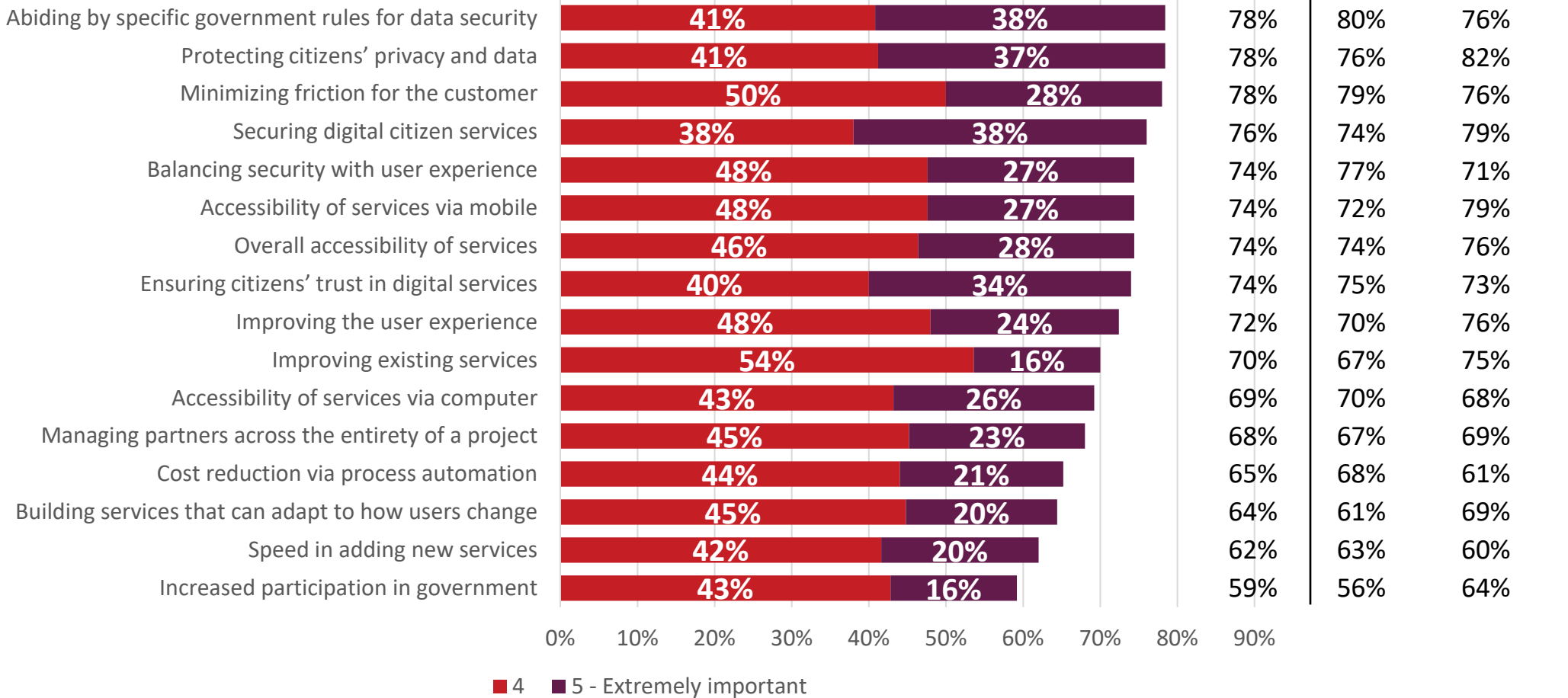


Q Currently, where is your organization in terms of digitizing its citizen services?



Importance When Thinking About Citizen Services

- Abiding by government data security rules and protecting citizens' privacy and data are the most important to this audience.
- There are no statistically significant differences between federal and state/territories.



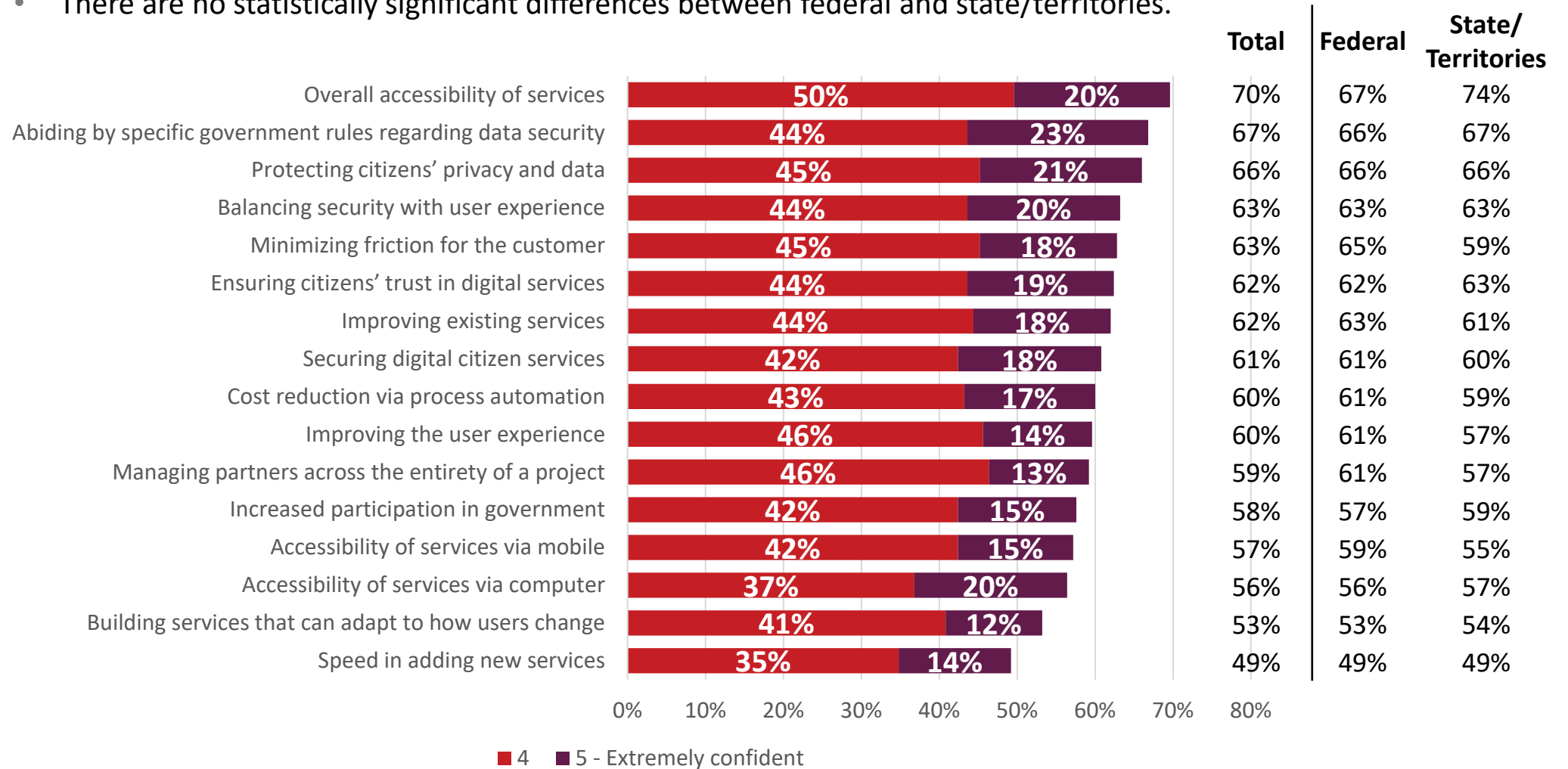
How important are each of the following to your {custom25} when thinking about its citizen services?



