Top Technology Trends in Government for 2021

By Rick Howard, Bill Finnerty, Ben Kaner, Arthur Mickoleit, Michael Brown, Irma Fabular, Neville Cannon, Alia Mendonsa, Dean Lacheca, Apeksha Kaushik, Katell Thielemann

Published 1 March 2021

Gartner®

Top Technology Trends in Government for 2021

Published 1 March 2021 - ID G00742950 - 30 min read

By Analysts Rick Howard, Bill Finnerty, Ben Kaner, Arthur Mickoleit, Michael Brown, Irma Fabular, Neville Cannon, Alia Mendonsa, Dean Lacheca, Apeksha Kaushik, Katell Thielemann

Initiatives: Government Digital Transformation and Innovation

Gartner's 2021 technology trends for government offer public-sector leaders the potential to accelerate digital innovation. Government CIOs can use this research to assess the impact of these trends on their postpandemic digital strategies to improve operational performance and program outcomes.

Overview

Opportunities

- The COVID-19 pandemic has spurred the acceleration of digital innovation across the government sector in all regions of the world (see 2021 CIO Agenda: Government CIOs Step Up to Action for Digital Acceleration). This acceleration presents government leaders with new opportunities to leverage data and technologies that build trust, agility and resilience in public institutions.

- While government CIOs will continue to face pandemic-related challenges in 2021 and beyond, technology trends have emerged that address critical challenges in areas such as security, cost containment and citizen experience.

- Government executives and CIOs have an opportunity to sustain the pace of digital innovation and adapt to changing risks by identifying technology trends that best address their postpandemic recovery priorities.

Recommendations

Government CIOs involved in digital transformation and innovation should:

- Assess the potential impacts of government technology trends on your organization by using scenario planning to determine if prepandemic strategic goals and operating assumptions are still valid or need to be revised.

- Invite stakeholders to identify and prioritize technology trends that are of the greatest value to your organization by linking them to outcomes that will improve trust, agility and resilience. Use the selected trends for postpandemic strategy planning.

- Extend business capabilities by building custom Hype Cycles for the trends you have selected, and use them to develop an 18- to 24-month digital innovation roadmap consistent with possible future scenarios.

Strategic Planning Assumptions

By 2023, 50% of technology companies that provide products and services to the government will offer packaged business capabilities to support composable applications.

By 2025, 75% of government CIOs will be directly responsible for security outside of IT, to include operational and mission-critical technology environments.

By 2024, a true global, portable, decentralized identity standard will emerge in the market to address business, personal, social and societal, and identity-invisible use cases.

By 2024, over 30% of governments will use engagement metrics to track quantity and quality of citizen participation in policy and budget decisions.

By 2025, 95% of new IT investment made by government agencies will be made as a service solution.

By 2025, over 50% of government agencies will have modernized critical core legacy applications to improve resilience and agility.

By 2024, government organizations with a composable case management application architecture will implement new features at least 80% faster than those without.

By 2024, 75% of governments will have at least three enterprisewide hyperautomation initiatives launched or underway.

By 2024, 60% of government AI and data analytics investments aim to directly impact real-time operational decisions and outcomes.

By 2023, 50% of government organizations will establish formal accountability structures for data sharing, including standards for data structure, quality and timeliness.

What You Need to Know

As 2021 unfolds, government leaders face evolving challenges brought about by the pandemic and its aftermath. To meet these challenges and sustain the pace of digital innovation to realign spending, public-sector CIOs and IT leaders must link an expanding set of critical business priorities with continued investment in technology and information.

