CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Public Service Culture, Risk Management and Governance: The Prerequisite of Effective Strategic Governance to Realizing Our Digital Ambition

by Ron Lloyd

July 2024

POLICY PERSPECTIVE

PUBLIC SERVICE CULTURE, RISK MANAGEMENT AND GOVERNANCE: THE PREREQUISITE OF EFFECTIVE STRATEGIC GOVERNANCE TO REALIZING OUR DIGITAL AMBITION

by Ron Lloyd

July 2024

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T2P 3V4
www.cgai.ca

ISBN: 978-1-77397-310-4

All organizations, whether public or private sector, have an aggregate risk profile that can be measured between low to high. As the aggregate risk increases over time, eventually it will result in the loss of trust and confidence of an organization's stakeholders, shareholders, or citizens. One of the important objectives for senior executives is to lower the organization's aggregate risk profile to ensure that it continues to retain the trust and confidence of its stakeholders. To accomplish this objective innovation and opportunity are foundational. In the context of the Canadian government, realizing that digital technologies are instrumental in lowering the overall aggregate risk profile of the nation, the Government of Canada's Chief Information Officer (GC CIO) published Digital Ambition 2022.

Digital Ambition 2022 provides a roadmap for government to transition from a pre-2000s digital enterprise to a modern 21st century digital enterprise that leverages cloud, artificial intelligence/machine learning, new security solutions, and embraces new ways of working to deliver modern government services to Canadians. The implications of not realizing the Digital Ambition are significant. From a Canadian citizen's perspective it will mean continued dependency on paper-based processes, poor data security, risks associated with 30-50 year old legacy platforms, inabilities to properly leverage digital solutions in defence and security, with real world implications, challenges recruiting government employees, including members of the Canadian Armed Forces and defaulting to using the phone for government services after your credentials are inexplicably revoked. From a public servant's perspective, the adverse impact on their morale and productivity from not being able to leverage these technologies is equally as important. The observation by the former clerk of the Privy Council Janice Charette that "The public service is still working in what I would describe as analog ways and the world has moved on…" underscores the importance of successfully implementing the Digital Ambition.

In 2023, an update on the progress implementing the Digital Ambition was published. In the update the GC CIO stated "I am encouraged by what we have accomplished as a community in the last year…" with recognition that "there is much more work to be done". Specifically, the update declares that although Canada is one of the most connected countries in the world, it has the lowest usage frequency of digital government services in a recent survey of 36 countries. In addition, Canada continues to drop in the E-Government Development Index from 28th to 32nd according to the 2022 United Nation's E-Government survey. With the government putting such a priority on digital, the question that begs to be asked is why are we not being successful? One of the reasons for the lack of progress is hinted at in the update. It notes the requirement for "driving a systemic shift in culture across government that continues to look at evolution of policy and programs through the service lens with a digital-first mindset".

While culture is certainly an important consideration, the largest impediment to achieving Canada's digital ambition is the outdated and no longer fit for purpose security classification framework of the nation. In order to enable a digital reset and to unlock the digital potential of the nation, the important first step is the adoption a three-tier framework of Official (Official Sensitive), Secret and Top Secret. Even once this all important first decision is made, the

realization of the digital ambition will not be assured unless the numerous supporting policies are also amended to reflect leadership intent. If these supporting policies are not amended, then the digital ambition will not be achieved, and the public service will continue to work in analog ways while the world continues to move on.

As risk is the lens through which all government decisions are made and policies developed, it is important to understand the important role risk management has on public service culture. The implications are significant and overcoming the associated challenges to implement a transformational initiative that spans the depth and breadth of government will only occur if dedicated and effective strategic governance is put in place. The aim of this paper to examine how risk management influences public service culture, decision making and policy development, introduce the concept of an aggregate risk profile, reaffirm that the important first step to enabling a digital reset is the adoption of the new security classification framework, demonstrate that making that decision in of itself will not assure the digital reset it merely unlocks its potential, and finally, define how dedicated and effective strategic governance would enable a more timely and successful achievement of the outcomes articulated in Digital Ambition 2022.

Culture

How many times have you heard the quote attributed to Peter Drucker "Culture eats Strategy for breakfast"? In the intervening decade, the challenges associated with changing culture persist and the Drucker's quote has been expanded in the digital age to "Culture eats strategy for Breakfast, Innovation for Lunch and Digital Transformation for Dinner". The challenge to having a meaningful conversation about culture is that it means different things to different people, particularly when it comes to defining organizational culture as it "resists specific definition as there are countless interpretations across both the public and private sector." As a result of its broad interpretation, culture is often identified as *the* reason why large-scale initiatives fail when in reality there are deeper underlying systemic issues that remain undiagnosed. This is not to say that culture does not have a role, as you need to take it into consideration. However, separating culture from policy is not always easy. This is particularly applicable in the public sector and specifically to the realization of Canada's Digital Ambition.

There are many negative characteristics often attributed to public sector culture that are believed to be the reasons why large-scale transformations or initiatives fail. Characteristics include failing to embrace innovation, its hierarchical construct, risk aversion, and a "cover-your-behind" mentality to ensure promotion, are but a few of the more prevalent. Although, there are always instances of such, in my experience these perceptions are not accurate and even if they were, they would at best be symptoms of the underlying problem. In order to put this in context we need to begin by being honest with ourselves. Bureaucracies deal with innovation and change (risk) like white blood cells deal with infection. If it gets past the first line of defense their purpose is to eradicate it.

A bureaucracies' first line of defense to change and innovation is a comprehensive suite of policies directives, orders, standards, guidelines or any document that defines process, henceforth referred to in aggregate as policies. All of which reinforce the status quo. In order to ensure an understanding of the consequences of not implementing policy, TBS has provided a Framework for the Management of Compliance for its policies, directives, standards and guidelines. As such, being non-compliant with policy represents risk. In order to ensure departments remain compliant with central agency or functional authority direction they will typically put out their own departmental direction which restricts the actions of their employees despite those actions being perfectly compliant with higher level policies. Even more problematic is when divisions inside a department put out their own internal guidance which further restricts the freedom of action of their employees. It is not uncommon for departments to put out documents of hundreds of pages to define internal processes to meet the intent of tens of pages of direction and guidance from a central agency or functional authority. Once departmental policies are implemented, they define the culture and reinforce a belief that this is "what right looks like". It is therefore not the culture that needs to be changed it is the policy suite itself. Changing policy sounds simple, but it is anything but in the context of how government approaches risk management.

Risk Management

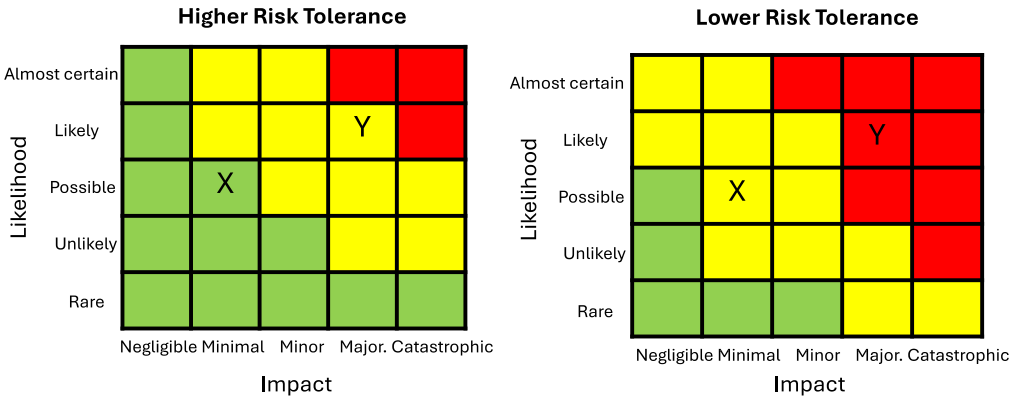
The lens through which all decisions are made and policies developed in the public service is risk management. The Treasury Board has a comprehensive Integrated Risk Management Framework consisting of principles, guides, tools and models. Collectively, effective risk management should:

- support government-wide decision-making and priorities as well as the achievement of organizational objectives and outcomes, while maintaining public confidence;
- be tailored and responsive to the organization's external and internal context including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests;
- add value as a key component of decision-making, business planning, resource allocation and operational management;
- achieve a balance between the level of risk responses, established controls and support for flexibility and innovation to improve performance and outcomes;
- be transparent, inclusive, integrated and systematic; and
- continuously improve the culture, capacity and capability of risk management in federal organizations.

In accordance with this Treasury Board Secretariat (TBS) policy, Deputy Heads of departments are accountable to foster a risk-informed organizational culture that supports risk-informed decision making, enables a dialogue on risk tolerance, focuses on results, and enables the consideration of both opportunity and innovation.

In the Canadian government, departments typically prioritize risks using a matrix (3x3, 4x4 or 5x5) that assesses the probability of a risk occurring and the anticipated impact should it arise. There is no departmental standardization and as illustrated in figure 1, using red, yellow, green to define low, medium and high risks respectively, you can get a sense of the potential variance in its application. In department A an organization with a large risk tolerance as portrayed by the risk matrix to the left, a risk/decision might be considered low, denoted by the X, whereas in department B, a less risk tolerant department portrayed by the risk matrix to the right, that same risk/decision would be considered medium. Similarly, a medium risk/decision in department A would be considered a high-risk/decision in department B as denoted by the Y.

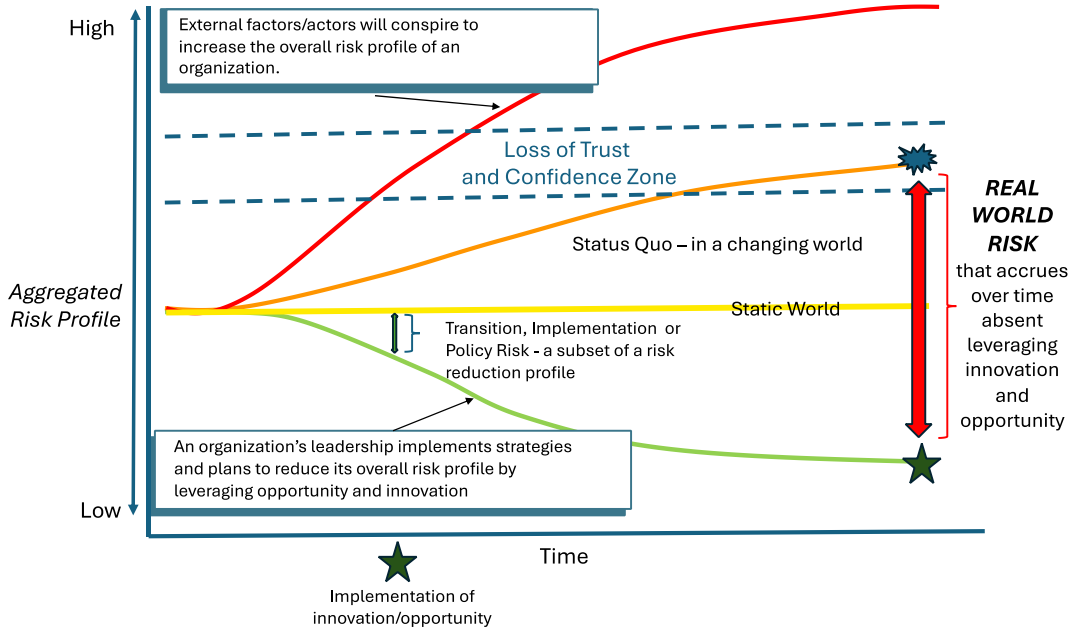
Figure 1: Examples of 5 x 5 matrix and differing risk tolerances.



Not only are there different appreciations of risk across departments, there is often a different appreciation of risk internal to a department between the different levels of management. What middle management may identify as a high-risk activity/decision within their scope, is often a low to medium risk activity/decision on the spectrum of risks a senior executive is managing in the context of their corporate risk profile. It is important to underscore that a departmental or corporate risk profile differs considerably from the concept of an aggregate risk profile. A corporate risk profile identifies the top 5 or 10 organizational risks which are plotted on the risk matrix for senior executive visibility and management. An aggregate risk profile recognizes the complex interdependencies between all risks whether they are low, medium or high.

As discussed previously, all organizations have an aggregate risk profile between low to high. In the context of the Canadian government, the Digital Ambition is aimed at leveraging opportunity and innovation to reduce real world risk to the nation as characterized by the green line in figure 2.

Figure 2: Status quo leads to increased aggregate risk over time



Although there are those that believe it is possible to adopt a risk avoidance posture, such a state does not exist. Either an organization is managing risk or risk is managing the organization as external factors and actors conspire to increase the overall aggregate risk profile of the organization denoted by the orange line. Risk management represents a proactive posture that identifies, accepts and manages "transition risk" to ensure "real world risk" is mitigated as represented by the green and red arrows respectively. Transition risk represents the deviation of a complex tapestry of policies, processes, standards, directives, and guidance documents that have been implemented over years. Whereas the focus should be on the mitigation of real-world risk as an organization, often the focus is on the transition risks identified by departments and functional authorities. Because transition risks are often examined in isolation of the broader aggregate risk to the enterprise, the result is often a status quo outcome.

With respect to risk mitigation activities/postures there is a lower limit which I would define as due diligence. Do the risk mitigation actions meet the threshold of what a reasonable person would do under similar circumstances? It would be exceptionally rare that the threshold of due diligence would not be met by government. At the other end of the spectrum, is the over-mitigation of a risk where the level of investment does not represent value for money, or the opportunity cost adversely impacts the enterprise thereby increasing real world aggregate risk. This occurs more frequently than expected. As central agencies and functional authorities implement policies to mitigate risk across the enterprise it is difficult to understand the total cost of implementation, the opportunity costs associated, second and third order effects, and the impacts of technology over time.

In some instances, a risk mitigation posture for a low risk is actually the root cause of one or several high risks. As the risk is low and mitigated it will not appear on a corporate risk profile nor likely inform risk management conversations. The identification of such policies and their amendment can be extremely challenging in a large bureaucracy. Canada's security classification framework is one of the better examples of such a policy. The adoption of the current security classification framework over 40 years ago significantly constrains the government's ability to leverage modern digital technologies. The important first step to realizing the Digital Ambition of Canada is the recommendation to adopt a three-tier classification framework of Official (Official Sensitive), Secret and Top Secret. If the government were to adopt such a recommendation it would be a clear signal to the enterprise that they wanted to reset how government classified its data holdings, their business impact and their IT security requirements. One of the more important data holdings that would be part of that analysis is personal information because of its importance in delivering citizen centric digital services.

Every day Canadians provide personal information to industry knowing that their data is protected in law by the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA defines personal information and the requirement to ensure its protection. As a result, Canadians do not have to put a security classification on their personal information data when they share it with industry as they know what it is. With respect to personal information provided to government it is also protected in legislation by the Privacy Act. The act very specifically articulates what information constitutes personal information and how government is required to collect, retain and dispose of it. As such, there is no requirement to classify personal information although it is a useful tool. When Canada decided to classify personal information over 40 years ago, it stratified personal information into three categories and correlated it to the existing classification framework that was in place at the time. Protected A data (address, age, race, date of birth and unique identifiers such as social insurance number) was the equivalent in injury to Confidential, Protected B data (medical information, personnel evaluations, individual financial information, and political beliefs and associations) was the equivalent in injury to Secret and Protected C data (life threatening information and serious criminal intelligence) was the equivalent in injury to Top Secret. In comparing how the Canadian government classifies and defines the level of injury of personal information relative to our closest allies and partners, it is clearly evident that based on the level of injury and its associated IT security profile we over classify and over secure personal information.

Because the Canadian framework was established in a pre-digital era the cost of implementation and the opportunity costs were insignificant as the storage and transmission of data at the time were largely physical, including fax and mail. In a digital world the implications are significant. A reset of the classification framework and the IT security profiles that support them, would enable government to mitigate the risks associated with the current state. As discussed previously, the current state is impacted by a culture of overclassification with its attendant negative consequences, precludes leveraging technologies that citizens use every day confident that their data is secure, drives up costs to maintaining the digital enterprise, adversely affects procurement,

decreases interoperability with our allies, constrains collaboration, sharing of data and the ability to leverage new tools such as AI, and many other initiatives codified in Canada's Digital Ambition.

Since Canada's approach to personal information constrains the delivery of modern digital citizen services, revisiting the approach in the context of an aggregate risk profile would be useful. To do so the following questions should be answered:

1. Will the new classification and associated IT security requirements meet privacy legislation requirements?
2. Will the new classification and associated IT security requirements meet due diligence?
3. Will the new classification and associated IT security posture enable as, or more, secure means than faxing or mailing personal information?
4. Will the new classification and associated IT security requirements reflect the standards of our closest allies?
5. Will the new classification and associated IT security requirements meet the security standards that citizen's use every day in their lives whether dealing with industry, provincial or municipal governments?
6. Will the new classification and associated IT security standard decrease high risks elsewhere in the enterprise and mitigate accruing real world risk?

If the answer to all of the aforementioned questions is "yes", then a reasonable person would expect a new classification framework and corresponding new IT security profiles to be implemented to address the aforementioned risks associated with the current construct.

However, as much as amending the new security classification framework and specifically our approach to personal information would lead leadership to believe that they will realize the outcomes articulated in the Digital Ambition, it would still not be guaranteed. The authority to amend the security classification framework is the GC CIO. However, once amended the technical requirements for each of the new classifications is the authority of the Canadian Center for Cyber Security which is part of the Communications Security Establishment (CSE) Canada. Whereas the OCIO is looking to reverse Canada's continued fall in the E-Government Development Index and manage risk in that context, it is likely that the risk calculus in CSE is not focused on digital services but rather the assurance that data is securely protected. Although there is a high probability that the senior executives will be aligned on their risk tolerance to deliver the Digital Ambition there is equally a high probability that their departments are not aligned. If for the sake of argument the departmental risk cultures are similar, I would suggest with equal high probability that those responsible for amending the classification profiles at the working level have a more restrictive risk tolerance than leadership because they are looking at this through the narrow lens of an individual risk as opposed to in the larger context of an aggregate risk profile. This is where culture, or existing policies, could ensure the continuation of the status quo.

The codification of the specific technical requirements for each of the security classifications is IT Security Risk Management: A Lifecycle Approach (ITSG-33). ITSG-33 was released in 2012, and it defined the security control profiles, a collection of technical, operational and management security controls, for Protected A, Protected B and Secret. At some point in time the profile for Protected A was removed and the Protected B and Secret profiles were last updated in January 2015. The fact that the last update was almost a full decade ago is significant because there have been at least three major IT paradigm shifts since then that include cloud, virtualization and containerization. For at least the last decade, the IT security community have treated Protected B and Secret profiles as medium integrity / medium availability as defined in ITSG-33. For IT security professionals this is what "right looks like".

Now imagine a new classification framework is established and personal information that is currently classified Protected B is reclassified as Official: Sensitive. The reason leadership would have done this is to enable a new IT security profile for Official: Sensitive to reflect the significant advances in cyber security technologies, the more accurate calibration of its business impact, and the opportunity to leverage innovation and opportunity. However, if the IT security practitioners believe that adjusting the IT security profile would represent significant risk to the enterprise then they would believe that it is their responsibility to protect it. All that they would be required to do is simply change the name of the Protected B security profile in ITSG-33 to Official: Sensitive. Even if a business impact tool was provided as part of the new classification framework, there is still sufficient latitude for IT security practitioners to justify ongoing equivalency. Put more bluntly, if the responsible agents believe that senior executives and central agencies do not understand their perception of the significant risks that would accrue, there are ways for them to preserve the status quo by another name in order to "protect" the institution. If the OCIO releases Digital Ambition 2028 having changed the security classification framework with a corresponding business impact tool, having amended the privacy impact assessment tool, and having issued new guidance on data aggregation, and yet Canada continues to fall even further in the E-Government Development survey and continues struggling to provide citizen-centric digital services, will we blame culture or the fact that we didn't amend ITSG-33 to reflect the outcomes expected by leadership?

The unfortunate reality is that the security classification policy, and its supporting policies, represent but one of many low-risk mitigation postures that are driving up the real-world risk of the nation. The relevant security, privacy, and contract security program polices have not been substantively updated in over a decade. This likely reflects the hyper-sensitivity associated with making *any* changes to these policies or the fact that the risk management culture that focuses narrowly on risks makes it impossible.

The longer the status quo is maintained in these three areas, the greater the increase in the aggregate risk profile of the nation. The corresponding implications of not enabling the Digital Ambition will mean Canada will continue to fall exponentially behind our allies, partners and potential adversaries increasing the probability of the eventual loss of trust and confidence in government by Canadian citizens and/or our allies and partners. If positioning risk management

in the context of managing an aggregate risk profile enables significant policy changes, the only way that they will be implemented to achieve the outcomes articulated in the Digital Ambition will be the establishment of dedicated effective strategic governance.

Effective Strategic Governance

Governance is a term that is used often but is not well understood nor implemented. Although there are several definitions of governance, for the purposes of this article governance is a leadership led proactive mechanism where appropriate authorities, responsibilities, and accountabilities (ARAs) are delegated and understood, and reporting requirements are established to ensure risks are identified in order to facilitate timely and effective decision making to oversee a line of effort/body of work to ensure the accomplishment of intended outcomes.

The first key attribute of effective governance is that it is leadership led. Governance is about enabling leaders to make timely and informed evidenced-based decisions. Unfortunately, in my experience, governance is seldom leadership led but rather staff led. Characteristics of staff led governance include: agendas are determined by the staff; issues or challenges need to be resolved in advance of meetings (aka the fait accompli brief); staff can remove their item from the agenda or change the reporting cadence; governance is perceived as an actual barrier as opposed to a vehicle where obstacles/barriers are removed; non-decisions often become decisions; minutes/record of discussion/decision are not produced and if they are, are not timely or do not accurately reflect action items/decisions/risks; and finally, there is limited conversation at the meeting. Governance should always be critical to the process but not in the context of protecting it, but rather enabling informed deviation from it, and that is the purview of leadership. There are numerous reasons why governance can become staff led. Reasons include less frequent turnover than leadership, different risk focus (on the process and transition as opposed to real world risk), a narrower interpretation of policies, and a desire to protect their boss and the institution. In order to ensure transition risks do not become the focus of implementing Digital Ambition 2022, it will be critical that leadership is unified and committed to realizing the outcomes intended.

There are typically three levels of governance. Tactical governance typically involves the day-to-day transactional activities required to deliver an outcome which are often informal in nature. Operational level governance is typically codified and consists of the leadership at the programmatic or senior stakeholder level. The highest level of governance is strategic governance.

Strategic governance is comprised of the senior executives (leadership led) who own the outcomes or are the functional authorities who shape and inform them. It is the bridge between different cultures, language, differing risk perspectives, and serves to build trust. Just as bridges require tension to be effective, so too does strategic governance. Effective strategic governance is characterized by healthy and respectful tension as required and at all times underscored by collective trust. Far too often tactical and operational governance become very protectionist and view the world through the lens of win/lose whereas strategic governance attempts to identify

win/wins. As is often said in the military, in times of crisis or conflict it is easy to surge forces but you can not surge trust. As such, it is important to implement strategic governance at the earliest opportunity to establish trusted relationships at the most senior level to deal with unanticipated issues and or a crisis. In times of crisis, strategic governance should be operating at the speed of trust, not meeting for the first time. As decisions are made by individuals, ideally governance committees have a single chairperson empowered to make decisions which are informed by the input of the committee members. For a number of valid reasons, it may be required to have co-chairpersons. However, where there are three or more co-chairs split accountability equaling no accountability is difficult to avoid. In addition, as a result of having three separate staffs involved in supporting the committee the complexity of setting an agenda is exponentially more difficult. Staffs will aim to protect their boss by removing agenda items that they don't believe their boss is well prepared for or have the issue "watered down" to vanilla. Having no chair is not an option because absent a chairperson everyone around the table is actually a co-chair. Put simply, the more co-chairs there are the more difficult it is to "strategically" govern. For large initiatives such as the implementation of the digital ambition, a dedicated strategic governance committee with a single chairperson comprised of the appropriate functional authorities empowered with the appropriate ARAs could and should streamline informed deviation and amendments to mitigate transition risks.

The second attribute of effective governance is proactive delegation. Ideally ARAs are delegated to the lowest possible level of leadership that understand the key outcomes to be achieved and the risk tolerance of the senior executive. This is not to say delegate and disappear, as this is offset by reporting requirements that enable timely decision making. It was my experience that the more significant the change the more significant the reporting requirements. I became convinced that from the moment the team left my office after I gave direction to embark on a change initiative, they would begin to diverge from the outcomes that leadership had intended to be achieved.

The reasons for the divergence are numerous and only in very rare occasions are they malicious. The first reason often stems from communication. Putting direction in writing is tremendously important. The first reason is because it forces the leader to reflect on the outcomes to be achieved, the steps necessary to achieve them and any risks that could be encountered. The second reason is that it provides staff an authoritative document. Unfortunately, although written on paper, it doesn't necessarily mean that everyone will read the direction and subordinate direction often defaults to the spoken word. Five quick reasons for miscommunication - there was what I said, what I wanted to say, what I meant to say, what the team heard and what they wanted to hear.

The realization of the Digital Ambition would benefit from the promulgation of an implementation plan that identifies milestones, proactively delegates ARAs, and synchronizes and phases initiatives to maximize concurrent activity. The development of such a plan would enable the adoption of a Plan, Execute, Measure and Adjust (PEMA) posture. To best mitigate divergence, implementing strategic governance with a bi-weekly cadence would be very effective. This would ensure alignment to leadership's intent, reinforce accountabilities, ensure the focus remains on real world risk while managing transition risk, and ensure key performance indicators

are understood and being effectively measured and activities adjusted. Unfortunately, some interpret an increased reporting cadence as "micro-managing", which it is anything but. Rather, it more accurately reflects adherence to PEMA and the saying "you get what you inspect, not what you expect".

In addition to the establishment of strategic governance the following critical success factors are recommended to mitigate real-world risk and ensure the successful implementation of the new policies required to enable the realization of the Digital Ambition:

- Unified Leadership: Any seams at the DM level will be exploited at the staff level. The level of internal inertia, if not outright opposition, should not be underestimated.
- Stakeholder engagement: Will need to be extensive and participative.
- Communications: Early and often, clear, concise, unambiguous explanation of why the status quo is no longer tenable and the timelines to effect the change.
- Implementation plan: A meticulously detailed and sequenced plan outlining the implementation of each of the recommendations and any dependencies.
- Dedicated team: Although the policy amendments will be made by the staff of the respective functional authorities, the actual implementation will require more than a "from the side of your desk" level of effort. The quality and composition of the team and who they directly report to will be a direct reflection of leadership's commitment to the success of the initiative.
- Accountability alignment: Ensuring that leaders are empowered to make decisions that affect multiple functional authorities and that it is well understood by all stakeholders.

Conclusion

Despite Canada's commitment to becoming a digital nation, the unfortunate reality is that we are struggling to do so. In order to realize our true potential and be competitive globally we need to be successful in leveraging the opportunity and innovation that Canada's Digital Ambition represents. As seized with this undertaking as leadership is, the complexity of their challenge should not be underestimated.

The risk management culture that exists and the focus on transition risks makes it difficult to change policy. Some of the challenges and complexities of amending a single policy and the subordinate policies that would also be required to be amended to enable government to realize its true digital potential have been outlined above. Implementing the numerous policy changes and subordinate guidance documents within the largest single employer in Canada distributed across 22 ministerial departments, 17 departmental corporations, three service agencies, 50 departmental agencies, six agents of parliament, and 12 special operating agencies geographically located from coast to coast to coast is exponentially more challenging. In order to overcome these

challenges effective strategic governance is essential to ensuring the successful implementation of Canada's Digital Ambition.

I believe that Digital Ambition 2022 is a helm order for the nation and in that context, I share the following vignette. When I was a ship's captain or Task Group Commander at the tactical and operational level and I directed the ship, or indeed all the ships, to come 30 degrees to starboard, I would hear a flurry of orders and the ship or task group would come 30 degrees to starboard. When I arrived at National Defence Headquarters as the Commander of the Royal Canadian Navy (RCN) and I directed the team that we needed to bring the RCN 30 degrees to starboard do you know what the response was? "Starboard, why starboard? The status quo and port are also options." So after several weeks of convincing the team that starboard was indeed the correct direction, the next response was "why 30 degrees, that seems significant, perhaps we should ease into this with maybe 5 or 10 degrees". All that to say, at the tactical and operational level an order is an order, but at the strategic level it is a point of departure for a conversation. I have observed that this phenomenon is not unique to the RCN but is also applicable in many large public and private sector bureaucracies. As a nation we have been discussing the Digital Ambition for over two years now and we should be well beyond the conversation stage, to that I say, Starboard 30!

About the Author

Vice-Admiral (Ret'd) ***Ron Lloyd*** *was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38 year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.