Confidence in Delivering

- These respondents are the most confident in their organization’s ability to deliver on the overall accessibility of services and abiding by government rules regarding data security.
- There are no statistically significant differences between federal and state/territories.

5 – Extremely Confident/4

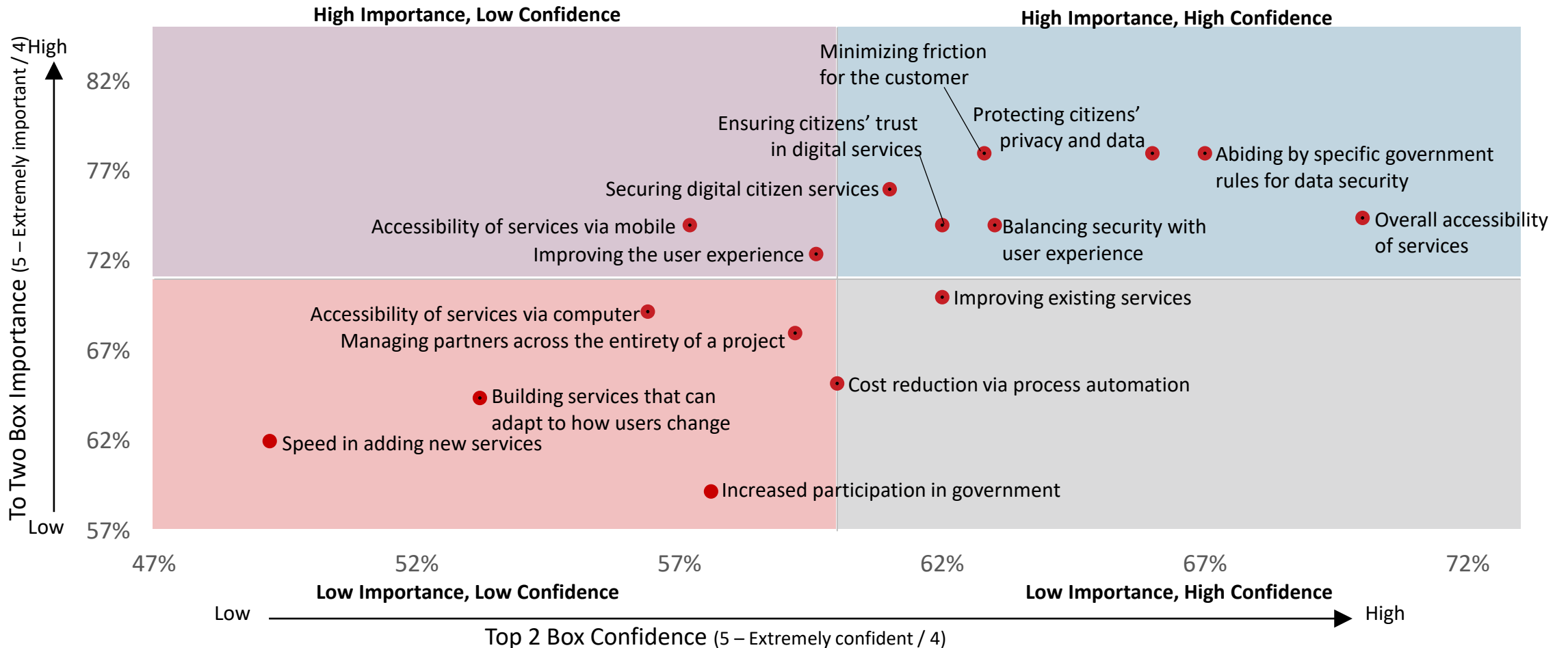


Q How confident are you in your [organization's/organisation's] current ability to deliver on each of the following aspects of citizen services?



Importance/Confidence: Total

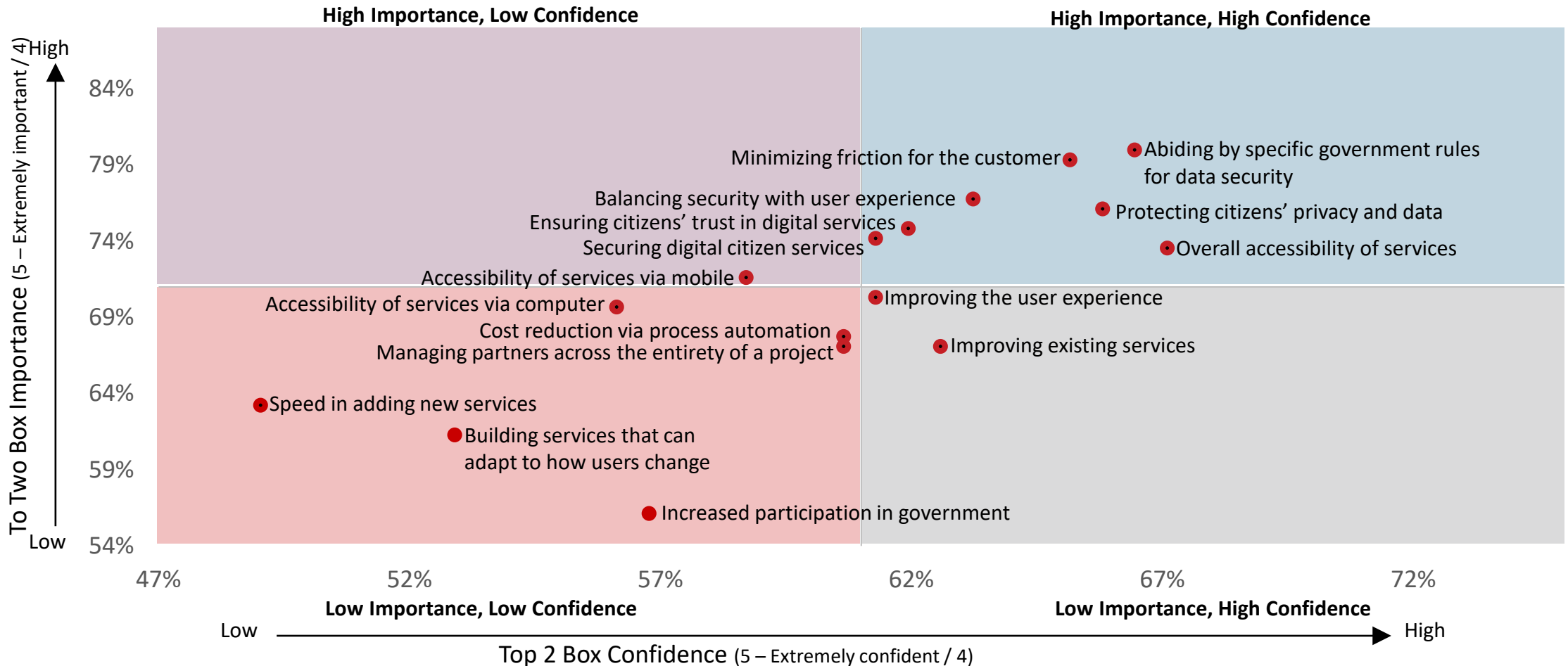
In ANZ, these respondents have key perceived weaknesses in the accessibility of services via mobile and improving the user experience.