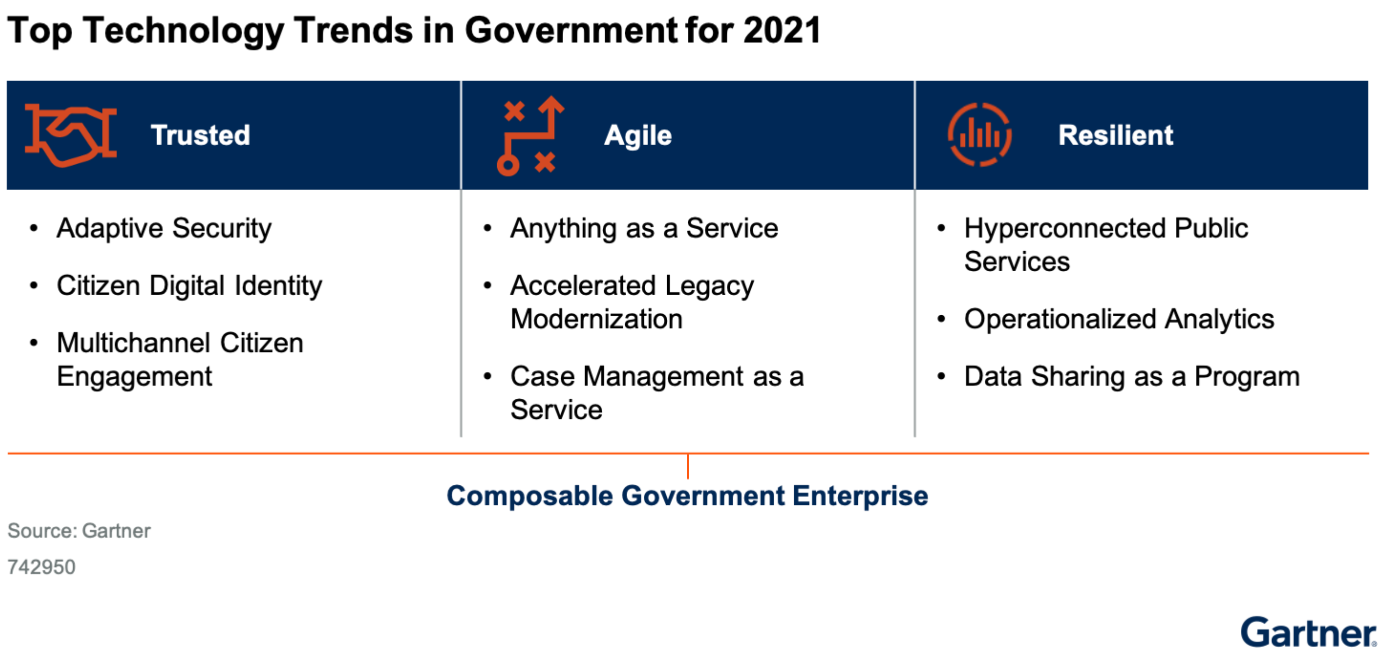
The pandemic forced government agencies to reassess their digital strategies and transform (see Predicts 2021: Governments Tackle Transformation Out of Necessity). Governments' priorities shifted, as resources were scarce. The impact of COVID-19 accelerated the move to remote work while negatively impacting cities with a significant proportion of government workers. The pandemic forced governments to accelerate the implementation of digital services; yet, much of the increased volume lacked digital maturity.

Our top technology trends impacting government in 2021 arise from the challenges wrought from the pandemic. They evolve as a response for government CIOs to design flexible operating and organizational models that support tremendous disruptions. Further, they build on Gartner's 2019-2020 technology trends, where we had focused on how those trends had the potential to optimize or transform public services (see Technology Trends in Government, 2019-2020).

The top technology trends are directly linked to public administration and policy issues that government leaders must address into 2023. We refer to these issues as "business" trends. For more about Gartner's government trend development process, see Top Business Trends in Government for 2021. From these business trends, we developed 10 technology trends that will impact government (see Figure 1). We then grouped nine of the business trends into three strategic goals that government leaders have long aspired to achieve:

- Trust in government among citizens
- Agility in response to a rapidly changing world
- Increased resilience of the public-sector workforce and institutions

Figure 1. Top Technology Trends in Government for 2021



Top Technology Trends in Government for 2021

Trusted	Agile	Resilient
• Adaptive Security • Citizen Digital Identity • Multichannel Citizen Engagement	• Anything as a Service • Accelerated Legacy Modernization • Case Management as a Service	• Hyperconnected Public Services • Operationalized Analytics • Data Sharing as a Program

Composable Government Enterprise

Source: Gartner

742950

Trend Profiles: Click links to jump to profiles

Trusted	Agile	Resilient
Adaptive Security	Anything as a Service (XaaS)	Hyperconnected Public Services
Citizen Digital Identity	Accelerated Legacy Modernization	Operationalized Analytics
Multichannel Citizen Engagement	Case Management as a Service (CMaaS)	Data Sharing as a Program
	Composable Government Enterprise	

A composable government enterprise, as depicted in Figure 1, represents the evolution of software design and delivery that began with object-oriented programming and service-oriented architecture. It evolved with advances in technology or practices, such as agile development, APIs, microservices, digital product management. By supporting the nine other technology trends, the composable government enterprise serves as the foundation upon which leaders achieve the trust, agility and resilience objectives of government.

Public-sector CIOs and IT leaders can leverage our government technology trends research to develop and nurture their understanding of the connection between technology investments and social policy objectives. These trends analyses help CIOs make informed decisions to improve their business capabilities and support their organizations’ goals in a postpandemic environment.

Trend: Composable Government Enterprise

Back to top

Analysis by Bill Finnerty, Rick Howard

Strategic Planning Assumption: By 2023, 50% of technology companies that provide products and services to the government will offer packaged business capabilities to support composable applications.

Description:

The composable government enterprise is any government organization that adopts composable design principles (see Seize the Moment to Compose a Resilient Future: Key Insights From the 2020 Gartner IT Symposium/Xpo Keynote). It makes composable design a core aspect of the enterprise architecture (EA) design principles. Being a composable government enterprise enables an organization to extend the reuse of capabilities and continuously adapt to changing regulatory, legislative and public expectations.

To be flexible in design programs and services, composable government enterprises take a modular approach to use and reuse business and technical capabilities. Existing applications must be decomposed into packaged business capabilities that allow them to be assembled into new application experiences. New solutions, whether individual capabilities or an application with multiple capabilities, should be architected in a modular fashion using a mesh app and service architecture.

Why Trending:

The rapidly evolving needs of the emerging digital society require the government to reconsider its industrial era constructs. However, legacy, monolithic government systems have been inhibitors to changing needs, frequently impairing consideration of process changes due to their inflexibility. CIOs are embracing composable government to overcome existing, siloed approaches to managing services, systems and data that limit the ability of governments to adapt. By focusing on modular business and technology capabilities, government leaders are reconfiguring government services and creating new application experiences with the necessary speed and agility.

Implications:

EA programs must be elevated to a business support function, not just technical, to enable the focus on rearchitecting the way services are designed and delivered. The role of chief enterprise architect (CEA) will need to be equal parts talent, data, technology and operations prognosticator.

Digital leadership is essential for government organizations to establish the capabilities necessary to be composable. Reimaging public services to most effectively deliver value and establish the trust of constituents will require a clear vision, an enterprise-level view of citizen experience and maintaining the governance essential to adapting to a changing environment.

Actions for Government CIOs:

- Direct the enterprise architecture program to develop, or update, the business and technology capability models across the enterprise and then identify common business capabilities used across multiple programs to establish a roadmap for decomposing existing systems.
- Work with governance and business leaders to embrace modular design to adjust investment decisions to take advantage of the solutions that are most capable of providing needed business functionality, versus best-of-breed solutions, and enable continuous modernization.

Trusted

Trend: Adaptive Security

Back to top

Analysis by Michael Brown, Katell Thielemann, Irma Fabular

Strategic Planning Assumption: By 2025, 75% of government CIOs will be directly responsible for security outside of IT, to include operational and mission-critical technology environments.

Description:

The adaptive security model is one in which cybersecurity systems operate more like an autonomic biologic immune system. [1] The adaptive security architecture features components for prediction, prevention, detection and response. The adaptive model forgoes traditional notions of perimeter, assuming there is no boundary for safe and unsafe, a necessary conceptual shift given the migration to cloud services.

Why Trending:

The imperative for an adaptive approach derives from both the evolving threat and the increasingly sophisticated tools at the CIO's disposal. From a threat perspective, the operative security assumption is not when, or if, threats will be present, but rather that threats are continuous. The trend toward an adaptive model for cybersecurity necessarily follows the relentless and rapidly evolving assaults on government IT systems. From a tools perspective, it is much like an arms race.

In government organizations, cybersecurity has historically been addressed in terms of compliance with volumes of written artifacts that are periodically reviewed and updated. This is changing quickly with risk management frameworks that now require continuous monitoring and ongoing authorization. [2] That shift in how risk management is conducted is another catalyst for change that forces government agencies to implement adaptive security.

Implications:

Two implications are paramount — sustained funding and talent. A robust cybersecurity program can be expensive. The cost of tools and outside services or consultants to establish or reinvigorate a security program can be quite high. Further, dedicating an increased budget to cybersecurity may well come at the expense of capability and services that business unit leaders want and expect. In the eyes of business unit leaders who might get less support from IT teams, investments in cybersecurity may appear as unnecessary insurance. The ability, or lack thereof, to differentiate an adaptive security implementation from traditional document-based compliance may also limit ability to obtain support for necessary budget resources.

Cybersecurity expertise is in extremely high demand. Government agencies can be challenged to compete with the private sector for staff with necessary skills. This can aggravate the budget issue by requiring more dependence on outsourced labor. Skills shortages for cybersecurity are widely reported in the media. [3,4,5] The operational imperative and possible compliance requirement to implement adaptive security in the face of budget and staffing challenges, require CIO leadership and creativity.

Actions for Government CIOs:

- Offset resistance and cost for the adoption of an adaptive security mindset and operational behavior by deprioritizing document-based compliance activities and linking value to broader digital innovation and transformation objectives.
- Create a holistic risk management program by collaborating with leaders for physical and personnel security and collaborating with mission units for operational technology security.
- Mitigate the tools arms race by ensuring that the full capability and value of current cybersecurity tools are being exploited, avoiding duplicative products, retiring tools where appropriate and scaling tools where needed most for high-value assets.
- Reduce the need to acquire scarce talent by growing from within through training programs with the explicit intent of developing skilled IT security staff and maintaining their competencies over time.

Trend: Citizen Digital Identity

Back to top

Analysis by Arthur Mickoleit, Michael Brown

Strategic Planning Assumption: By 2024, a true global, portable, decentralized identity standard will emerge in the market to address business, personal, social and societal, and identity-invisible use cases (see Predicts 2021: Identity and Access Management and Fraud Detection).

Description:

The definition of citizen digital identity is evolving with its use cases. In retrospect, citizen digital identity was defined mostly as electronic identification (eID), authentication and electronic signatures in online government services. The contemporary definition of citizen digital identity has grown to include use cases like age validation while preserving privacy, sharing identity data through digital wallets, acting as a delegate for a parent or a company. A near-future-oriented definition considers the growing convergence of physical and virtual identities. When digital identity data flows seamlessly between individuals, organizations and objects, decisions about sovereignty over digital identity data will become, at best, politically contentious.

Why Trending:

Digital identity has become front and center in political discourse. The topic is high on political agendas: a proposed Improving Digital Identity Act in the U.S. for a standards-based approach to digital identity;

German Chancellor Merkel's commitment to building a strong digital identity ecosystem; Australia's public consultation on the national digital identity framework. As a result of the pandemic, many government agencies realized the importance of providing and validating identity information remotely for resilient operations.

Digital identity ecosystems are quickly evolving and leading governments to assume new roles and responsibilities. Today, government ID is only one way citizens and consumers prove identity in digital contexts. New governance approaches like "bring your own identity," decentralized and self-sovereign identity are bound to spread further (see Innovation Insight for Bring Your Own Identity). The sometimes conflicting interests of different ecosystem actors unsettle some governments, while others take on the challenge by assuming new roles and responsibilities.

Implications:

Government CIOs must link digital identity to salient use cases. Governments have in the past rolled out digital identity schemes without ever validating intended uses with the intended users. But digital identity requires exploration, a business case, gradual expansion and validation of assumptions for use cases.

Pressured by the pandemic, many governments are forced to react quickly but need to keep sight of long-term objectives. Remote onboarding and authentication technologies have stood the crisis test and can be quickly deployed (see California EDD's 8-Week Acceleration Plan). The bigger challenge is to steer such quick fixes in desired directions for building trust and resilience in the long term — for example, by mandating adherence to established standards like NIST or eIDAS.

Governments should be more proactive in a changing digital identity ecosystem. Government is no longer the sole authority on identity in a digital context, but it should assume its privileged role as facilitator, regulator or federator. Proactive stance is important to ensure that digital identity developments support, not sideline, policy priorities like personal privacy, national security, universal service access or digital sovereignty (see Trend: Digital Sovereignty in Top Business Trends in Government for 2021).

Actions for Government CIOs:

- Revise your adoption strategy for citizens and government bodies by putting use cases front and center in digital identity plans, e.g., by exploring pressing use cases like COVID-19 vaccination passes.
- Raise trust in citizen digital identity by anticipating and addressing issues that often dominate — sometimes distort — public perception: biometrics, privacy, digital sovereignty.
- Assume a new posture by defining your roles beyond just provider and consumer of digital identity, but also as facilitator, regulator and federator in rapidly evolving digital identity ecosystems.

Trend: Multichannel Citizen Engagement

Back to top

Analysis by Bill Finnerty, Alia Mendonsa

Strategic Planning Assumption: By 2024, over 30% of governments will use engagement metrics to track quantity and quality of citizen participation in policy and budget decisions.

Description:

Multichannel citizen engagement is a seamless, bidirectional engagement with constituents across organizational boundaries while delivering a personalized experience using the preferred and most effective channels to reach constituents. Multichannel citizen engagement uses data to actively monitor the effectiveness of engagement efforts and revises them as needed to deliver a more satisfying set of citizen interactions. It is essential that governments that implement multichannel citizen engagement adhere to regulations and user preferences around the use of personal data.

Why Trending:

Citizen direct participation in the government, particularly at the local level — city councils, school boards — reached new heights in 2020 as communities dealt with the pandemic, civil unrest, wildfires, hurricanes and other events. At the same time, the need for effective communication with citizens and visitors to ensure safety and efficient operations of a jurisdiction has been essential for governments. Where governments successfully accomplish this through the use of a combination of technologies and data, they build trust within communities.

The convenience of digital civic engagement enables the government to effectively engage a more diverse set of constituents. Digital channels provide a data-driven approach to ensure selective outreach to targeted populations, while providing increased capabilities to measure the effectiveness and impact of efforts (see A Practical Guide to Stakeholder Management). By doing so, governments can also improve their digital equity efforts, a top business trend for the government.

Implications:

Investment in a multichannel communications platform to enable engagement with constituents across preferred channels will be essential to improving engagement efforts.

Governments should invest in a multitude of engagement tools, approaches and instruments to create holistic engagement plans that leverage in-person, remote, synchronous and asynchronous interactions. Failing to do so will create an imbalanced weighting of population segments.

Actions for Government CIOs:

- Consider data architecture, technologies and marketing techniques when developing an effective multichannel engagement strategy to enable program areas to deliver a consistent message across all channels. When present in the organization, work with communications to achieve this goal.
- Establish standards for instrumenting communications to collect supporting data for engagement metrics. Work with business leaders to establish and clearly communicate to engagement teams and stakeholders a set of KPIs to ensure that engagement efforts effectively reach the targeted audiences in breadth and depth.

Agile

Trend: Anything as a Service (XaaS)

Back to top

Analysis by Alia Mendonsa, Neville Cannon

Strategic Planning Assumption: By 2025, 95% of new IT investment made by government agencies will be made as a service solution.

Description:

Anything as a service (XaaS) is a cloud-only sourcing strategy that embraces acquiring the full range of business and IT services on a subscription basis.

Why Trending:

Pandemic response and the critical need for digital service delivery have exacerbated the pressures to modernize legacy applications and infrastructure and provide mission-critical capabilities (see Predicts 2021: Governments Tackle Transformation Out of Necessity). Consequently, key service delivery applications, such as unemployment insurance, drivers licensing, tax collection and enterprise resource planning (ERP), proved not to be flexible enough to adjust to quickly evolving scenarios and subsequent policy execution.

In response, cloud-based products and digital services, including CRM, 311, grant management, GIS, and data and analytics platforms, were deployed quickly using cloud delivery models to quickly stand up new digital services. In some cases, these were workarounds to inflexible legacy applications.

Government CIOs and their organizations are increasingly turning to the “as a service” model as an alternative to traditional capital-intensive modernization and investment. According to the 2021 Gartner CIO Survey, 56% of government organizations expect to increase the amount of spend on cloud services and solutions in the coming fiscal year (see 2021 CIO Agenda: Government CIOs Step Up to Action for Digital Acceleration).

Implications:

XaaS technologies can offer a much shorter time to value than traditional on-premises implementations, while also alleviating limited IT resources and capacity, and normalizing IT investment and upgrade costs into operating expense (opex) budgeting practices.

The pace of XaaS adoption in government is quickening as leadership has become more comfortable with cloud delivery models while overcoming concerns regarding security and data ownership (see 2021 CIO Agenda: Government CIOs Step Up to Action for Digital Acceleration).

Government CIOs must strategically manage the shift toward XaaS models for IT applications and infrastructure by reconsidering all elements of the I&T operating model. XaaS changes the financials and tools of I&T and, therefore, requires new ways of working and managing performance (see Establish the Impact of Cloud on Your Organization's Opex and Capex Budgets).

Actions for Government CIOs:

- Identify services currently delivered on-premises that are good candidates for modernization via XaaS delivery models, and prioritize according to stakeholder needs, organizational urgency for specific digital capabilities, IT capacity and skill sets.
- Develop SLAs for both in-house and contracted service performance and proactively monitor and articulate performance metrics to help stakeholders understand the business value being achieved via IT services, regardless of the delivery model.
- Evaluate skill set and competency gaps for managing XaaS IT investments and create a workforce development and augmentation plan that redirects resources to the new skill sets that cloud services technology demands.

Trend: Accelerated Legacy Modernization

Back to top

Analysis by Neville Cannon, Michael Brown

Strategic Planning Assumption: By 2025, over 50% of government agencies will have modernized critical core legacy applications to improve resilience and agility.

Description:

Governments have seen, firsthand, the limitations and risks posed by decades-old legacy infrastructure and core systems. To be better equipped to deal with the next disruption, government CIOs are accelerating the move to systems and the need to adopt modern, modular architectures. Technologies such as public cloud, API management and software-defined networks are used to create the platforms upon which agility and responsiveness can now be built with confidence. Legacy modernization also requires agencies to equally address the historically poor data quality contained within many systems of record.

Why Trending:

The need for legacy modernization is not new to government CIOs, nor is the staff's need for working around inflexible legacy systems working in core agencies. Staff developers, often as shadow IT, work around solutions to adapt to rising constituent needs. Recent COVID-19-related case studies highlight how legacy applications cannot scale or operate at speed and should be protected by the use of cloud-based front-end wrapper technologies (see Case Study: Crisis Delivery of New Furlough Systems for COVID-19 (HMRC)). The use of microservice-based architectures and cloud technology allows vital core systems, such as taxation and social welfare systems, to be replaced over time using agile methodologies (see Application Modernization Should Be Business-Centric, Continuous and Multiplatform). The challenges related to the global pandemic have only served to heighten the awareness of the attendant risks and the need for modernization.

Implications:

Government CIOs will find themselves competing with higher priorities for investment funds to complete this much needed work. Business cases will be heavily scrutinized in an environment where reducing impacts on citizens and businesses will be high on the political agenda. CIOs must balance momentum and lessons learned from risks faced and mitigated with the need to reduce costs and progress at pace.

Many governments are placing increased trust in the hyperscale cloud providers. However, there is an increased tension in some communities about becoming overly reliant on these providers. Efforts are being made in Europe, for example, to create an underlying infrastructure to provide more open competition and increase data sharing and ease of use (see Market Trends: Europe Aims to Achieve Digital Sovereignty With GAIA-X).

Actions for Government CIOs:

- Establish the case for modernization by working with program area leaders to identify risks, costs and missed opportunities related to legacy systems (see Choose the Right Approach to Modernize Your Legacy Systems).
- Develop a modernization roadmap by working with the governance committee/executive to clearly define both the business and technical needs of the enterprise and the operating parameters, such as cloud, data sovereignty and support, needed to access available solutions.
- Assess the solutions on the market by engaging a broad range of vendors in demonstrations and talking with peers in other jurisdictions that have already modernized parts or all of their environment.

Trend: Case Management as a Service (CMaaS)

Back to top

Analysis by Rick Howard, Apeksha Kaushik

Strategic Planning Assumption: By 2024, government organizations with a composable case management application architecture will implement new features at least 80% faster than those without.

Description:

A modular and interoperable approach, case management as a service (CMaaS) is used for the design and development of cloud-based case management solutions as digital products. CMaaS products are developed according to four composable business design principles: modularity, autonomy, orchestration and discovery.

With CMaaS, each process of the case management life cycle — such as intake, assessment, referral, investigation or close — is designed as a collection of application building blocks called packaged business capabilities (PBCs). A case management PBC:

- Encapsulates its own data, rules, interfaces and workflow
- Operates independently of other CMaaS PBCs that are developed and deployed with a low-code application platform.

Why Trending:

Case work is the predominant workstyle of government; as the entire legacy-heavy portfolio of monolithic case management point solutions can be found in many government departments. The brittle and inflexible architecture of these mission-critical applications reinforces operational silos in government; often preventing integrated service delivery. Yet, case management life cycle processes have similar requirements that can be extended from point solutions and packaged as reusable business capabilities to be shared enterprisewide.

As the COVID-19 pandemic made clear, governments must become more responsive, adaptable and resilient when confronting a global crisis, keeping up with accelerating social change or achieving better outcomes for citizens (see Top Business Trends in Government for 2021). CMaaS can build institutional agility in government by applying composable business principles and practices to replace legacy case management systems with modular case management products. A CMaaS strategy ensures capabilities delivered by applications are modular, rapidly and safely assembled, disassembled and recomposed in response to changing business needs.

Implications:

A composable approach to case management modernization — where application capabilities are extracted, encapsulated and surfaced via APIs — enables organizational resilience and faster innovation. These API-wrapped application modules form a platform of PBCs that can be rapidly composed and augmented in multiple patterns to quickly support new:

- Experiences
- Processes
- Partners
- Service models

CMaaS will also necessitate new ways of working through the formation of case management product teams with skills in development, test automation, integration, DevOps and APIs, data analytics and user experience (UX).

As government organizations embrace the concept of a composable business architecture, business technologists, aka "citizen developers," will increase their proficiency in the use of enterprise low-code application platforms (see Forecast Analysis: Low-Code Development Technologies).

Actions for Government CIOs:

- Develop a CMaaS application strategy that is modular, resilient and product-oriented by adopting a composable business architecture, composable technologies and composable thinking to design case management PBCs.
- Support the participation of business technologists and case work end users in developing case management products by adopting low-code platform technologies suitable for fusion team collaboration.

Resilient

Trend: Hyperconnected Public Services

Back to top

Analysis by Irma Fabular, Arthur Mickoleit

Strategic Planning Assumption: By 2024, 75% of governments will have at least three enterprisewide hyperautomation initiatives launched or underway.

Description:

Hyperconnected public services is the whole-of-government use of multiple technologies, tools or platforms to automate as many business and IT processes as possible.

Government CIOs and technology service providers can use hyperautomation principles and practices to develop hyperconnected, highly automated end-to-end business processes and public services that require minimal human intervention.

Why Trending:

The COVID-19 pandemic exposed vulnerabilities and limitations of siloed, vertical service models of government. To address public health and safety emergency measures, government organizations needed to provide essential "contactless" services.

Hyperautomation refers to effective combinations of complementary tools that can integrate functional and process silos to automate and augment business processes. These tools include artificial intelligence (AI), machine learning (ML), event-driven software architecture, RPA, integration platform as a service (iPaaS), packaged software and other types of decision, process and/or task automation tools.

According to Gartner's annual CIO survey, 41% of government CIOs indicate they plan to increase investments in process automation in 2021.

The hyperautomation of government business processes and public service models can increase resilience and flexibility while lowering operational costs.

Implications:

- Hyperconnected public services is a business-driven approach to process transformation that begins with the principle that "everything that can and should be automated will be automated."
- The hyperautomation journey is ongoing and iterative. It will involve numerous business-driven initiatives across government ecosystems and will leverage an extensive array of technologies.
- Hyperconnected public services require investments in new capabilities to manage end-to-end constituent journeys and as well as consistency of employee experience.

Actions for Government CIOs:

- Solicit executive leadership commitments by linking initiatives with operational resilience, economic recovery, and broader digital government transformation strategy.
- Gain support from diverse stakeholders by assigning a product leader who can facilitate collaboration among agencies and with industry partners.

- Generate and sustain momentum and funding support by leveraging political, business and technical “quick wins” in addressing COVID-19.

Trend: Operationalized Analytics

Back to top

Analysis by Ben Kaner, Dean Lacheca

Strategic Planning Assumption: By 2024, 60% of government AI and data analytics investments aim to directly impact real-time operational decisions and outcomes.

Description:

Operationalized analytics in government is the strategic and systematic adoption of data-driven technologies, such as AI/ML and advanced analytics, at each stage of government activity. This shifts government agencies from the dashboard reporting of lagging indicators to predictive decision support, and will help decision makers — from front line to executives — make better context-based operational decisions in real time. Operationalized analytics generate proactive business processes that leverage AI/ML and advanced analytics to improve the quality of the citizen experience.

Why Trending:

Operationalized analytics is trending because of the increased pressure on individual government organizations to:

- Improve the quality, consistency and effectiveness of their services and decision making.
- Shift the focus of service delivery from reactive to proactive.
- Free up knowledge workers by reducing the effort spent doing repetitive administrative tasks or collecting data available by other means.

Operationalized analytics, which guides decisions in real time rather than being a lagging indicator, improves efficiency, effectiveness and consistency of decision making. This improvement started before the pandemic. It delivered results to a more demanding citizenry within constrained budgets that drove AI-driven automation (for example, intelligent process automation) and risk-based case assessment based on ML. Government leaders still deal with challenges associated with oversight, control, accountability and the ability to explain the basis of decisions. Operationalized analytics allows people to remain central to the process yet benefit substantially from additional tools and insights (see Effective Data Governance for Government AI Projects — What CIOs Need to Know).

Implications:

For governments to scale and reap the benefits of digital transformation, CIOs must integrate AI and data and analytics capabilities with service delivery and operational processes while ensuring governance covers data usage and quality. Data generated by citizen-facing applications, ecosystem partners, the Internet of Things (IoT) and back-office systems requires a flexible analytics architecture that supports real-time analysis and AI-based decision support. CIOs must take action that involves integrating disparate information management and security policies into a cohesive framework that fosters a culture of data literacy (see Tool: Enable Data Literacy Through Stakeholder Analysis and Linking to Business Outcomes).

Government CIOs and chief data officers — or equivalent roles — must collaborate to execute an “analytics everywhere” strategy that steadily advances the impact and expands the use of real-time analytics capabilities (see Connect Accountability and Transparency With Government Data and Public Dashboards). This includes adopting pragmatic, just-enough approaches to adaptive governance, data architecture, standards and developing workforce competencies that yield higher business value over time (see Adaptive Data and Analytics Governance to Achieve Digital Business Success).

Actions for Government CIOs:

- Develop a compelling future-state vision of the business value and public benefit of operationalized analytics by building a concise data and analytics strategy aligned with desired business outcomes. Sustain this with adaptive governance practices.
- Demonstrate the effectiveness and efficiency opportunities of operationalized analytics by conducting pilot projects that have immediate impacts on productivity or morale, amplifying human talents and reducing errors. Common examples are corporate services tasks, including HR, payroll or finance.
- Build a roadmap for capability development by assessing AI and analytics capabilities within your organization and across your government and plan to close gaps by contracting with suitable service providers or academic institutions and leveraging cloud-based AI and analytics services.

Trend: Data Sharing as a Program

Back to top

Analysis by Ben Kaner, Arthur Mickoleit

Strategic Planning Assumption: By 2023, 50% of government organizations will establish formal accountability structures for data sharing, including standards for data structure, quality and timeliness.

Description:

Data sharing is often ad hoc, driven by high-profile use cases such as child protection incidents (see Queensland Government Finds Missing Children Using an Automated Data Sharing and Response

System) or gender violence that cannot easily be generalized. Data sharing as a program moves it into being a scalable service, with multiple reusable capabilities, supporting the drive toward more composable approaches in government service delivery.

This needs support from cross-functional data governance, for example, across multiple agencies. Successful ad hoc collaborations provide blueprints for more structured approaches to controlling data value, sensitivity and privacy, as well as more consistent incentives for innovation. This requires balancing decentralized ownership of data, distributed benefits of reuse and central political priorities.

Why Trending:

By 2021, several factors accelerated the need for data sharing to be programmatic rather than project-based. These included a realization that it is the user of data that receives value, while cost and risk lie largely with the provider; increasing prevalence of end-user analytical tools outside historical IT. Some successful examples include France and Scotland. and, of course, many aspects of COVID-19.

COVID-19 drove the need for data sharing that had previously met resistance for years, in just weeks (see Case Study: U.S. HHS Develops Rapid Response to COVID-19 Data Challenge (HHS Protect)). Once through that bottleneck, the challenge becomes leveraging maximum mission value from what is available while managing risk. This requires ongoing management and a well-balanced distribution of labor and risks — for example, between those incubating an idea and those scaling it later. This drives data sharing as a program.

Implications:

Sharing means compromise, and requires:

- All participating parties accept increased risk to data they previously controlled, as well as exposure of data inadequacies, in return for contribution to mission delivery or budget savings (see 4 Steps to Drive Sustainable Value for Government Shared Data Initiatives).
- Political will and balancing of the financial risk. A program has a continuing remit to deliver value and improve over time. It does not need to solve the whole problem at once, and can develop value in proportion to effort (see Smart Data Sharing — Five Insights to Get It Right).

As the organization sees increasing value in leveraging data, the CIO will need to establish policies and guidance for data sharing which support both small and large-scale initiatives and allow for continual escalation, resolution and learning from challenges. This will require a balance of controls versus incentives, and a level of dynamic risk sharing between participating agencies as initiatives evolve.

Actions for Government CIOs:

- Reduce blockers to data sharing by establishing a common policy with agency leaders with whom data is likely to be shared to cover privacy, sensitivity and balance of risk and value between participating agencies.
- Establish senior cover by identifying the main policy- or executive-level beneficiaries from early identifiable use cases, and recruiting them as political sponsors.
- Balance controls with incentives by establishing funding and other support mechanisms (e.g., incubators, catalysts) to stimulate collaboration between stakeholder communities.
- Ensure continuing support with a constant emphasis on discovering new value from existing or accessible data.

Evidence

[1] Designing an Adaptive Security Architecture, Oracle-Sun Microsystems.

[2] FISMA Implementation Project, CSRC, National Institute of Standards and Technology (NIST).

[3] 76% of Cybersecurity Leaders Face Skills Shortage, Security Magazine.

[4] Survey: Cybersecurity Skills Shortage Is 'Bad,' but There's Hope, Threatpost.

[5] The Skills Shortage Presents a Looming Cyber Security Threat, Cyber Security Intelligence.

Document Revision History

Technology Trends in Government, 2019-2020 - 16 September 2019

Recommended by the Authors

Top Business Trends in Government for 2021

Drive Adoption of a Digital Government Technology Platform for Government Transformation

Gartner provides leadership support across the federal, state and local government sectors to help leaders and their teams improve organizational efficiency and drive digital government transformation.

Learn more: gartner.com/en/industries/government-public-sector

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner®