Digital Government 2030: Planning for an Uncertain Future

FOUNDATIONAL **Refreshed:** 10 September 2019 | **Published:** 31 January 2018 **ID:** G00347838

Analyst(s): Dean Lacheca, Cathleen Blanton, Alia Mendonsa, Bill Finnerty

Government CIOs must anticipate and correctly respond to the increasingly disruptive forces that affect their organizations. This research presents four plausible future scenarios to help government CIOs develop digital strategies that can adapt to a rapidly changing world.

FOUNDATIONAL DOCUMENT

This research is reviewed periodically for accuracy. Last reviewed on **10 September 2019**.

Key Findings

- Scenario planning helps government CIOs work with business executives on the strategic plan, and better envision plausible futures that can inform their strategic direction in view of uncertainty and volatility.
- The convergence of multiple forces can profoundly change how governments and society function. Gartner selected two unrelated forces that will significantly impact government operating models in the future — the role that government plays in service delivery, and the acceptance and adoption of artificial intelligence and related emerging technologies.
- Despite a wide divergence among all four scenarios, a common set of critical capabilities emerged from them. These capabilities include provisioning a digital government technology platform, managing the flow of data throughout the ecosystem, and focusing on data analytics capabilities to support varying levels of business process automation and decision making.

Recommendations

Government CIOs developing the digital strategies that guide the transition to digital government should:

- Examine the range of forces that may impact the organization's future, whether technological, political, economic, social and cultural, trust and ethical, regulatory and legal, and

environmental forces. Use strategic planning techniques such as scenario planning and ecosystem modeling to determine the impact of these forces and to develop resilient strategies.

- Ensure investments are future-proofed. Develop a reference architecture, and focus on the management and analysis of data. Coordinate a technology roadmap and investment strategy that lay out an achievable path to a digital government technology platform.
- Lead the cultural change to create a resilient and future-oriented organization. As a first step, adopt and apply Gartner's ESCAPE change leadership model.

Table of Contents

List of Figures

Analysis

Purpose of This Research Series

Governments worldwide face multiple, concurrent global and local forces, including political, social and technological, which are rapidly changing their societies. New technologies are constantly emerging, raising citizen and business expectations, and changing citizen behavior as innovations are normalized. Significant changes in how government services are offered and consumed are inevitable. The rate of change, and the manner and degree of shifts in government's approach to service delivery, is exceedingly difficult to predict with accuracy.

Digital government transformation is a long-term endeavor. Moreover, agility is essential so that governments can adapt to the changes they have anticipated and mitigate the risks of changes they cannot anticipate. Scenario planning is a proven technique used by top-performing organizations to model plausible futures and reveal the strategic choices that are most likely to produce ongoing business value, regardless of which scenario emerges.

The Value of Scenario Planning for Government CIOs

In an uncertain environment, with many near-term priorities, the purpose of such a long-term exercise may not be immediately evident. Economic cycles, societal changes, elections and major disruptive events make a 13-year time horizon impossible to predict with precision. And yet, this scenario-planning research does lead to specific actions that government CIOs must take now to ensure tactical enhancements are coordinated toward a long-term vision for digital government that can support and sustain various government service styles. Scenario planning is an invaluable tool for:

- Engaging imagination to explore the unpredictable
- Investigating the combination of trends that can be observed today
- Planning for a range of unexpected possibilities by visualizing extreme cases
- Highlighting central, foundational activities and capabilities that should be invested in and would otherwise be overlooked under the pressure of urgent tactical requirements

Scenario Development Process

Our research approach leverages scenario-planning techniques (for additional background, see Note 1). Such techniques do not lead to a single view of the future, but identify a variety of potential scenarios, as they are created and influenced by driving forces in the economy, technology, society

and politics (see Note 2 for a description of our approach and "Use Scenario Planning to Make Business and IT Strategies More Resilient in an Increasingly Volatile World").

Scenario planning is only one of several tools that should be used in combination to create long-term strategies. Other tools include ecosystem modeling, Gartner Hype Cycles, and top business and technology trends (see "Hype Cycle for Digital Government Technology, 2017").

The first step in this exercise is to identify the critical uncertainty, focal issue or central question that the scenario-planning exercise should answer (see "CEB Ignition Guide to Conducting a Scenario Planning Exercise"). The focal issue for this research, simply stated, is:

> How will government deliver services in 2030?