Importance/Confidence: Federal

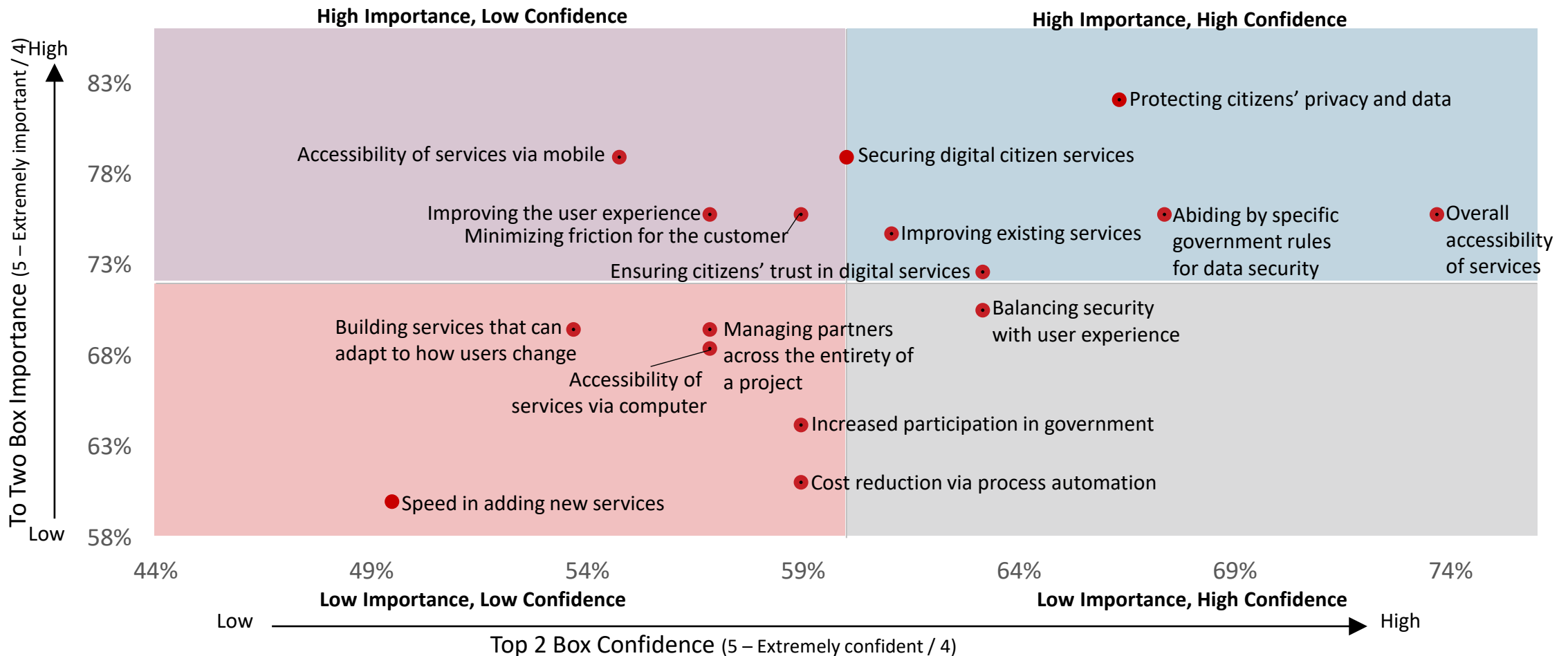
Federal respondents have a key perceived weakness in the accessibility of services via mobile.





Importance/Confidence: State/Territories

State/Territories respondents have key perceived weaknesses in accessibility of services via mobile, improving the user experience and minimizing friction for the customer.



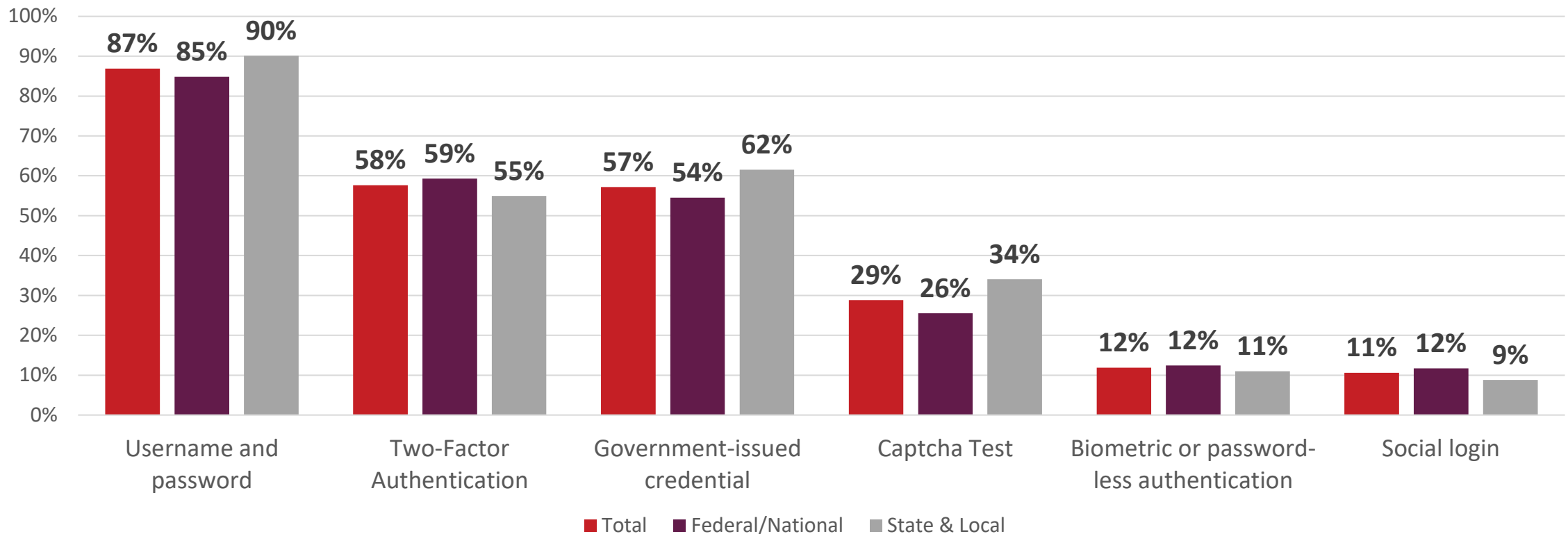


Authentication
Landscape



Current Authentication Methods Used by Citizens

Overall, username and password is the most frequently used, following by two-factor authentication and government-issued credential.

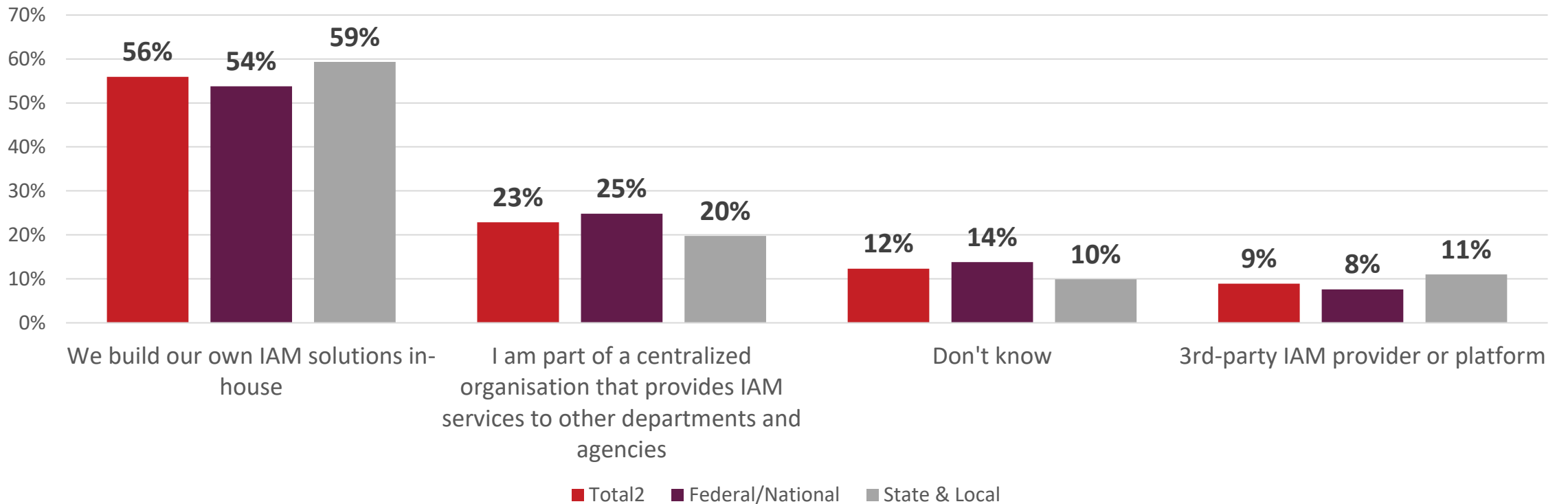


Which authentication method are citizens currently using to access your digital applications or services? Select all that apply



Current Providers of IAM

Over half currently build their own IAM solutions in-house, while less than one in ten currently outsource IAM to a 3rd party.

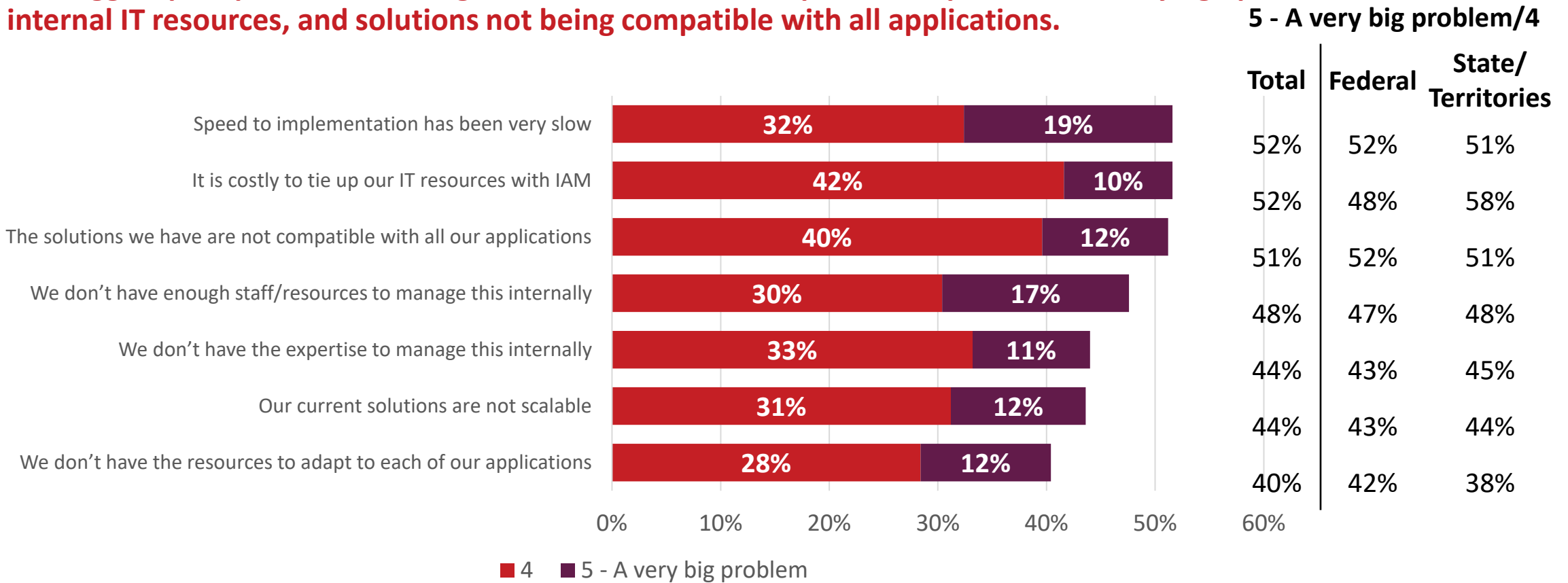


Who currently provides Identity and Access Management (IAM) services for your [organization/organisation]?



Pain Points in Building IAM In-House

The biggest pain points of building IAM in-house are slow speed to implementation, tying up internal IT resources, and solutions not being compatible with all applications.

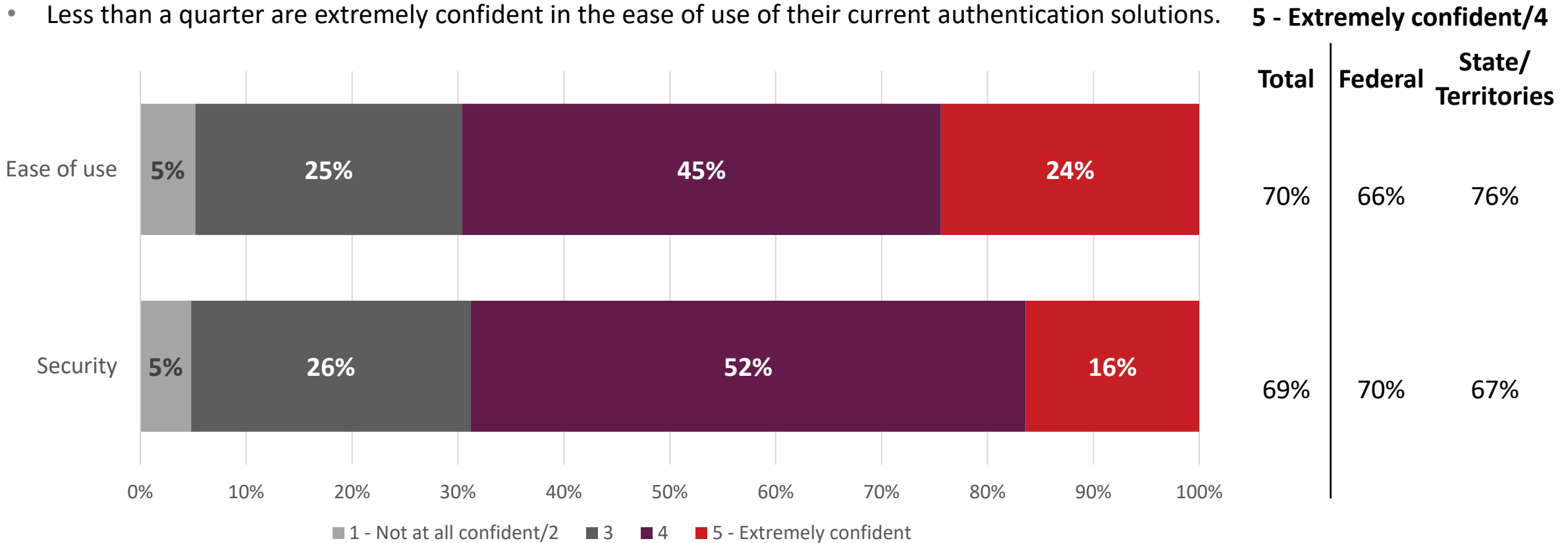


How much of a problem are each of these potential pain points in building Identity and Access Management (IAM) in-house for your [organization/organisation]?



