

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Chapter 1 : A Government Perspective: Technology Trends | Deloitte US

OMB Circular A provides guidance to Federal agencies on general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, information technology (IT) resources and supporting infrastructure and services.

The focus of Information Technology IT within the federal government is changing. This includes a number of staffing actions at all levels including at the supervisor, manager and executive level. In addition, the directorate was recently re-located within the organization. ITSD officials work with, and support, PSC senior management in carrying out their respective mandates and adjusting to an ever-changing operating and IT environment. The directorate also provides the full range of information management services to the organization. As such, it is important that IT governance structures support IT integration into the organizational governance framework. Strategic level committees act as primary decision-making bodies for the PSC on operational items, including IT expenditures. Operational level committees focus on information sharing, analysis and the provision of advice and recommendations. Furthermore, Corporate Affairs Sector management committee meetings provide a venue for the CIO to have strategic level discussions on IT-related governance and operational matters with the Vice-President and management team. Audit objective and scope 9. The scope does not include information management controls, as these were assessed in a previous internal audit in to IT controls related to financial reporting systems were also excluded, as these were included in an internal review completed at the end of to The following audit procedures were performed: The audit is in conformance with the Internal Audit Standards for the Government of Canada as supported by the results of the quality assurance and improvement program. Audit findings and recommendations Governance structure It was expected that the IT governance structure had defined roles and responsibilities and met Treasury Board requirements see Appendix B. The PSC has an established IT governance framework that forms part of the overall organizational governance structure. Each committee has defined roles and responsibilities that are documented. The processes put in place to manage the relationship with SSC are adequate with some room for enhancement. Two opportunities for improvement were identified related to reviewing committee terms of references to ensure that they are in line with current expectations, and assessing the implementation of the business agreement with SSC to ensure there are no outstanding risks to the PSC. IT governance structure The documentation includes, but is not limited to, the identification of committee members, committee mandates and frequency of meetings. Operational level committees focus primarily on reviewing the technical and architectural aspects of IT , as well as projects that are either primarily IT focused or have an IT component. These committees provide advice to presenters and make recommendations to strategic level committees for decision-making purposes. In March the focus of the EMC retreat was on finalizing sector budgets for fiscal year to , which includes approving the IT budget for PSC and the projects that will receive funding in an IT prioritization exercise. The audit noted some shortcomings that affect the functioning of the IT governance structure. The role of some of the committees was not always clear, and some committee terms of references had not been updated. In addition, the communication of information, analysis, decisions and recommendations among the governance committees was not always considered adequate to support decision-making. The audit team was also informed that the value-added of the strategic committees is at times challenged by focusing on detailed technical or operational decisions that may be better suited at the operational committee level or the CIO directly. For example, some records of discussion and committee documentation did not sufficiently identify and support the recommended approach for particular items. As such, there is an opportunity to improve coordination of information among the committees and improve records of discussion to support decision-making processes. This is of particular interest due to the high level of new hires in the past year within ITSD , from the working level and through the levels of management. This review should include assessing the manner in which records of discussion are