The second step is to determine the key driving forces and prioritize them. We developed a list of social, technological, economic, environmental and political (STEEP) factors that influence and reshape the future of government, and the forces that we considered the most influential in answering this question. We then ranked those factors, considered dependencies, and selected the two independent forces that are both the most important for the focal issue and the most uncertain.

Role of Government

The first force — role of government — captures the different approaches that governments can take vis-à-vis the regulation of economy and society or the delivery of services. Governments can have a tight grasp or a light touch. For example, the possible roles include:

- Regulator of services (such as for finance, telecommunications, education, healthcare or a subset thereof)
- Controller or payer for services (assuming the services are delivered by commercial enterprises or nonprofit organizations)
- Direct provider of services, including in the case of publicly owned corporations that blur the distinction between the public sector and private sector

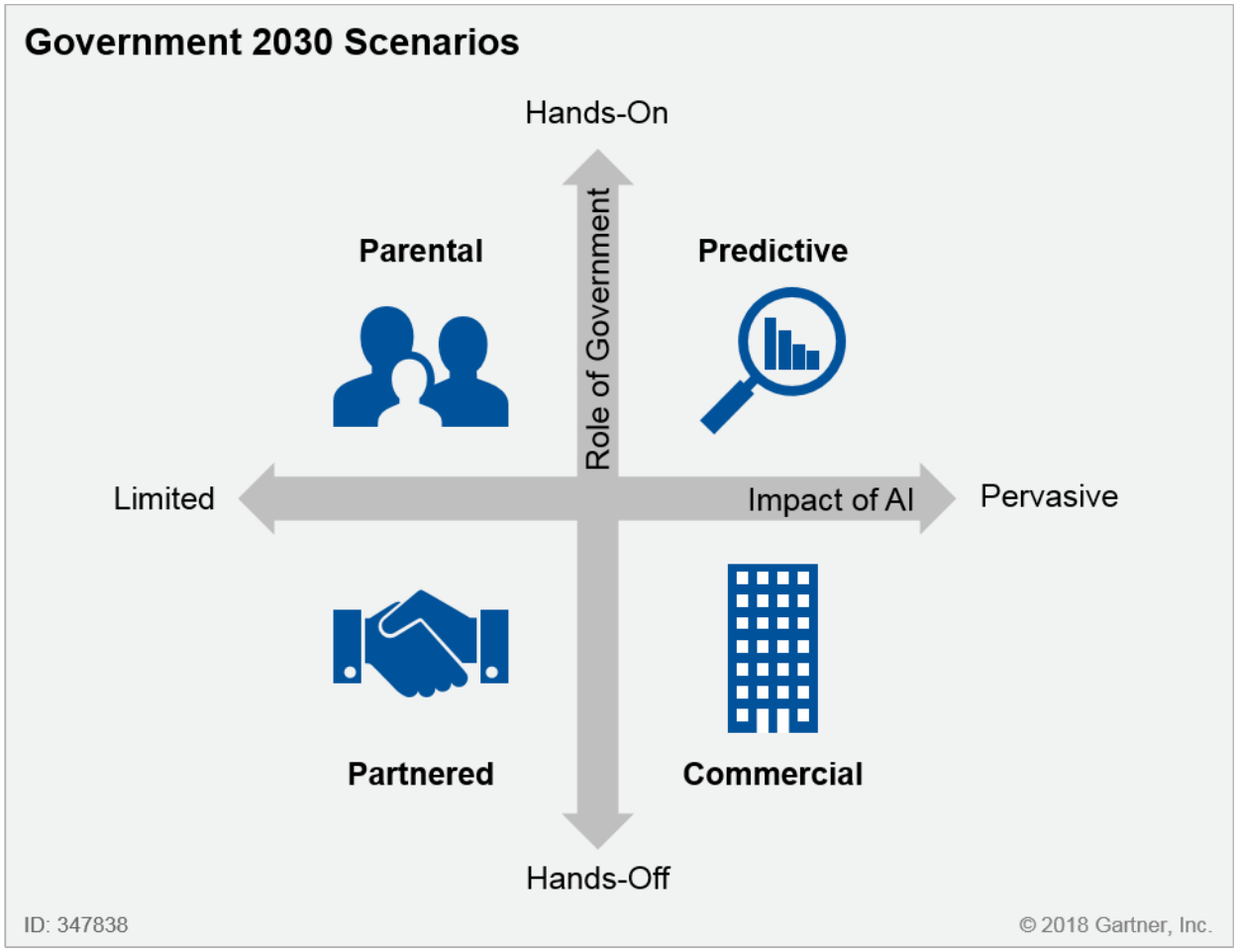
Impact of AI on Society

The second driving force — impact of artificial intelligence (AI) on society — concerns how deeply business operations, people's lives and government services will be affected by the application of AI to all facets of daily living. AI was specifically chosen, because its potential impacts and risks are great, and the potential for diversity in outcomes is high. While technology advances are a certainty, the societal and regulatory consequences and attitudes may vary considerably, from limited to pervasive. AI relies on a combination of technologies that encroach on citizens' privacy and challenge communities' trust in technology-based decision making.

Scenarios for the Future of Government Services

The two extremes of the two driving forces yield four possible scenarios. We have given each scenario a descriptive label for ease of reference (see Figure 1).

Figure 1. Four Long-Term Scenarios for the Future of Government



Source: Gartner (January 2018)

The scenario-planning technique does not attach any probabilities to these scenarios. Instead, each scenario enables an exploration into how future technologies will affect government and, conversely, how the government's service delivery style will influence technology adoption and development, as well as government and private-sector interactions.

Scenario 1: Parental

The parental scenario emerges where the impact of AI and emerging technologies that leverage AI is relatively low, and the government maintains a very hands-on role in the delivery of government-

related services (see "Digital Government 2030: Parental Governments Augment Internal Capabilities").

Familiar to many governments today, this scenario would see an agency focus on iterative innovation without any fundamental changes in the business model. Governments in this scenario will prioritize personalized service delivery and will leverage AI to augment the capabilities of a mobile, hands-on workforce.