Confidence Regarding Current Authentication Solution

- Less than one in five are extremely confident in the security of their current authentication solutions.
- Less than a quarter are extremely confident in the ease of use of their current authentication solutions.



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

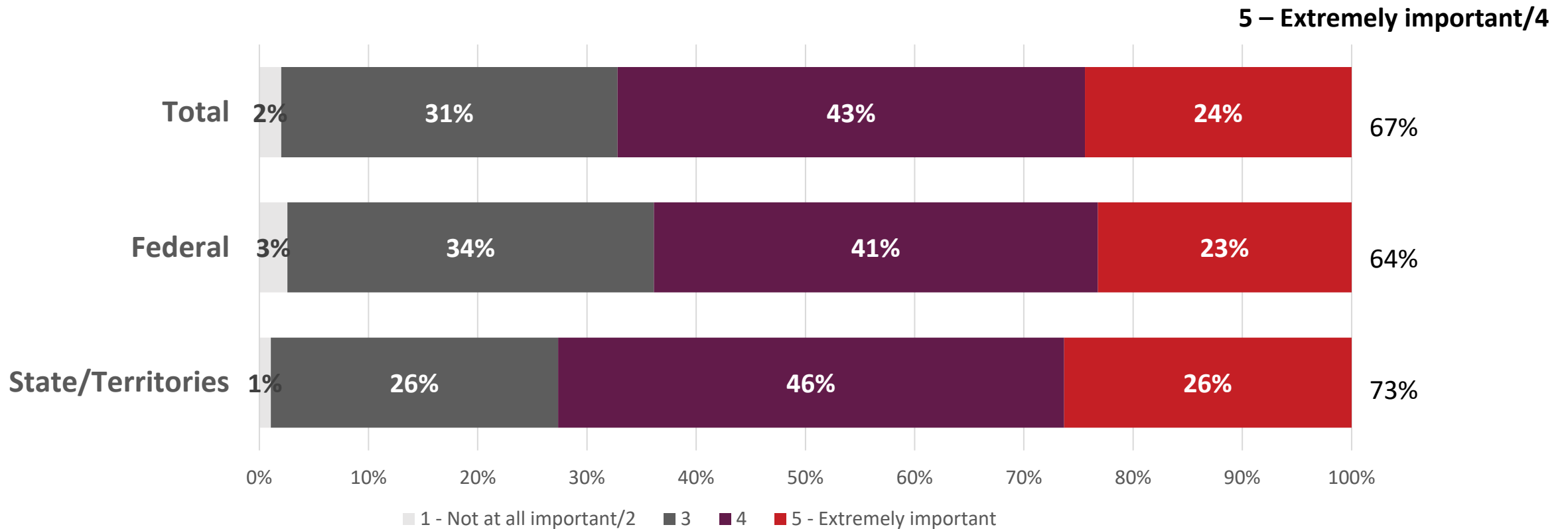


Single IAM System



Importance in Having One Digital Credential Across Services

Overall, having one digital credential for authentication and authorization across all services is seen as important across the board.

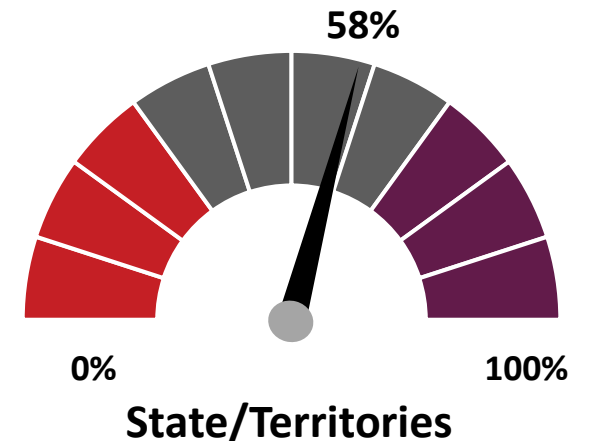
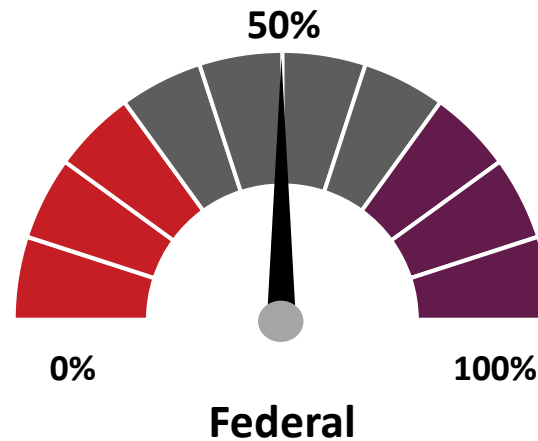
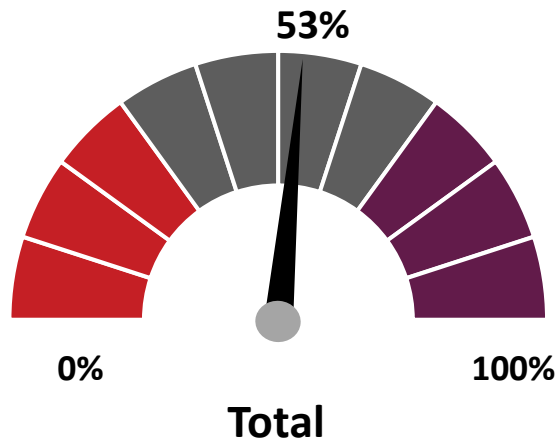



How important is it to your [organization/organisation] to have one digital credential for authentication and authorization across all your services? By this we mean enabling users to securely authenticate with multiple applications using a single set of credentials (username and password)



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.

