# Discover Ways to Navigate the Digital Ecosystem with Confidence

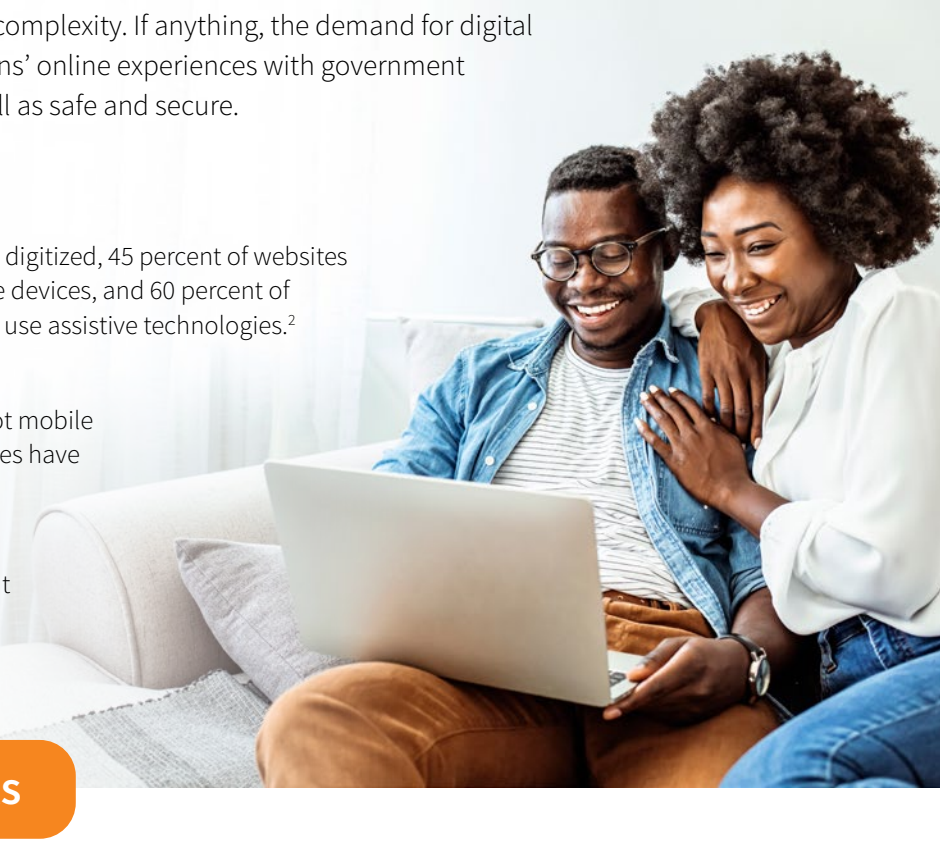
Digital Government and Services

This infographic is part of an overarching series **focusing on four of NASCIO's[1] top priority pillars**, which identify and prioritize the biggest policy and technology issues facing government agencies – as well as provide solutions for addressing these needs. The first infographic takes a deep dive into **Digital Government and Services**.

## Current Landscape

Digitization is the new normal and will increase in complexity. If anything, the demand for digital modernization is escalating in order to make citizens' online experiences with government platforms more convenient and accessible – as well as safe and secure.

Meeting that demand is evolving rapidly.



Only two percent of government forms are digitized, 45 percent of websites have not been designed to work on mobile devices, and 60 percent of websites are not fully usable by those who use assistive technologies.[2]

45 percent of public sector websites are not mobile friendly; 60 percent of public sector websites have a possible accessibility issue.[3]

Nearly $140 billion in potential government benefits goes unclaimed each year due to complicated or outdated processes.[4]

## Modernization Drives Benefits

Digitization and modernization make government operations more efficient, transparent, and accessible to the public.

- **Easier Access to Services**
- **Customization for Equitability**
- **Time and Money Saved**

## Digital Government Top Challenges

Government agencies continue their modernization and security journeys, undertaking processes to go fully digital and provide seamless access for trusted citizens – as well as continue to protect against identity risks.

Understanding citizen identities is central to navigating the ever-evolving cybersecurity threat landscape and essential in ensuring government agencies have a secure, effective, positive interaction with those they serve. Delivering safe and friction-appropriate service starts with a clear understanding of what contextually comprises an identity.

This journey comes with difficulties around identity and security risks, but solutions are available to navigate the digital ecosystem with confidence.

## Identity Security Risks and Privacy

**The Problem:**

Fraudsters' data breach tactics – particularly through Artificial Intelligence (AI) and generative AI (Gen AI) – are constantly evolving, putting citizens' identities and private information at risk. Variants of AI models are designed for malicious purposes and facilitate cybercriminal activities. These tools can create highly convincing phishing emails, generate malicious code, and conduct other illegal activities that put agencies at risk – and make it difficult to be sure people are who they say they are.

- Automated attacks can identify and exploit system vulnerabilities at high speed and with a lower barrier to entry for non-expert attackers.
- Detecting these attacks and responding to them is challenging.
- They can be created in less than 24 hours and scaled rapidly.

Malicious AI can also be used for sophisticated forms of identity fraud using Deepfake videos, voice-cloned audio clips, high-precision fake IDs, and other documents. For agencies, identity fraud brings risk of financial losses, misinformation spread, and undermining of public trust.

**The Solution:**

Identity assurance means having the confidence and certainty that the individual with whom a government agency interacts – and the devices they're using – is, in fact, who they claim to be. Assurance is crucial because people engage more often now with online web portal sessions and less physically in person, creating added complexities. Traditional identity proofing and identity verification solutions only verify that the entity claiming to be an individual has that individual's information, leaving agencies vulnerable for taking the entity at its word.

**LexisNexis® Risk Solutions can be an extension of an agency's own systems** and can look for evidence of whether the device is trying to conceal its true source or location. These tools evaluate whether that risk is consistent with an online entity using a stolen identity. **The verification we complete through digital identity assurance exposes online risk and, by exposing risk, we can determine whether this entity can be trusted and is the purported individual.**

## Data in Silos

**The Problem:**

Data silos within government agencies cause inefficiencies, use outdated constituent information, and miss opportunities to share critical information due to data being stored by individual departments. The results are:

- Bureaucratic obstacles.
- Security and privacy concerns.
- Critical differences in data within each department.
- Conflicting data management practices across agencies.

To effectively understand the concerns impacting citizens, government organizations must be able to gain a line of sight into their population's current and historical needs – and weave in transparency to effectively understand the concerns impacting citizens.

**The Solution:**

Working with LexisNexis Risk Solutions can help agencies better understand the current state of their populations' data by making links between agencies' records with, for example, those who have passed away, people who have moved, and updated contact information. By doing so, agencies can be confident in planning for and implementing data-driven strategies, and coordinating care across departments.

With over 10,000 referential data sources, we provide:

- **Continuously updated data** on citizens to improve public health outreach and coordination.
- **Precision linking** to ensure more accurate data tracking, avoiding duplicate records and efforts.
- **Data that includes people with limited available information**—often society's most vulnerable.

## Legacy Systems

**The Problem:**

Legacy systems can create a host of issues within government agencies that are modernizing or moving to new systems, including:

- Lack of security features to protect against modern threats.
- Incompatibility with new technologies, such as mobile devices, and current software and hardware.
- Inability to convert all data from the old system to the new when modernizing, which can lead to significant data loss.

These vulnerabilities leave agencies open for fraudsters to exploit their systems, wreaking havoc on the security of constituents' data and private information.

**The Solution:**

Digitization shines a spotlight on the importance of agencies investing in innovation to modernize their infrastructure. Integrating and centralizing systems are now the norm. Our solutions work within agencies' current systems to ensure more accurate, updated data is brought over.

**From enabling transformative initiatives to delivering secure government services in real-time** through a centralized portal, or augmenting team resources with investigative analytics, we create confidence by driving efficiency, transparency, and oversight across channels and agencies.

LexisNexis® RISK SOLUTIONS

**For more information:**
**Scan QR Code or Call 1-888-216-3544**

1. https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2024/
2 https://www.whitehouse.gov/omb/briefing-room/2023/09/22/why-the-american-people-deserve-a-digital-government/
3 https://www.whitehouse.gov/omb/briefing-room/2023/09/22/fact-sheet-building-digital-experiences-for-the-american-people/
4 https://www.whitehouse.gov/omb/briefing-room/2023/09/22/fact-sheet-building-digital-experiences-for-the-american-people/