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

documented to ensure clarity of the issues, the advice provided and the expectations of the next level committee review. Management of the relationship with SSC A particular goal is ensuring that the budgeted work can be performed in a given time period to prevent potential funding lapses. The management of the business operations component involves regular meetings with members of the team under the Director of IT Solutions Engineering and Service Management, and the Manager Infrastructure and Operations team. The audit team was informed that the PSC does not receive metrics regarding service delivery from SSC in accordance with provisions established in the business agreement. In order to risk manage this situation, ITSD officials have put compensatory controls in place to obtain some information to review services obtained from SSC. For example, ITSD officials have built relationships with their SSC colleagues through joint meetings, and they obtain some information and data through these sources. The audit team was also informed that there is a concern that the PSC may not be receiving sufficient support from SSC for new development projects. This could have a significant impact on key PSC IT -related projects on the horizon that have government-wide implications. IT policies, procedures and guidance It was expected that the PSC had IT policies, procedures and guidance in place that were aligned with Treasury Board policy requirements. The PSC has policies, procedures and guidance in place that support consistent IT application that are aligned with Treasury Board policy requirements. A number of internal policy and guidance documents have not been recently updated. The CIO is awaiting publication of the new Treasury Board IT policy framework in order to assess the extent to which internal PSC policies will have to be renewed, updated or cancelled. IT policies and procedures In the past, the PSC developed a suite of internal IT policies and guidance documents to support and supplement Treasury Board policies and directives. The audit found that some of these internal policies had not been recently updated. For example, internal policies related to IT security and IT governance had not been updated since The recent approach taken within the PSC is to only review and update internal IT policies when a change or update is identified or required. The CIO informed the audit team that since Treasury Board officials are currently reviewing and updating all IT policies and related directives, the goal is for ITSD to perform a detailed review of all existing internal policy and guidance documents once the new Treasury Board policy suite is published. IT governance risk management The PSC has effective processes in place to manage and mitigate IT risks related to the achievement of corporate objectives. ITSD specific operational risk management processes that clearly identify directorate specific risks and mitigation strategies have not been fully documented. In addition, there are effective processes in place to manage IT risks from a project perspective, including through the governance committees. Furthermore, the CIO must assess risk mitigation strategy implementation in response to corporate risks and report on progress. While ITSD provides input into overall corporate risk discussions, a formal, documented approach to identifying directorate-specific risks to successfully supporting business owners in achieving IT -related objectives and potential mitigation strategies has not been formally documented. Some examples of IT operational risks not currently captured in corporate risk documents include: For IT projects and projects with an IT component, there were effective processes in place at the PSC to identify, manage and develop mitigation strategies to reduce the likelihood and impact of identified risks materializing. As such, the audit found that IT -related projects risks were managed effectively on a project-by-project basis. It is recommended that ITSD formally document operational risk analysis, reporting and monitoring processes to provide clarity on ITSD -level risk management and the effectiveness of proposed mitigation strategies performed. Application portfolio and enterprise architecture management It was expected that the PSC had an application portfolio and enterprise architecture management framework that enabled business and IT alignment. An opportunity was identified to review and update enterprise architecture process documentation through the EMC -approved Enterprise Architecture Program investment. The audit noted that there is a risk that overlaps or gaps may exist in the distribution of responsibilities related to production release schedule approvals, or the comprehensiveness and adequacy of the processes in place to support the discharge of responsibilities related to how analysis is to be carried out when architectural change involves security considerations. The audit team was informed that the transition of the ARC from a

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

decision-making body to an advisory body has presented some challenges to members understanding their roles and responsibilities. The transition means that ARC members will have to focus on providing advice, which requires members to consider issues from a broad, horizontal perspective, and committee members need to be able to have both an operational and strategic perspective to provide value-added comments. In addition, the ARC is not always able to perform its advisory function effectively due to the document processes that are in place to support committee deliberations, particularly regarding project documentation. The lack of clear documentation standards is exacerbated by the fact that there is a relatively high level of turnover of committee members. The audit team was informed that the Enterprise Architecture Program Implementation Project, which is planned to be completed in , may address elements of documentation standardization. ITSD officials have developed processes on an ad hoc basis to mitigate some of the above-noted concerns. However, there has been no formal mapping or documentation of revised processes. Without proper documentation, there is a risk that expected procedures may not be understood or followed, which could impact ARC member architectural review processes and decision-making. Application portfolio management It is recommended that ITSD continue to review key enterprise architecture policy and guidance documentation as per the EA program project to ensure that they are up-to-date and support the effective management of enterprise architecture within the PSC. Overall, the PSC has an adequate management control framework in place to govern IT operations and mitigate corporate and IT project risks. The processes in place to manage the relationship with SSC are adequate with some room for enhancement. Four areas for improvement are identified in the report. The first relates to reviewing the mandates and terms of references of existing committees to ensure that they are in line with current expectations. A second area is in regards to assessing the implementation of the business agreement with SSC to ensure that there are no outstanding risks to the PSC. Finally, there is an opportunity to improve the documentation related to the enterprise architecture processes. Four recommendations are made in the report to address these opportunities for improvement. This review should include assessing the manner in which records of discussion are documented to ensure clarity of issues, the advice provided and the expectations of the next level committee review. Management agrees with this recommendation. The terms of reference documents will be presented and approved at their respective committees. With a high number of software assets not aligned to future Enterprise Architecture standards, EMC member support will be provided to help ensure a streamlined software asset portfolio that is effective and cost optimized.