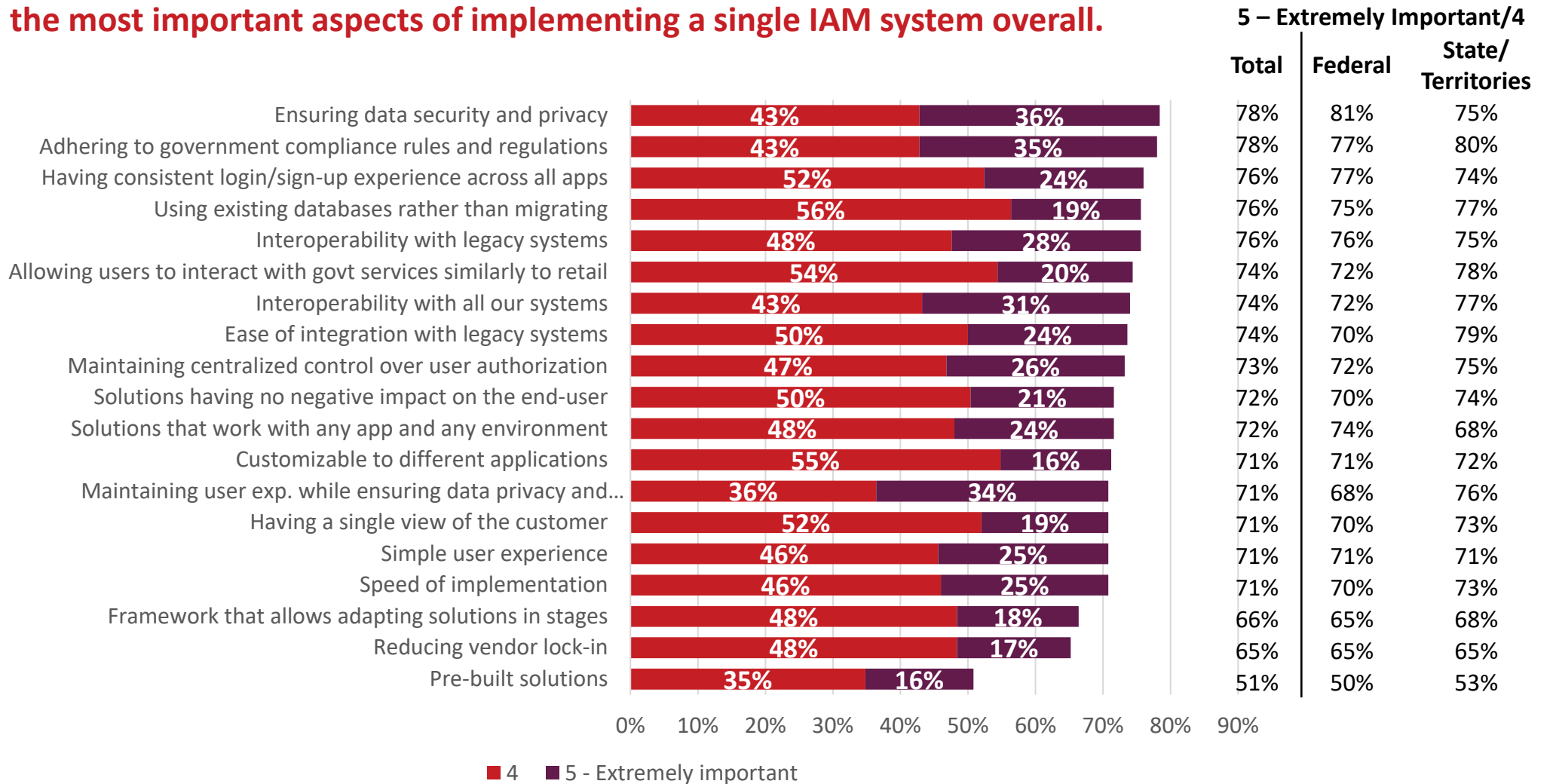


 Across what percentage of your services do you currently have a single digital credential for access?



Importance of Aspects of Implementing Single IAM System

Ensuring data security and privacy and adhering to government compliance are the most important aspects of implementing a single IAM system overall.



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?



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	Federal	State/ Territories
It is imperative that my org. be able to continue to control user authorization	77%	77%	77%
It is important for our devs. and engs. to be able to implement digital identity solutions quickly	74%	72%	77%
Digital identity is about more than authorization and authentication	73%	74%	72%
Implementing a single service hub for identity systems will simplify work for core dev. Teams	69%	68%	71%
The internal developer community should be part of the process of determining how identity authentication and security is managed, and by whom	62%	62%	62%
Our end goal is to have a single sign-on to be able to access services from the govt at all levels	60%	57%	63%
Having a 3 rd -party solution to identity authentication and security would free up internal resources	57%	56%	59%
My org. does not currently have the time and resources to adapt a single sign-on authentication to all our applications	57%	58%	56%
My org. has enough manpower to implement/maintain single sign-on authentication	56%	55%	56%
My org. has enough internal expertise to implement/maintain single sign-on authentication	55%	56%	54%
It is difficult to get internal stakeholders on board with single sign-on authentication	52%	50%	56%
Outsourcing identity authentication to a third-party vendor is too expensive	52%	49%	57%
It's difficult to justify the cost of having identity authentication via a 3 rd party	51%	46%	58%
It is difficult to get citizens on board with single sign-on authentication	49%	50%	47%





Key Takeaways



KEY TAKEAWAY

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

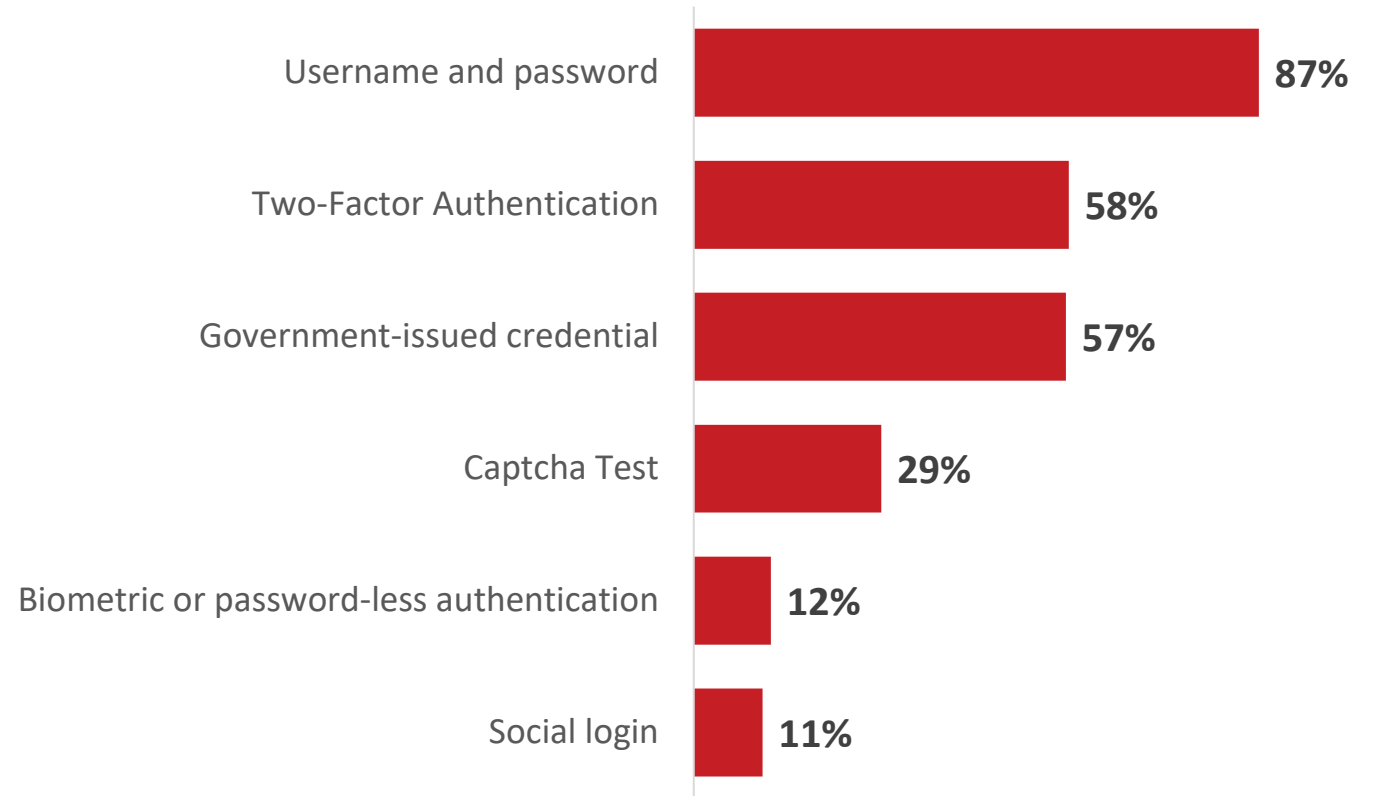
INSIGHT

- 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 over half building them in-house.

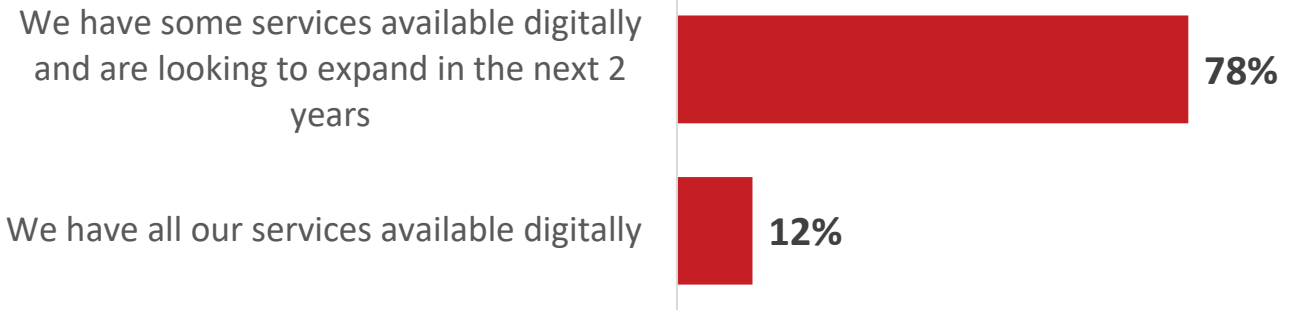
INSIGHT

- While one in ten have all their services currently available digitally, nearly eight in ten have some available digitally and are looking to expand.
- Over half currently build their own IAM solutions in-house, with less than ten percent outsourcing.

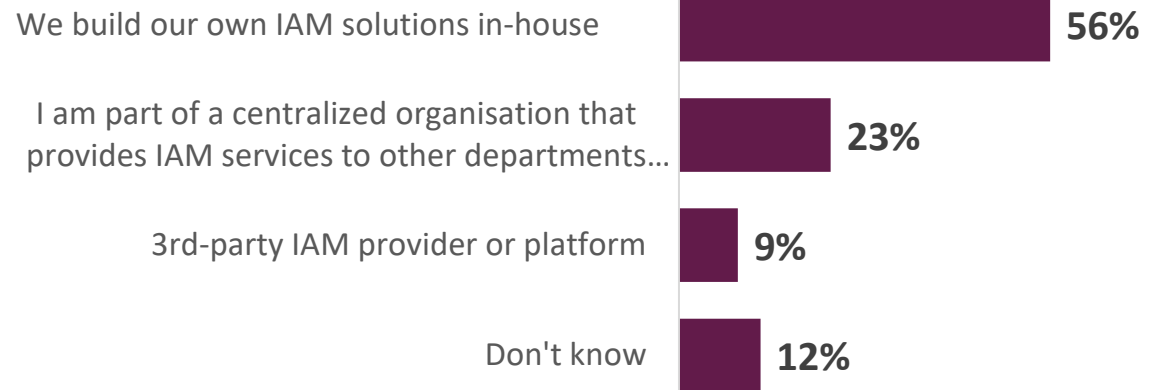
ACTION

- 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

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

INSIGHT

- Eight in ten or more cited each potential pain point as at least a 3 on a 5-point scale.

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





KEY TAKEAWAY

Respondents saw key weaknesses of improving the user experience and the accessibility of services via mobile.

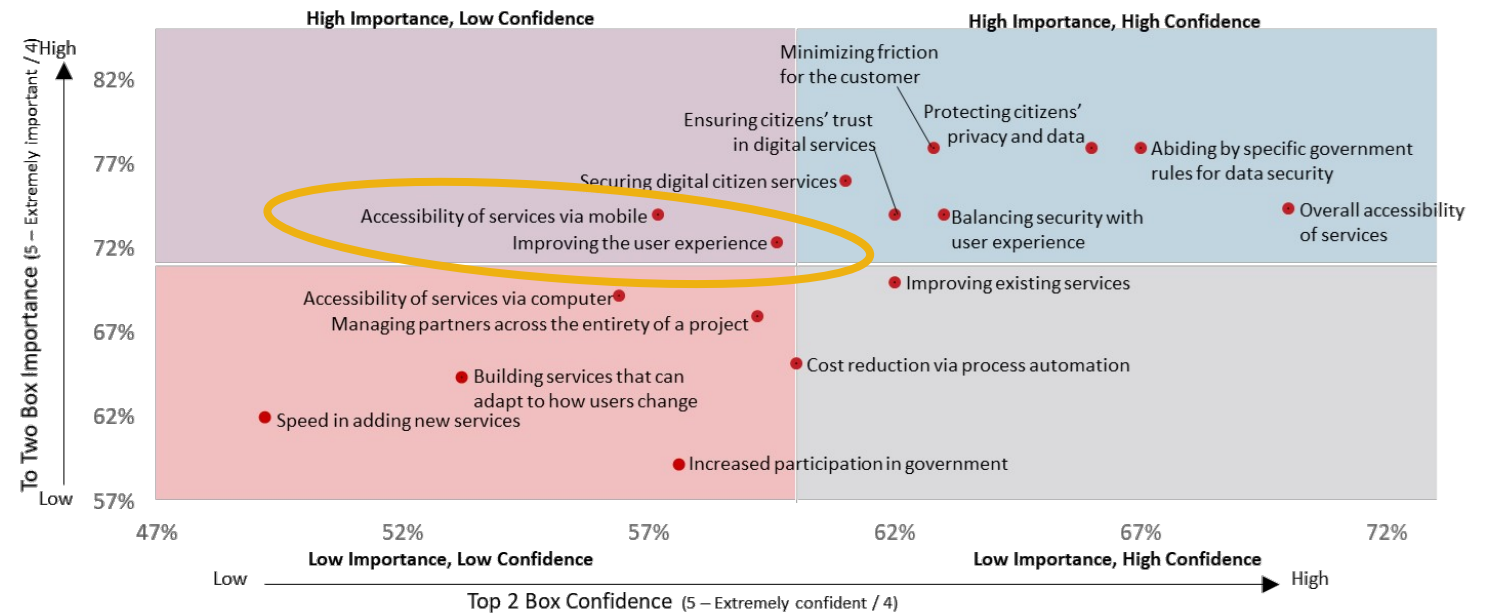
INSIGHT

- 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 the user experience 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.

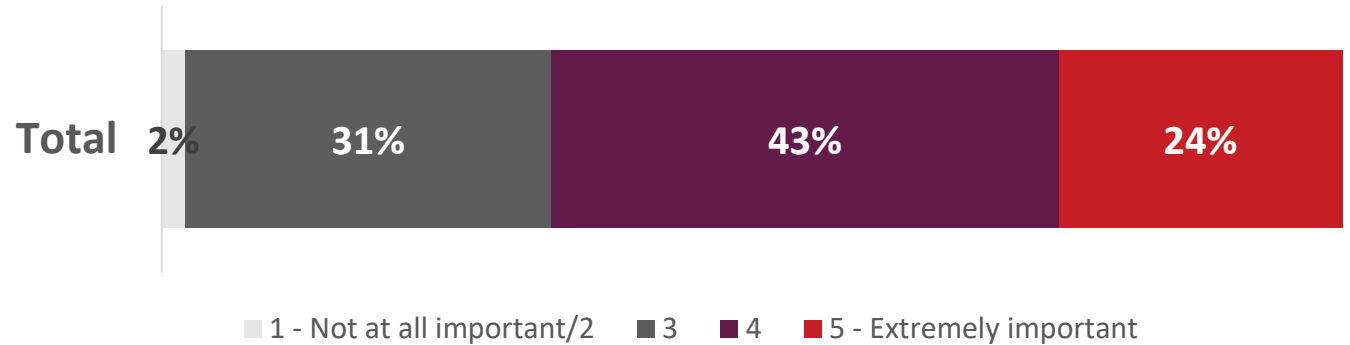
INSIGHT

- 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.

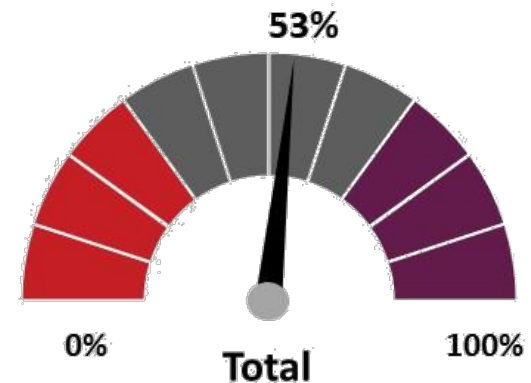
ACTION

- 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 data privacy, compliance, and a consistent user experience must be addressed.

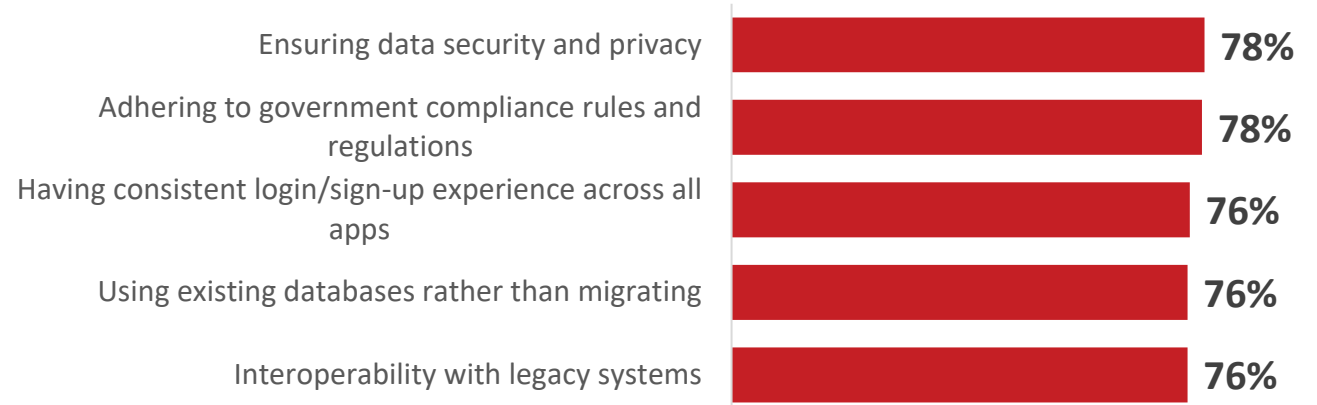
INSIGHT

- Ensuring data privacy/security, compliance, consistency in experience, using existing databases and interoperability are of top importance in implementing a single IAM system.

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



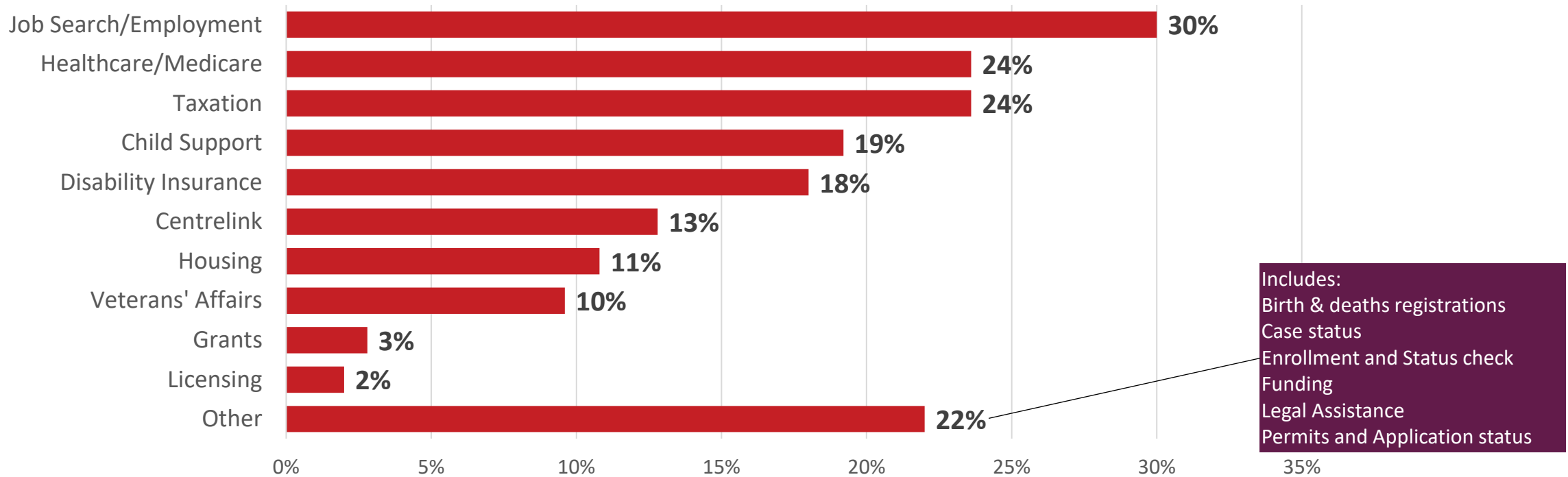


| Appendix



Respondent Classifications – Services Provided

The majority of services provided in Australia/New Zealand were job search/employment, healthcare/Medicare or taxation.



Note: Asked only of Australia/New Zealand

Which of the following services does your organisation provide to businesses and/or citizens?



Respondent Classifications: Years Served

Six in ten respondents have served at least six years.



	ANZ
Less than 1 year	4%
1-5 years	36%
6-10 years	40%
11-15 years	15%
16-19 years	4%
20+ years	1%

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