THE RISK OF THE DIGITAL STATUS QUO

How Governments Can Enable Digital Transformation

OCTOBER 2019

PUBLIC POLICY FORUM

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES

PPF

ABOUT PPF

Good Policy. Better Canada. The Public Policy Forum builds bridges among diverse participants in the policy-making process and gives them a platform to examine issues, offer new perspectives and feed fresh ideas into critical policy discussions. We believe good policy is critical to making a better Canada — a country that's cohesive, prosperous and secure. We contribute by:

- Conducting research on critical issues
- Convening candid dialogues on research subjects
- Recognizing exceptional leaders

Our approach — called **Inclusion to Conclusion** — brings emerging and established voices to policy conversations, which informs conclusions that identify obstacles to success and pathways forward. PPF is an independent, non-partisan charity whose members are a diverse group of private, public and non-profit organizations.

1400 - 130 Albert Street
Ottawa, ON, Canada, K1P 5G4
613.238.7858

ISBN: 978-1-988886-77-8

ppforum.ca

@ppforumca

WITH THANKS TO OUR PARTNER

amazon web services
institute

AUTHORS

Dr. Satyamoorthy Kabilan
Former Vice President, Policy, Public Policy Forum

CONTRIBUTORS

Diana Del Bel Belluz
President, Risk Wise

Nicole Foster
Head of Amazon Web Services (AWS) Public Policy (Canada)

Katherine Feenan
Policy Lead, Public Policy Forum

Maysam Ali
Content Lead, AWS Institute

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Governments across the world are reaping the benefits of digital technologies, from creating efficiencies to enabling new services, and enhancing openness and transparency. Embracing technology, however, can be hampered by government leaders' perceptions of and appetite for risk. Leaders tend to focus on assessing the risks and cost associated with embracing new systems and mechanisms and can fail to account for the risks associated with maintaining the status quo.

This paper examines the repercussions of failing to adopt digital technologies to improve public services in Canada. It was informed by a series of interviews, a survey, and a roundtable discussion with senior Canadian public servants. The analysis also drew on the knowledge of 16 current and former government leaders from the United Kingdom, Scotland, New Zealand, Australia, Finland, the United States and Canada to understand the global context around this issue and build new insights into how to overcome this challenge.

There are four key risks associated with maintaining the status quo:

1. **The legacy systems risk** arises from the use of outdated technologies that may no longer be supported by their creators, require special skills to maintain, create barriers to integration with new technologies, and require significant spending to maintain. This risk includes the impact of outdated procurement methods that lead governments to maintain legacy systems instead of seeking newer enabling technologies. Factoring in the legacy systems risk provides a more holistic picture of the price of maintaining the status quo versus moving forward with digital transformation.
2. **The cyber security risk** increases with the use of legacy systems due to the inability to secure them and a lack of updates. Legacy replacement must be framed as a cyber security issue in digital transformation risk assessments.
3. **The culture and people risk** are multifaceted: first, failing to keep up to date with digital transformations may drive away emerging talent in an increasingly competitive and digital labour market. Second, workplace culture can tend to be stagnant, creating a significant barrier to digital transformation.
4. **The risk of service failure** increases as the gap between government service delivery and citizen expectations widen. Failure to embrace expectations could lead to irrelevance, citizen frustration and eventual disengagement.

Governments need to consider the risks associated with maintaining status quo, not just those arising from change and modernization. Strategies identified for dealing with the status quo risk include:

1. **Factor in the cost of legacy maintenance** when considering digital transformation. This should include the skills costs, the risk of losing the ability to understand and support legacy systems and the accumulating technical debt in legacy systems. This additional analysis will provide a much more complete picture around digital transformation decisions and the potential cost savings and risk mitigation to be gained by transformation. Reviewing outdated procurement processes will also enable the consideration of long-term digital opportunities.
2. **Frame the need for legacy replacement as a cyber security issue** to elevate its importance. The potential impact of digital transformation is best assessed when weighed against the potentially greater risk of cyber security issues such as a data breach — and being publicly named and shamed for it.
3. **Factor in the financial cost of cyber security risks posed by legacy systems.** Organizations that are affected by a breach must consider the cost of data loss, business disruption, regulatory penalties and other factors when evaluating the overall costs of digital transformation. This provides a more complete picture of the overall risk analysis for making a change.
4. **Leverage digital transformation to attract and retain talent**. Shifting to a digital workplace culture and embracing flexibility, innovation and rapid technology adoption can reduce the risk of losing or failing to attract skilled workers. In an environment where private and public sectors are competing for the best talent, considering how digital transformation can attract talent is key.
5. **Factor in the risks to government relevance and citizen engagement**, which is now a key performance indicator for many governments. Governments need to improve how they provide services in order to meet the needs of their citizens. Resisting digital transformation risks diminishing citizen engagement.

The status quo represents a substantial risk and should be a core part of the overall risk assessment process for any digital transformation initiative.

INTRODUCTION

The proliferation of digital technologies in the economy has changed the way people receive services and has disrupted many industries including retail, finance and transportation. Digitization has also turned citizens into tech-savvy consumers who expect efficient delivery of government services. But governments still hesitate to fully embrace digital transformation. While the risks around digital transformation have been widely explored, what hasn't been considered as thoroughly is that sticking with the status quo can also carry significant risk.

For government, digital transformation can take many forms, from granting citizens access to existing services online and enabling open access to data, to connecting services across departments and providing citizens with a seamless experience. This, in turn, encourages the development of new or enhanced services that can provide public servants with the digital tools they need to work more efficiently. Governments around the world have responded to citizens' changing expectations by adopting a digital transformation agenda.

Is Canada stalling out?

In 2017, Canada ranked 12th of 60 countries on the Digital Evolution Index, but 48th in digital momentum.

Many government bodies now strive to use digital technologies to deliver the efficient and user-friendly experience citizens are demanding. The Fletcher School's Institute for Business in the Global Context at Tufts University has tracked digital development across 60 countries since 2008. It evaluates countries on 170 indicators to assign a Digital Evolution Index (DEI) score. In the most recent ranking[1], Canada was assigned to the "Stall Out" category, in which digitally advanced nations risk falling behind in development due to their slowing momentum.

Since this assessment, the Government of Canada has created a digital strategy[2] that aims to improve and modernize service delivery through digital transformation. However, this paper posits that ingrained risk aversion among Canadian public servants[3] has created a bias towards maintaining the status quo rather than adopting new technology[4], and that resistance comes with a cost.

[1] Chakravorti, B., and Chaturvedi, R.S. 2017. Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World. The Fletcher School, Tufts University.

[2] The Government of Canada. 2018. Digital Operations Strategic Plan: 2018-2022.

[3] Office of the Auditor General of Canada. 2018. Message from the Auditor General of Canada. Government of Canada.

[4] Aitken, K. 2018. Governance in a Digital Age. The Public Policy Forum.

"Legacy System"

Is broadly defined as an information system based on outdated technologies that is still critical to day-to-day operations

Yes, changing a system, with all the legacy technologies attached to it, can result in massive failures. Look no further than the recent and highly public failure of the Phoenix pay system, recently implemented by the Government of Canada: The Office of the Auditor General of Canada found that the Phoenix pay system is less efficient and less cost-effective than the system it replaced, with thousands of employees inaccurately paid or not paid on time.[5] However, high profile failures like Phoenix can exacerbate the bias against change, making catastrophic outcomes seem much more likely than they are. When the taint of past failures outweighs the perceived benefits of change, this decreases the appetite for risk and creates an overwhelming bias towards the status quo.

However, maintaining the status quo and choosing not to embrace new technologies also comes with significant risks, too. And while the challenges related to transformation have been well documented, the risks associated with sticking with the status quo remain mostly unexplored.[6] These risks can play a significant role in whether an organization chooses to proceed with digital transformation or not.

This paper was informed by a series of one-on-one interviews with key senior IT officials in Canada and other countries, as listed in the Appendix. To study Canada's experience with digital transformation at the staff level, a survey was conducted with IT professionals in the Government of Canada. Finally, the paper benefited from a roundtable discussion hosted by the Public Policy Forum and the Amazon Web Services Institute, which gathered senior public and private sector leaders to discuss risks and opportunities for modernization. Through these interviews, the survey and an examination of recent literature, this initiative explores some of the risks associated with maintaining the status quo as they relate to digital transformation within government in Canada. International interviews and case studies were used to add a broader context and develop strategies for overcoming the status quo.

[5] Office of the Auditor General, 2018. Report 1—Building and Implementing the Phoenix Pay System
[6] Davey, L. 2014. The Status Quo is Risky, Too. Harvard Business Review.

GOVERNMENT IT: THE STATUS QUO RISK

Current and former government officials interviewed identified a host of obstacles to digital transformation. These include:

- A rapidly evolving digital landscape where it is difficult to define a successful strategy, and where the nature, direction and magnitude of potential changes in digital technology shift in unpredictable ways;[7]
- A poor understanding of the digital state of an organization, which makes it difficult to define a path forward for transformation;
- A leadership mindset focused on policy development rather than moving digital transformation forward; and
- A short-term focus based on immediate success requirements and election cycles.

These factors create an environment where government officials view sticking with the digital status quo as the least risky option. Many of the foreign government officials interviewed indicated public servants in their countries share this status quo bias, as well.

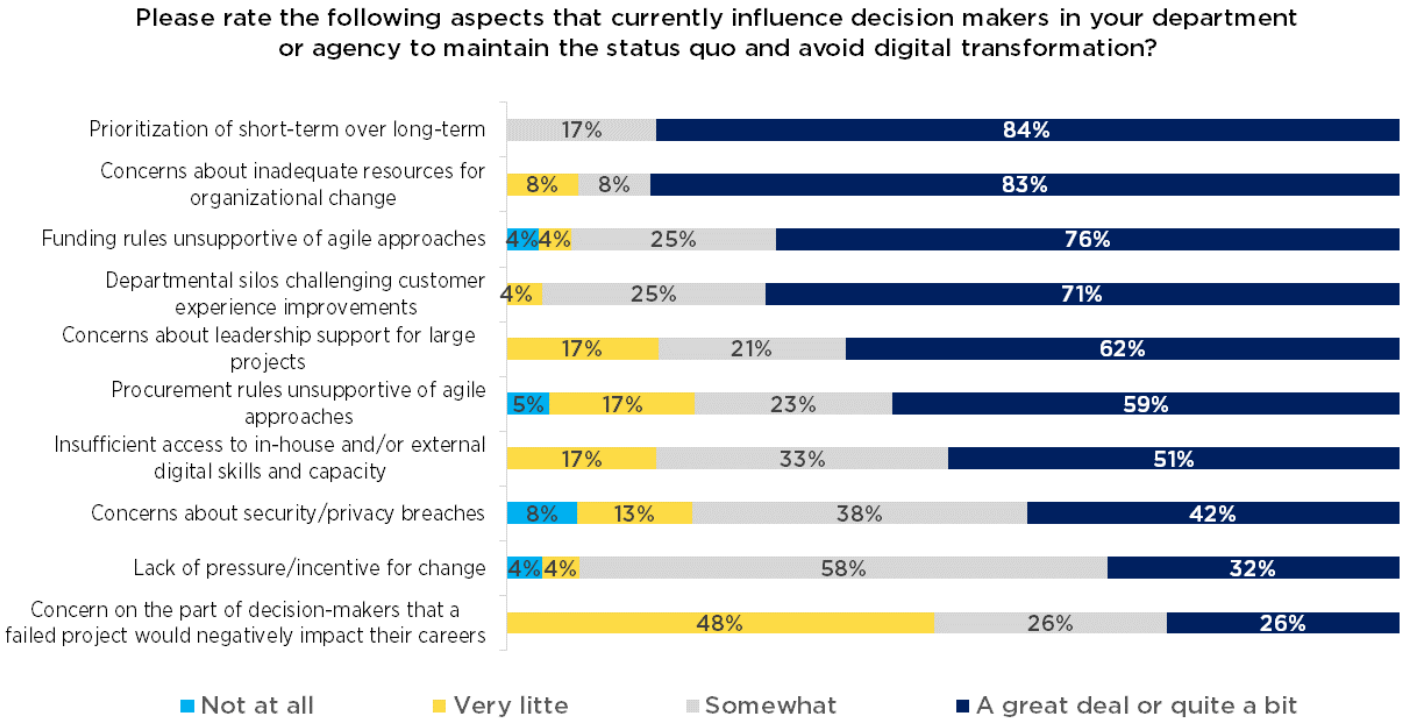
In Canada, the status quo bias is reinforced by a strong aversion to risk and failure, according to a recent report by the auditor general:

> "A large cadre of ministerial political staff give policy advice to the same ministers that deputy ministers are responsible for advising, so it's harder for a Deputy Minister to be heard. This means that it's easier for a Deputy Minister to just implement the will of the Minister without question rather than provide fearless advice on the pitfalls that could arise and how to avoid them. This is how deputy ministers keep the trust of their ministers, and keep whatever influence they have.
>
> The result is an obedient public service that tries to eliminate risk and mistakes, which of course is not possible, so it has to try to avoid responsibility for those mistakes.
>
> In this culture, for a public servant, it is often better to do nothing than to do something that doesn't work out."[8]

[7] This sentiment is further explored in McKinsey & Company, 2019. Navigating a World of Disruption.

[8] Office of the Auditor General of Canada. 2018. Spring Report to the Parliament of Canada: Incomprehensible Risk .

However, our survey respondents[9] show that several factors beyond the fear of failure tend to drive decision-makers to maintain the status quo, as well.



Well-documented risks of digital transformation, combined with a number of structural factors, discourage change, meaning governments tend towards the status quo. However, status quo risks are not discussed as often as the risks of embracing transformation.[10] To broaden that conversation, we have identified four key risks facing governments who stick with the status quo:

1. THE LEGACY SYSTEMS RISK

Legacy systems can be broadly defined as information systems based on outdated technologies that are still critical to day-to-day operations.[11] Discussions with senior government and private sector IT leaders revealed that legacy IT systems are a barrier to digital transformation, IT modernization and the adoption of innovative new technologies. In the United Kingdom, 46 percent of British local authorities' systems are still running software dating to 2000.[12] In many cases, the cost and complexity of modernizing these systems is viewed as a barrier to change. Outdated procurement methods also influence government decisions to rely on legacy systems instead of seeking out newer enabling technologies. Interviewees pointed to

[9] There were 24 survey respondents, 42 per cent of whom indicated their role in digital transformation was to provide executive leadership, while 17 per cent specified that they were responsible for providing technical leadership. The full survey text is available online (see the Appendix for hyperlink).

[10] Davey, L. 2014. The Status Quo is Risky, Too. Harvard Business Review.

[11] Gartner IT Glossary. 2019. Legacy application or system.

[12] Frazzetto, A. 2018. Rewrite or rebuild? 5 legacy system upgrade considerations. CIO.

cumbersome procurement methods, which deter departmental leadership from considering long-term solutions. Instead, short-term fixes to outdated systems seem to be an easier and more cost-efficient path — but keeping such legacy systems in place does come with significant, often overlooked, costs.

According to a recent Information Technology Association of Canada (ITAC) white paper, the continued dependence on outdated legacy systems is also an issue in Canada[13]. ITAC estimates that the Canadian government is spending approximately $12.5 billion per year maintaining outdated IT. These legacy systems may require specialist skills and knowledge to maintain and as the individuals involved in building and maintaining these systems move on or even retire, the ability to continue to maintain these critical systems deteriorates rapidly. Finding workers who know and can maintain bespoke legacy technologies is getting harder and costlier. A rapidly shrinking talent pool must be considered a cost and a vulnerability[14] for the entire system.

Digital consultant Accenture's measure of the U.S. government technical debt — the money it would take to upgrade the legacy systems an organization has accumulated over time — comes to about $1.5 million per application.[15] In 2016, this amounted to $7.5 billion in hardware and software that are reaching end-of-life, without accounting for outdated systems already significantly constraining operations.[16] Such costs only continue to grow.

In the U.K., as one interviewee indicated, there are about 900 different information systems currently used by government and up to 800 of them are considered legacy. Continuing to use, update and repair legacy technology can potentially lead to additional issues related to security, international legislative or standard compliance requirements — such as the European Union's General Data Protection Regulation (GDPR) — and the diminishing capability of these systems to meet user needs.

Maintaining the status quo through legacy systems is becoming increasingly expensive. The costs of maintenance and operations for legacy systems in the U.S. government accounted for 70 percent of the total IT budget, or $85.2 billion, in fiscal year 2018 compared to 68 percent in fiscal year 2015.[17] Digital transformation may, in fact, be a lot cheaper and less risky once the real costs of legacy systems are factored in.

[13] ITAC, 2019. Developing a commercial first approach.
[14] Ibid.
[15] Accenture. 2018. Decouple to Innovate.
[16] Miller, J. 2016. Why $39,000 shows why the IT modernization effort matters so much. Federal News Network.
[17] Abel. R. 2019. Looming retirement of legacy system custodians put global IT systems at risk. SC Magazine.

STRATEGY

Factor in the cost of legacy maintenance

When contemplating digital transformation, the costs and risks of continuing to rely on legacy systems need to be a factor. Considerations should include the skills costs, a decreasing ability to understand and support legacy systems, and the accumulating technical debt in those systems. This additional analysis will provide a much more holistic picture around decisions to upgrade and the potential cost savings and risk mitigation to be gained by transformation. Reviewing outdated procurement processes will also enable the contemplation of long-term digital opportunities.

2. THE CYBER SECURITY RISK

One of the major challenges posed by legacy systems is security.[18] Once a piece of technology becomes obsolete, it gets increasingly difficult to protect it and the data it holds from cyber security threats.[19] Having a legacy system within a secure, modern enterprise architecture is akin to having a guarded front door while leaving the back door unlocked. When deciding whether to replace a legacy system, the cost of cyber security breaches needs to be taken into account.

The 2014 U.S. Office of Personnel Management (OPM) breach — one of the largest privacy breaches in history involving the personal details of U.S. government employees — was attributed to the use of legacy systems that could not support data encryption.[20] The breach affected 21.5 million individuals[21] and resulted in the issuing of a $133-million contract for identity theft protection.[22] The cost of credit monitoring alone increased to $416 million in subsequent years and is expected to rise as OPM continues to provide this service to the people affected by the breach.

Likewise, a flaw in a legacy system caused a catastrophic data breach of U.K. telecommunications company TalkTalk in 2015, leading to the theft of 157,000 customers' bank details and personal information, as well as a then-record-breaking fine from the U.K. Information Commissioner's Office of £400,000.[23]

There are numerous examples where continued reliance on legacy systems and tools has resulted in major data breaches, security issues and/or legal ramifications. With the global average total cost of a single

[18] DeBrusk, C., Mee, P., and Brandenburg, R. 2018. The Marriott Data Breech. Oliver Wyman.

[19] Frazzetto, A. 2018. Rewrite or rebuild? 5 legacy system upgrade considerations. CIO.

[20] Bisson, D. 2018. Lagging Legacy Systems: How Federal Agencies Are Tackling Old IT. Tripwire.

[21] OPM Cybersecurity Resource Center, https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[22] OPM. Sept. 1, 2019. OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract. OPM News release.

[23] Shephard, A. 2018. "It's the legacy that get's you", warns ex-TalkTalk boss. ITPro.

breach hitting $3.89 million[24], the risks and potential fallout costs of maintaining legacy systems from a cyber security perspective are continuing to rise.

STRATEGIES

Make the need for legacy replacement a cyber security issue

Adding a cyber security lens to digital transformation can elevate the importance of this issue. Greater acceptance of the challenge of digital transformation is more likely when framed against the potentially greater risk of fallout from cyber security issues, such as a data breach — and being publicly named and shamed for it.

Factor in the financial cost of cyber security risks posed by legacy systems

Though it can be difficult to estimate the true cost of a cyber security incident, organizations that are affected must consider the cost of data loss, business disruption, regulatory penalties and other factors when evaluating the overall costs of digital transformation. This additional focus provides a more complete picture of the overall risk analysis of digital transformation.

[24] Ponemon Institute and IBM Security. 2018. 2018 Costs of a Data Breach Study: Global Overview.

3. THE CULTURE AND PEOPLE RISK

A key mantra in digital transformation — repeated in many ways by those interviewed for this study — is that it does not just involve technology. Digital transformation needs to be holistic, encompassing people, processes and culture. As one CIO said: "Digital transformation is a fundamental change in the way you do government and deliver services. Thus, it's a long-term business and culture process. You can't go far wrong if you start with people."

The move to a workplace culture that enables both digital transformation and encompasses rapid technology adoption is understandably difficult. In fact, one in three programs of organizational culture change fail and only a few ever truly succeed.[25] The challenge in dealing with people and unions, as well as the high failure rate of organizational culture change programs, creates an aversion to risk. Whether organizations choose to go down the digital transformation road or not, there is an inherent bias in favour of the status quo in terms of maintaining current organizational culture.

Unfortunately, there are additional risks attached to traditional organizational cultures that have not fully embraced today's digital reality. Workers make employment choices based on workplace culture, organizational values and innovative recruitment strategies.[26] They seek a workplace environment actively embracing a digital world characterized by regular changes and upgrades. Having a digital culture can be a magnet for talent[27] and with the competition to attract employees with technology skills — who tend to be younger — organizations failing to embrace a digital culture run the risk of losing out on talent. This concern was also raised by participants at the roundtable session.

The recent PPF-AWS Institute report on developing Canada's digital-ready public service highlighted how the traditional hierarchical environment and culture in government is not attractive to many younger, tech-savvy employees, especially women.[28] This finding was repeated by those surveyed and interviewed for this project. In fact, as the chart above notes, when asked about aspects influencing decision makers in maintaining the status quo and avoiding digital transformation, 83 percent of those surveyed indicated they were concerned about inadequate resources for organizational change. Half of them said that insufficient access to in-house and/or external digital skills and capacity was a determining factor.

Governments need to provide current and new employees with opportunities to upskill while continually upgrading their technology to support an evolving workplace. Maintaining an organizational culture that does not embrace technological change risks alienating the very skills most needed for today's

[25] Lyons, R. 2017. Three Reasons Why Culture Efforts Fail. Forbes.

[26] The Government of Canada's experimental Talent Cloud platform does provide a new take on public sector recruitment processes and job offering; however, greater attention across government departments and increased funding will be needed for success.

[27] Hemerling, J.; Kilmann, J.; Danoesastro, M.; Stutts, L.; and Ahern, C. 2018. It's Not a Digital Transformation without a Digital Culture. BCG.

[28] Cukier, W. 2019. Developing Canada's Digital Ready Public Service. The Public Policy Forum.

organizations. The added benefit of having tech-savvy employees is that they become advocates for digital change and for adopting new technologies.

STRATEGY

Digital transformation helps attract and retain talent

Shifting to a digital workplace culture that embraces flexibility, innovation and rapid technology adoption can reduce the risk of failing to attract skilled workers. In an environment where private and public sectors are competing for the best talent, considering how digital transformation can attract that talent is key.

4. THE RISK OF SERVICE FAILURE

A key principle emerging across the globe is that citizens want to experience the same level of service and convenience from the public sector as they do from private corporations.[29] This principle has been a driving force for the digital transformation agenda for many governments, including Canada.[30] In the private sector, the failure to meet changing customer needs and demands can lead to loss of business, as competitors step up to offer a better alternative. Over the past decade, not meeting customer expectations has been a key factor in the global digital disruption of many industries.

If governments fail to provide services as expected, and fail to simplify processes using technology, other organizations are likely to step in. As such, governments risk becoming less relevant[31], and ultimately less trusted, if citizens feel forced to seek out alternative sources to better support their needs in a digital environment. As former Treasury Board president and minister for Digital Government Scott Brison stated: "Today, more than ever, companies and governments need to understand their core purpose. Otherwise, they'll be irrelevant before they know it."[32] Ultimately, "we can't be a Blockbuster government serving a Netflix citizenry."[33]

While the risks around digital transformation may hold government departments back from change, this needs to be balanced against the risk of losing relevance and trust. Interviewees pointed to the importance of focusing on delivery as today's consumers expect it: basic services need to be provided in a digitally seamless manner across government departments. Services are currently fragmented, with citizens having

[29] Bertrand, A. 2019. How does digital government become better government? EY.
[30] Treasury Board Secretariat. 2019. Digital Operations Strategic Plan: 2018- 2022. Government of Canada.
[31] May, K. 2017. Government relevance at stake in digital age. iPolitics.
[32] May, K. 2018. Driving digital transformation of government. This time they mean it. iPolitics.
[33] Ibid.

separate touchpoints with services, after the birth of a child, when moving and when handling the death of a loved one, often in different physical locations and requiring that they provide the same information over and over. Providing easy-to-access and seamless service offerings will lead to a more positive interaction with government. Technological solutions could be used to enable a single-step approach that automatically sends information to several departments seamlessly rather than requiring citizens to provide the same information to multiple departments.

STRATEGY

Factor in the risks to government relevance and citizen engagement

Citizen engagement has become a key performance indicator for many governments. Governments need to be concerned about their relevance and should regularly review how they provide services. Resisting digital transformation risks diminishing citizen engagement. Governments should consider this outcome as they weigh the risks of maintaining the status quo.

CONCLUSION

Digital transformation presents a range of challenges, particularly for governments. The Government of Canada has been focused on delivering digital transformation, but our research has shown that a number of barriers remain. While there has been a significant focus on the risks associated with embracing digital transformation, sticking with the status quo is far riskier and ultimately more costly in the long run. Factoring in the risks of the status quo as part of the assessment process for digital transformation, especially in the four aspects we have described, will give a more realistic view of the overall risk around digital change.

Substantial risks posed by maintaining the status quo — including the reliance on legacy systems, increasing cyber security vulnerabilities, creating barriers to attracting digital talent, potential service failures, and disengagement through the lack of digital service delivery — illustrate why government leaders need to reassess their perception of risk when considering digital transformation. Lessons learned from governments around the world show that, ultimately, proceeding with digital change is the less risky choice.

APPENDIX - METHODS

ROUNDTABLE

The roundtable took place Jan. 30, 2019. Participants included senior government decision makers, academics and private sector representatives.

INTERVIEWS

Interviews took place between late-January and mid-February 2019. In order to protect confidentiality, interviewees are not named; however, those who participated represent the following organizations:

International participation:

- Scottish government
- U.K. Ministry of Justice
- Ark (U.K.-based education charity)
- Government of New Zealand
- Australian government
- Ministry of Finance, Finland
- U.S. Customs and Immigration Service

Canadian participation:

- Bank of Canada
- Treasury Board Secretariat
- Centre for Data Innovation at the B.C. provincial government
- Canada Health Infoway
- Shared Services Canada
- Transport Canada
- Agriculture and Agrifood Canada
- Canada Mortgage and Housing Corporation

SURVEY

The survey was in field from March 6-23, 2019. Of 176 survey recipients, we received 24 complete responses. Survey recipients were from a range of provincial, federal, and international government departments and agencies. The survey was conducted in English only.

To read the complete survey questionnaire, please visit:
ppforum.ca/publications/digital-status-quo


PUBLIC
POLICY
FORUM