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Chapter 2 : Policy on Information Management- theinnatdunvilla.com

However, as information may be directly provided by public institutions, public service providers and public decision makers through ICT, the role of CSOs and media seems to shift more towards investigation as a verification of information shared by public decision makers.

The way we manage information technology IT , security, data governance, and privacy has rapidly evolved since A was last updated in This data is duplicated, stored, processed, analyzed, and transferred with ease. As government continues to digitize, we must ensure we manage data to not only keep it secure, but also allow us to harness this information to provide the best possible service to our citizens. It also establishes general policy for IT planning and budgeting through governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. In particular, A focuses on three key elements to help spur innovation throughout the government: Real Time Knowledge of the Environment. In such a setting, the Government cannot afford to authorize a system and not look at it again for years at a time. In order to keep pace, we must move away from periodic, compliance-driven assessment exercises and, instead, continuously assess our systems and build-in security and privacy with every update and re-design. Throughout the Circular, we make clear the shift away from check-list exercises and toward the ongoing monitoring, assessment, and evaluation of Federal information resources. To keep pace with the needs of citizens, we must constantly innovate. As part of such efforts, however, the Federal Government must modernize the way it identifies, categorizes, and handles risk to ensure both privacy and security. Significant increases in the volume of data processed and utilized by Federal resources requires new ways of storing, transferring, and managing it Circular A emphasizes the need for strong data governance that encourages agencies to proactively identify risks, determine practical and implementable solutions to address said risks, and implement and continually test the solutions. This repeated testing of agency solutions will help to proactively identify additional risks, starting the process anew. Citizens are connecting with each other in ways never before imagined. From social media to email, the connectivity we have with one another can lead to tremendous advances. The updated A helps to ensure everyone remains responsible and accountable for assuring privacy and security of information “ from managers to employees to citizens interacting with government services. This update to Circular A underpins many of the policies and technological advances the Federal Government has undergone thus far. And it reflects the extensive thoughts and feedback of the public and stakeholders across government and industry. Find out more about the revised and updated A Circular via the fact sheet below. Tony Scott is the U. Anne Rung is the U. Managing Information as a Strategic Resource OMB Circular A provides guidance to Federal agencies on general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, information technology IT resources and supporting infrastructure and services. The revised Circular consolidates in one guidance document a wide range of policy updates in information governance, acquisitions, records management, open data, workforce, security, and privacy. In particular, the revisions highlight requirements from the Federal Information Technology Acquisition Reform Act to improve the acquisition and management of information resources. The revised Circular also emphasizes and clarifies the role of both privacy and security in the Federal information lifecycle. Importantly, the revised Circular represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial components of a comprehensive, strategic, and continuous risk-based program. The updated Circular promotes innovation, enables information sharing, and fosters the wide-scale and rapid adoption of new technologies while protecting and enhancing security and privacy. Responsibilities for Protecting and Managing Federal Information Resources This Appendix establishes minimum requirements for Federal information security programs and assigns responsibilities for the security of information and information systems. It also establishes minimum requirements for Federal privacy programs, assigns responsibilities for

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

privacy program management, and describes how agencies should take a coordinated approach to implementing information security and privacy controls. Among other things, these revisions require agencies to: Perform ongoing reauthorization of systems replacing the triennial reauthorization process to better protect agency information systems; Continuously monitor, log, and audit user activity to protect against insider threats; Periodically test response procedures and document lessons learned to improve incident response; Encrypt moderate and high impact information at rest and in transit; Ensure terms in contracts are sufficient to protect Federal information; Implement measures to protect against supply chain threats; Provide identity assurance for secure government services; and, Ensure agency personnel are accountable for following security and privacy policies and procedures. While Appendix I focuses on both security and privacy, Appendix II is devoted to summarizing the responsibilities for Federal agencies managing information resources involving PII. Among other things, Appendix II summarizes requirements for Federal agencies in the following areas: The prior version of Appendix II which was historically issued as Appendix I described agency responsibilities for reporting and publication under the Privacy Act of

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Chapter 3 : Managing Federal Information as a Strategic Resource | theinnatdunvilla.com

Information Technology Governance Guide. and further emphasized in the Federal Information Technology Acquisition Reform Act of The Service Engineering.

E-government Although the two terms are often used interchangeably, there is a difference between e-governance and e-government. E-government refers to the use of the ICTs in public administration which, when combined with organizational change and new skills, are intended to improve public services and democratic processes and to strengthen support to the public. However, e-government has no provision for governance of ICTs. The governance of ICTs typically requires a substantial increase in regulation and policy-making capabilities, as well as additional expertise and opinion-shaping processes among various social stakeholders. The perspective of e-governance is "the use of the technologies that both help to govern and have to be governed". Ideally, the government will automatically recognize the importance of achieving this goal in order to maximize its efficiency. Furthermore, e-government uses one-way communication protocol whereas e-governance uses two-way communication protocol. Statistical information published by governments and global bodies do not always reveal the facts. The best form of e-governance cuts down on the unwanted interference of too many layers while delivering governmental services. It depends on good infrastructural setup with the support of local processes and parameters for governments to reach their citizens or end beneficiaries. A budget for planning, development, and growth can be derived from well laid out e-governance systems. The relevance of BI Analytics has brought forth a paradigm shift in assimilating and visualizing huge chunks of data in near real-time manner. The pivot of all good decision-making systems is correct, up-to-date and compliant data. Governments not only want the transformation of their own country and countrymen but also expect improved relations and healthy trade across the world. Development should be transformative and continuously evolving. Internal as well as external IT systems should work in tandem with government policies and procedures. Data Analytics has the ability to change the color and complexion of the world. E-governance should induce up-to-date information, initiate effective interaction, and engage with transparent transactions in compliance with rule of law, thus enabling a sustainable transformation model. The public-private partnership PPP -based e-governance projects are hugely successful in India. Many countries implement e-government policy in an attempt to build a corruption -free government. Government to citizen[edit] The goal of government-to-citizen G2C e-governance is to offer a variety of ICT services to citizens in an efficient and economical manner and to strengthen the relationship between government and citizens using technology. There are several methods of government-to-customer e-governance. Two-way communication allows citizens to instant message directly with public administrators, and cast remote electronic votes electronic voting and instant opinion voting. Transactions such as payment of services, such as city utilities, can be completed online or over the phone. Mundane services such as name or address changes, applying for services or grants, or transferring existing services are more convenient and no longer have to be completed face to face. The Federal Government of the United States has a broad framework of G2C technology to enhance citizen access to Government information and services. The Digital States Survey ranks states on social measures, digital democracy , e-commerce , taxation, and revenue. The report shows Michigan and Utah in the lead and Florida and Idaho with the lowest scores. Much like states, cities are awarded for innovative technology. The Single Point of Access for Citizens of Europe supports travel within Europe and Europe is a initiative supporting an online government. Main focuses are to provide public information, allow customers to have access to basic public services , simplify online procedures, and promote electronic signatures. Taiwan has top ranking G2C technology including an online motor vehicle services system, which provides 21 applications and payment services to citizens. Such G2C communication most often refers to that which takes place through Information and Communication Technologies ICTs , but can also include direct mail and media campaigns. G2C can take place at the federal, state, and local levels.

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Customers identified the following barriers to government-to-customer e-governance: For gaming trade show, see Global Gaming Expo. E-governance to Employee partnership G2E Is one of four main primary interactions in the delivery model of E-governance. It is the relationship between online tools, sources, and articles that help employees maintain communication with the government and their own companies. E-governance relationship with Employees allows new learning technology in one simple place as the computer. Documents can now be stored and shared with other colleagues online. Some of the benefits of G2E expansion include: E-payroll " maintaining the online sources to view paychecks, pay stubs, pay bills, and keep records for tax information. E-benefits " be able to look up what benefits an employee is receiving and what benefits they have a right to. E-training " allows for new and current employees to regularly maintain the training they have through the development of new technology and to allow new employees to train and learn over new materials in one convenient location. E-learning is another way to keep employees informed on the important materials they need to know through the use of visuals, animation, videos, etc. It is usually a computer-based learning tool, although not always. It is also a way for employees to learn at their own pace distance learning , although it can be instructor-led. Maintaining records of personal information " Allows the system to keep all records in one easy location to update with every single bit of information that is relevant to a personal file. Examples being social security numbers, tax information, current address, and other information [11] Government-to-employees abbreviated G2E is the online interactions through instantaneous communication tools between government units and their employees. G2E is one out of the four primary delivery models of e-Government. Governments have now tried to use the efficiencies of their techniques to cut down on waste. E-government is a fairly broad subject matter, but all relate to how the services and representation are now delivered and how they are now being implemented. Historically, many governments in this sphere have only been reactive, but recently there has been a more proactive approach in developing comparable services such things as e-commerce and e-business. Recently that has all changed as e-government begins to make its own plan. Not only does e-government introduce a new form of record keeping, but it also continues to become more interactive to better the process of delivering services and promoting constituency participation. The framework of such an organization is now expected to increase more than ever by becoming efficient and reducing the time it takes to complete an objective. Some examples include paying utilities, tickets, and applying for permits. So far, the biggest concern is accessibility to Internet technologies for the average citizen. In an effort to help, administrations are now trying to aid those who do not have the skills to fully participate in this new medium of governance, especially now as e-government progressing to more e-governance terms. An overhaul of the structure is now required as every pre-existing sub-entity must now merge under one concept of e-government. As a result, Public Policy has also seen changes due to the emerging of constituent participation and the Internet. In practice, this has led to several responses and adaptations by interest groups, activist, and lobbying groups. This new medium has changed the way the polis interacts with government. Editorial[edit] The purpose to include e-governance to government is to means more efficient in various aspects. Whether it means to reduce cost by reducing paper clutter, staffing cost, or communicating with private citizens or public government. There are both internal and external advantages to the emergence of IT in government, though not all municipalities are alike in size and participation. In theory, there are currently 4 major levels of E-government in municipal governments: Simple information dissemination one-way communication Two-way communication request and response Service and financial transactions Integration horizontal and vertical integration Political participation The adoption of e-government in municipalities evokes greater innovation in e-governance by being specialized and localized. The level success and feedback depends greatly on the city size and government type. A council-manager government municipality typically works the best with this method, as opposed to mayor-council government positions, which tend to be more political. Therefore, they have greater barriers towards its application. Council-Manager governments are also more inclined to be effective here by bringing innovation and reinvention of governance to e-governance. The results are indicating that most governments are still in either

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

the primary stages 1 or stage 2 , which revolves around public service requests. Though application of integration is now accelerating, there has been little to no instigating research to see its progression as e-governance to the government. Overview[edit] Government-to-Government abbreviated G2G is the online non-commercial interaction between Government organizations, departments, and authorities and other Government organizations, departments, and authorities. Its use is common in the UK , along with G2C , the online non-commercial interaction of local and central Government and private individuals, and G2B the online non-commercial interaction of local and central Government and the commercial business sector. G2G systems generally come in one of two types: External facing - joining up multiple Governments IS systems - an example would include the integration aspect of the Schengen Information System SIS , developed to meet the requirements of the Schengen Agreement. Objective[edit] The strategic objective of e-governance, or in this case G2G is to support and simplify governance for government, citizens, and businesses. The use of ICT can connect all parties and support processes and activities. Lodging tax returns, applying for services and grants. To alter the national transition from passive info access to individual participation by:

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Chapter 4 : Governance - Wikipedia

governance of ICT in the Public Service. This was confirmed by the Auditor General's (AG) information systems review of governance of ICT in government conducted in.

Metagovernance[edit] "Metagovernance" is the "governing of governing". It is important to note that there are no clearly defined settings within which metagoverning takes place, or particular persons who are responsible for it. Examples of this include the publishing of codes of conduct at the highest level of international government, [27] and media focus on specific issues [28] at the socio-cultural level.

Collaborative governance A collaborative governance framework uses a relationship management structure, joint performance and transformation management processes and an exit management plan as controlling mechanisms to encourage the organizations to make ethical, proactive changes for the mutual benefit of all the parties.

Security sector governance Security sector governance SSG is a subpart concept or framework of security governance that focuses specifically on decisions about security and their implementation within the security sector of a single state. SSG applies the principles of good governance to the security sector in question. In the case of a business or of a non-profit organization , for example, good governance relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility, and proper oversight and accountability.

Good governance Good governance is an indeterminate term used in international development literature to describe various normative accounts of how public institutions ought to conduct public affairs and manage public resources. These normative accounts are often justified on the grounds that they are thought to be conducive to economic ends, such as the eradication of poverty and successful economic development. Unsurprisingly different organizations have defined governance and good governance differently to promote different normative ends. The World Bank defines governance as: An alternate definition sees governance as: Governance has been defined as the rules of the political system to solve conflicts between actors and adopt decision legality. It has also been used to describe the "proper functioning of institutions and their acceptance by the public" legitimacy. And it has been used to invoke the efficacy of government and the achievement of consensus by democratic means participation.

Measuring governance is inherently a controversial and somewhat political exercise. A distinction is therefore made between external assessments, peer assessments and self-assessments. Examples of external assessments are donor assessments or comparative indices produced by international non-governmental organizations. An example of a peer assessment is the African Peer Review Mechanism. One of these efforts to create an internationally comparable measure of governance and an example of an external assessment is the Worldwide Governance Indicators project, developed by members of the World Bank and the World Bank Institute. The project reports aggregate and individual indicators for more than countries for six dimensions of governance: The following domains, in the form of indicators and composite indexes, were selected to achieve the development of the WGI: The project examines to what extent governments can identify, formulate and implement effective reforms that render a society well-equipped to meet future challenges, and ensure their future viability. The OBS is a comprehensive analysis and survey that evaluates whether central governments give the public access to budget documents and provide opportunities for public participation in the budget process. While the OBS is released biannually, the IBP recently released a new OBS Tracker , which serves as an online tool for civil society, the media, and other actors to monitor in real time whether governments are releasing eight key budget documents. The Open Budget Index data are used by the Open Government Partnership , development aid agencies, and increasingly investors in the private sector as key indicators of governance, particularly fiscal transparency and management of public funds. Publishing performance reports openly on the Web in a standard, machine-readable format is good practice for all organizations whose plans and reports should be matters of public record.

DOWNLOAD PDF INFORMATION TECHNOLOGY, GOVERNANCE, AND THE FEDERAL PUBLIC SERVICE

Chapter 5 : Management and Oversight of Federal Information Technology

Public Service Delivery: Role of Information and Communication Technology in Improving Governance and Development Impact Abstract The focus of this paper is on improving governance through the use of information and communication.

Chapter 6 : Welcome to IT Dashboard | IT Dashboard

Definition: Information technology (IT) governance consists of the leadership, structures, and processes that enable an organization to make decisions to ensure that its IT sustains and extends its strategies and objectives [1].

Chapter 7 : IT Governance (ITG) - Gartner IT Glossary

The Department of Homeland Security Science & Technology Directorate conducts technology scouting, horizon scanning, and market analysis to identify, recommend, and report on emerging technologies and start-ups in the marketplace that may apply to the department's mission.

Chapter 8 : Audit of Information Technology General Controls Phase I – IT Governance - theinnatdunvilla.com

The Federal Information Technology Acquisition Reform Act, passed by Congress in December , is a historic law that represents the first major overhaul of Federal.

Chapter 9 : Government of Canada information management - theinnatdunvilla.com

information technology governance practices of the organizations that pertain to the policies, procedures, and standards used for application development and service provisioning, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services, should.