Operational excellence will be aimed at improving outcomes for citizens, rather than downsizing workforces. Where technology delivers efficiencies, the additional capabilities will be focused on citizen-facing services. Government IT organizations in this scenario will immerse themselves in the business to develop empathy for the citizen and citizen-facing staff, and government CIOs will be positioned as strategic enablers.

Because governments operating in the parental scenario try to anticipate and personalize citizen services, without relegating decisions to AI, they adopt new technologies where they can improve analytics and government responsiveness to citizen needs. With a large government workforce, digital workplaces and virtual digital workplaces are valued.

Scenario 2: Predictive

The predictive scenario arises where the impact of AI is very high across government, commercial and consumer domains. Government still maintains a very hands-on role in the delivery of government-related services (see "Digital Government 2030: Predictive Government Anticipates Citizen Needs With Autonomous Services").

Governments in this scenario will prioritize personalized service delivery and will leverage AI to deliver services in an AI-powered society. AI will transform the workplace and the workforce. Many traditional jobs across all sectors, including government, will have been automated. At the same time, AI will create new opportunities and new jobs.

The aim of operational excellence will have changed as the size of the workforce has already been optimized. Likewise, cost optimization will be aimed at reducing the need for government services. Government IT organizations in this scenario are now focused on direct business service delivery, and government CIOs will be positioned as business leaders.

Governments operating in the predictive scenario will leverage AI in all aspects of government and constantly seek new sources of data. The concept of using digital twins to organize information, monitor current state, model potential impacts or changes, and power AI, will be extensively used across all government assets and will also be applied to individual citizens (see "Top 10 Strategic Technology Trends for 2017: Digital Twins"). Analytics will be a significant focus of the AI investment, as pre-emptive service delivery is a key to the success of government.

Scenario 3: Partnered

The partnered scenario emerges where the role of government in service delivery is minimized, and the impact of AI is relatively low across the entire community as a result of trust and concerns over

potential employment impacts. In this scenario, government externalizes service delivery, leveraging nonprofit and commercial entities for direct service delivery. Government controls this service delivery through contractual key performance indicators (KPIs) and retains a regulatory role on behalf of citizens (see "Digital Government 2030: Partnered Governments Work to Empower the Ecosystem").

Governments in this scenario will prioritize empowering service providers with access to the right information to deliver highly personal services. Government will leverage AI to augment government staff as they perform their regulatory functions. Many traditional jobs will still exist, but they will now be supported by AI to ensure their safety and effectiveness. As the regulation workload shrinks, operational excellence will focus on improving the overall efficiency of citizen-serving ecosystems.

Government IT organizations in this scenario are now focused on the ecosystem that they regulate and enable, but also depend on to achieve their mission. Government CIOs will be positioned as strategic enablers to the ecosystem.

Governments in the partnered scenario will focus on offering seamless, low-level access to many government services. They will also attempt to monitor the data that flows throughout the ecosystem to understand how effectively citizens achieve their objectives. Like in the predictive scenario, governments are constantly seeking new sources of data to improve their analytics. Analytics remain a focus to measure and enforce contractual KPIs and support regulation.

Scenario 4: Commercial

The commercial scenario emerges where the impact of emerging technologies like AI is very high across government, corporate and consumer domains. Governments in this scenario continue to believe that the community is best served by nonprofit and commercial entities delivering government services. But in this scenario, the prevalence of AI has heightened the need for government to use advanced techniques to regulate the industries on behalf of citizens. The focus is to ensure fair, equitable access to government services and that the community's privacy expectations are met in the AI-driven society (see "Digital Government 2030: Commercial Partners Outpace Governments' Service Delivery").

Third-party service providers in this scenario will prioritize personalized service delivery and attempt to meet all citizens' needs effectively. Governments will have a supervisory, not driving, role in this ecosystem. Governments will monitor the citizen service ecosystems so that they meet citizens' expectations. Governments will leverage AI to perform most of the regulatory functions in real time, and escalate only exceptions that require intervention.

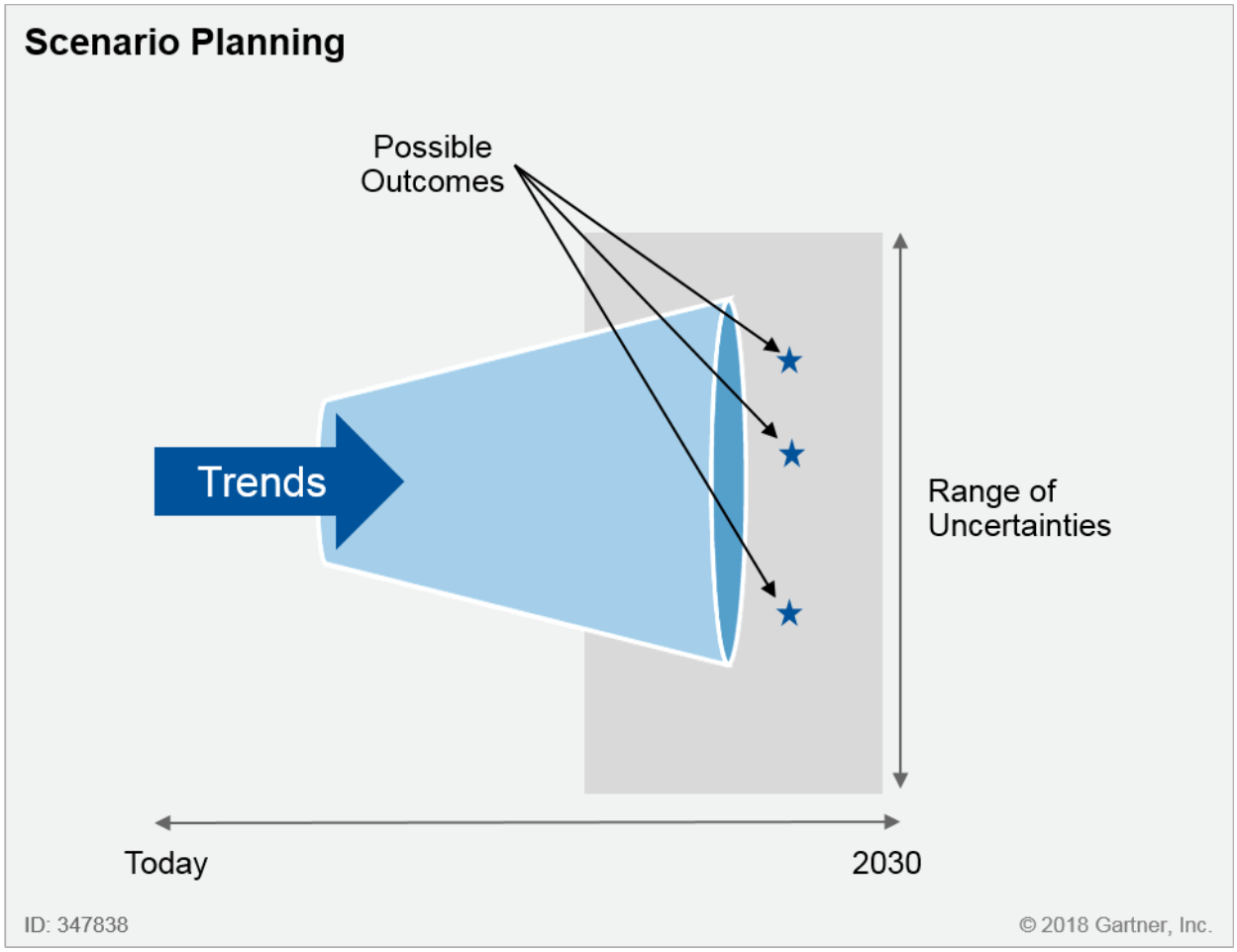
With AI automating most regulation activities, operational excellence initiatives will aim at improving the overall efficiency of the ecosystems that governments support. Government IT organizations in this scenario are now focused on the ecosystems that they support and regulate, and government CIOs will be positioned as business leaders.

Because governments operating in the commercial scenario can regulate in real time, they will need to monitor sentiment and outcomes with advanced analytics. Due to the high acceptance of AI in this scenario, data-driven policymaking and fraud detection will be automated.

How to Use These Scenarios

This collection of research describes how governments can respond to two disruptive trends — one technological and one societal. These scenarios create stories describing plausible future outcomes (see Figure 2) and can be expanded to create citizen journeys and ecosystem models that will help business and mission leaders plan for the future. No value or probability is assigned to any of the scenarios. For the sake of envisioning the future, they are all deserving of consideration.

Figure 2. Scenario Planning Addresses Multiple Outcomes Simultaneously



Source: Gartner (January 2018)

Another benefit of scenario planning is that it surfaces common themes across all scenarios that effectually become stable, useful requirements for the future. For comparison, the summaries of the government 2030 scenario-planning exercise are shown in Figure 3.

Figure 3. Summary of Government 2030 Scenarios

Summary of Government 2030 Scenarios

	Partnered	Predictive	Parental	Commercial
Digital Government Technology Platform	▪ Ecosystem interoperability ▪ IT system modernization ▪ Data and analytics capacity	▪ Complex networks of intelligent things ▪ AI-driven service delivery ▪ Decision automation based on real-time analytics	▪ Citizen experience ▪ IT system modernization ▪ API management	▪ Ecosystem interoperability, including data transfer ▪ AI for policy and compliance supervision ▪ IoT infrastructure scalability ▪ AI-driven transparency in process and data exchange
Cybersecurity	▪ Secure government and service providers through a reluctant use of AI-based cybersecurity ▪ Emphasis on digital ethics and transparency	▪ Defensive and offensive AI-based cybersecurity	▪ Internal cybersecurity team augmented with investments in AI-based cybersecurity tools ▪ Emphasis on digital ethics and transparency	▪ Governance of cybersecurity across the ecosystem for cybersecurity infrastructure and identity management ▪ AI and blockchain to ensure data integrity and block ransomware attacks
Cost Optimization	▪ Business process automation through non-AI methods are used to optimize service delivery and regulation costs	▪ AI-driven automation	▪ Focus on reducing the unit cost of IT through hardware reduction, application rationalization and tighter procurement deals	▪ AI-driven cost optimization by both government and private-sector service providers ▪ Competition among private-sector providers to reduce cost but improve service differentiation
People and Culture	▪ Decentralized government IT focused on contract and vendor management ▪ Difficulties in competing with private-sector companies using emerging technologies for IT and analytics talent	▪ Resource "sharing" used to address scarce specialist talent ▪ Focus on AI and data-driven innovation, rather than direct service delivery	▪ High levels of employment guaranteed by government ▪ Human interactions valued over those provided by machine ▪ Culture that will be challenging as staff seek to maintain their individual worth	▪ All government employees to evolve into generalists who are able to deploy AI, machine learning and virtual augmentation to address tasks across any government function ▪ Transitory government employment, as private-sector compensation and the opportunities of working with emerging technologies entice government employees

ID: 347838

IoT = Internet of Things

Source: Gartner (January 2018)

Common Themes in All Four Scenarios

The common themes identified as part of all four scenarios can be pursued with confidence. They are in areas such as business engagement, digital government technology platform evolution, and skills and competency management, which we discuss below.

Fused Mission of Business and IT

The nature of the business and IT areas vary greatly across the future scenarios. Ensuring the CIO acts as a strategic partner or advisor is a critically important concept that plays out across all four scenarios (see "Information and Technology Strategy for the Enterprise on the Cusp of Digital Business").

Data-, intelligence- and technology-based enablers must be incorporated into the mission strategy to ensure the IT environment is positioned to support the ecosystem and deliver services effectively. In all four scenarios, government interactions with the ecosystem will require better information, better ways of analyzing the information and better ways of interacting with the ecosystem. Therefore, the CIO's role is a critical component of how the government interacts with the broader ecosystem.

Government CIOs need to expand their efforts to build business acumen across all mission areas, not just business efficiencies. They should establish multidisciplinary teams from across the agency in all aspects of service delivery. CIOs should measure their own success and the success of their teams, based on business outcomes. As a business executive, the CIO must help lead the organizational change management that results from technological disruptions by applying Gartner's ESCAPE change leadership model (see "ESCAPE the Past: Six Steps to Successful Change Leadership").

Modular, Flexible, Service-Based Solutions That Underpin Agility

Constant change is evident across all future scenarios. Agility and flexibility are required as opportunities and expectations emerge at an increasing rate. Application modernization efforts will result in applications that offer citizens, suppliers and ecosystem partners a continuous experience across multiple logical and physical channels that emerge.

Whether government interacts directly or indirectly with citizens or ecosystem partners, the expectation is that all services will be resilient and underpinned by a mesh of services that are accessible via robust, reliable, available, scalable, secure and self-healing mediated APIs (see "Adopt a Multigrained Mesh App and Service Architecture to Enable Your Digital Business Technology Platform").

Emerging Technology Capabilities

All scenarios will also need to leverage and manage a variety of emerging technologies for strategic and operational benefit.

Workforce generational change (see Note 3), retirement of legacy technologies and the rate of technological advancement will challenge IT to develop and maintain the right capabilities. Even when the government is not planning to adopt the new technologies, a detailed understanding of how the new technologies could impact government oversight is required to appropriately regulate their use.

Government CIOs must have effective, reliable ways to explore emerging technologies, validate their benefits, and integrate them into business and mission capabilities. Government CIOs will also be responsible for establishing digital KPIs that measure service delivery to help the government plan and ensure the success of initiatives.

Talent Management

Government CIOs will need to expand their scope and evolve their approach to talent management. Delivering new value through emerging technology will require new skills and competencies not only in IT, but also in the business and mission areas.

Managing the government's talents and capabilities will require ongoing investment in experimental programs and bimodal delivery models to upskill the workforce and augment with industry experts and new capabilities shared across the government.

The long-term, iterative nature of transformation means that succession planning and knowledge management will be key to the success of talent management programs.

Focus on the Flow and Analysis of Data

Data is at the core of every future scenario. Integration, data management, security and analysis remain core competencies across all scenarios.

Data volumes will continue to increase as new data from both government and nongovernment sources become more readily available. Managing the flow, classification and storage of the data coming into and out of the agency will be essential to ensuring advanced analytics can deliver the right insights for each scenario.

Augmented analytics will become commonplace, as complex data linkage incorporates an increasingly large number of variables and is used to inform or drive decision making (see "Augmented Analytics Is the Future of Data and Analytics"). In all scenarios, it will be either impossible or impractical to manually explore every possible pattern and determine the optimal action. Analytics tools will increasingly automate reporting and routine analysis, as staff leverage self-service tools that are heavily augmented by AI.

Event stream processing also becomes commonplace, as responsiveness becomes a core expectation for governments enabled by real-time data (see "Technology Insight for Event Stream Processing").

Cybersecurity

Governments must secure their capabilities for a future society with readily available AI capabilities, or they will be marginalized and ignored (see "Cybersecurity Scenario 2025: Outrageous Intelligence"). Regardless of the position that society has taken on AI and machine learning (ML), the technologies themselves lead to increased risk exposures. Governments will need to address this concern by introducing more AI and ML into security risk programs.

Adaptive security architecture will be a required foundational element of solution design. Blocking and prevention capabilities are replaced by an adaptive process to predict, prevent, detect and respond to security breaches (see "Top 10 Strategic Technology Trends for 2017: Adaptive Security Architecture").

Government CIOs need to better leverage agency authorities and leadership skills to address apathetic attitudes to evolving risks, as well as engage across the ecosystems to address indirect risks from partners and consumers.

An Action Plan for Government CIOs

One fundamental principle that emerges from all four scenarios is that IT can no longer take an auxiliary role in strategic planning or expect to align with the mission or business strategy after the fact. Instead, CIOs must establish themselves as trusted business advisors who can innovate in ways that improve overall mission results. To do this, government CIOs must take the following steps.

Conduct a Scenario-Planning Workshop

Government CIOs should take a leadership position as part of the organization's strategic planning process. They should articulate the range of forces that may impact the organization's future and engage executives in addressing them, whether technological, political, economic, social and cultural, trust and ethical, regulatory and legal, and environmental forces.[1]

Government CIOs should use this information and Gartner's government scenario-planning workshop Toolkit (see "Toolkit: Use Scenario Planning to Spark Digital Government Transformation") to lead a scenario-planning workshop within the organization.

The findings from the workshop, combined with the common themes identified in this research, inform the strategic planning process and position IT as a vital part of the process.

Establish a Path to a Digital Government Technology Platform

The identified common themes highlight the importance of a modular platform approach to government services. The themes also highlight the importance of adapting to emerging technologies and focusing on integration and data analytics. Government CIOs should use the strategic planning exercise to reinforce the need for a long-term technology roadmap and investment strategy. CIOs must lay out an achievable, incremental path to a digital government technology platform focused on data, integration and adaptability.

Help Lead the Organization Through Culture Change

CIOs must go beyond advising on and delivering technology upgrades, to establishing themselves as business leaders. Organizations need to be adaptive, resilient and future-oriented to cope with the rate of change and disruption. CIOs can take a lead role in this change management process by applying Gartner's ESCAPE change leadership model as a first step (see "CIOs Need Organizational Change Management and Change Leadership for Digital Business").

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"'CIO Futures' Prepare CIOs for Their Role in 2030"

"Digital Twins Will Impact Economic and Business Models"

"Best Practices for Delivering Targeted and High-Impact Reference Architectures"

"Ten Absolute Truths About Talent Management in Digital Business"

"Cybersecurity Scenario 2025: Outrageous Intelligence"

"100 Data and Analytics Predictions Through 2021"

"2017 Strategic Roadmap for Application Architecture, Infrastructure and Integration"

Evidence

[1] A variation on a PESTLE analysis. See "What Is PESTLE Analysis?" ProcessPolicy.com.

Note 1 Additional Background on Scenario Planning

See P. Schwartz. "The Art of the Long View: Planning for the Future in an Uncertain World." Currency Doubleday. 1996. See also P. Schwartz. "Learnings From the Long View." 30 November 2011.

Note 2 Scenario-Planning Facts

To keep the approach in proper perspective, government CIOs should note:

- Scenario planning is not new. This proven business discipline simply adds a new framework to the process of strategic thinking.
- The scenarios described in this research series represent four different assumptions about the government environment. They are not forecasts, but rather present plausible views of how the future might emerge.

- The four scenarios are distinct, but not mutually exclusive. A government or agency can be involved in more than one scenario at a time, particularly if it operates across different ecosystems or different industry sectors.
- There is no right or wrong, good or bad to these scenarios. They are neutral. The intention is to give an unbiased account of each scenario. The role of a government CIO varies greatly across the four scenarios, which impacts the level of details offered.
- Scenarios are concerned less with predicting the future and more with understanding the environment and the risks and opportunities they present.
- No one scenario will prevail. It is more likely that aspects and influences of each scenario will be seen to exist and persist in parallel.
- The application of the four scenario alternatives can support decision making at many different levels within government, not just within the IT area.

Note 3 Generational Change

There is no exact definition of a generation. As a guide, we refer to millennials (or Generation Y) as those born between 1981 to 1994, Generation Z as those born between 1995 to 2009, and Generation Alpha as those born from 2010 on.

These generational guides and the current constructs of the workforce indicate a significant change in the workforce will occur by 2030. Millennials already dominate in the workforce today and will by 2030 be well-established leaders. Generation Z will also dominate the workforce, and the eldest of Generation Alpha will have entered the workforce.

More on This Topic

This is part of two in-depth collections of research. See the collections:

- Research Roundup for Public Safety and Criminal Justice
- How the Operating Model for Government in 2030 Drives Actions Today

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp