For Official Use **GOV/PGC/EGOV(2013)1**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **21-Oct-2013**

English - Or. English

PUBLIC GOVERNANCE AND TERRITORIAL DEVELOPMENT DIRECTORATE
PUBLIC GOVERNANCE COMMITTEE

OECD E-Government Project

Draft OECD Principles on Digital Government Strategies: Bringing Governments Closer to Citizens and Businesses

This draft of the "OECD Principles on Digital Government Strategies: Bringing Governments Closer to Citizens and Businesses" includes comments provided by a Task Force composed of 13 OECD member countries of the OECD Network on E-Government.

The draft will be discussed by the members of the OECD Network on E-Government at the OECD E-Leaders 2013 meeting:"ICT Governance to Deliver Public Value" , in Bern (Switzerland) on 29-30 October 2013.

Ms. Barbara Ubaldi (tel: +33 1 45 24 15 26; email: barbara.ubaldi@oecd.org)

JT03346827

TABLE OF CONTENTS

Figures

WHY ARE DIGITAL GOVERNMENT STRATEGIES NEEDED?

1. This document introduces draft "Principles on digital government strategies: bringing governments closer to citizens and businesses" for discussion by the Public Governance Committee (PGC).

Background: A changing digital governance context.

2. The steady integration of new technologies (e.g. cloud computing, social media, mobile technology) into the everyday lives of businesses, governments and citizens ("digital by default"[1]) is giving rise to new forms of public engagement and relationships that overlap across public, private, and social, spheres in a new digital governance environment. The shift from a ***citizen-centric*** to a ***citizen-driven model*** of digital government is also opening-up governments driving a move from "networked governance" (internal co-ordination and collaboration) to "collaborative and participatory governance" (more open forms to engage institutional and non-institutional stakeholders in public value creation). This shift offers opportunities for new joined-up approaches to face "wicked" problems – challenges of great complexity seemingly unresolvable by individual actors; and is changing public expectations of their relationship with governments and governments' ability to deliver public value.

3. But are governments really equipped to meet the new public expectations? Realising the value proposition if ICTs requires governments to reform processes and governance mechanisms in order to make use of information and of the communications channels made available. Data collection, analytical work and country reviews completed by the Public Governance and Territorial Development Directorate (GOV) show that governments are looking for ways to align technological opportunities with public demands for better performance and more openness, and to strengthen the ties between e-government and the broader reform agendas. But the Directorate's work also outlines that many governments are still following a logic of simply putting existing processes and products online, while many face challenges related to legacy ICT systems established during the first waves of digitisation of public information and services.

4. Governments can no longer afford to solely focus on governing and managing ICT to improve efficiency in service delivery, processes and outputs, and to anticipate citizens' needs. In the context of the economic and financial crisis, the new dynamic shows the importance of ICT use not just for improved service delivery and internal public sector efficiency, but also as a driver for economic growth, social equality, and governance outcomes of greater transparency, integrity and citizen engagement. The new digital environment raises new risks and challenges that require governments to re-examine their governance approaches in light of the new possibilities and expectations. The challenge is not to introduce ICTs into the public administration; it is how to adapt public sector digital processes, operations and frameworks to the rapidly changing dynamics and relations between people and organisations already enabled by the digital environment. New digital government strategies are needed to harness new technologies in order to create a new service environment, new joined business models, new organisational arrangements that add value for citizens and businesses, modify the cost structure of services, enable new economies of scale, and introduce many-to-many communication channels.

5. Unsuccessful ICT projects, privacy and security breaches, and loss of citizen confidence are just some of the possible consequences for governments who fail to make the transition. For this reason, strategies for effective digital governance need to reflect public expectations in terms of economic and social value, support return on ICT investments, and spur open and participatory governments to maintain public trust.

6. Trust in government, one of the main themes of the OECD 2013 Ministerial Council Meeting, is one of the most precious national assets. Public support can help mobilize ambitious and innovative government policies. While the level of trust obtained in each country depends, to some extent, on its history and culture, the three pillars of the Principles can help governments to increase the level of trust from the public. The Principles will help member and non-member countries to become more resilient and to foster forward-looking public institutions.

The Principles: Using ICTs to bring governments closer to citizens and businesses.

7. **Using new technologies as strategic drivers for open and participatory governance.** ICTs have become one of the most important vectors for making governments more transparent, open, and inclusive – a critical priority in a context where levels of trust in public institutions are declining or unchanging in several OECD countries. In addition to strengthening the accountability of government, increased openness enables new forms of collaboration with external actors and non-institutional stakeholders, as well as new forms of governance within and across levels of government. This is necessary to create open dialogue, real engagement and collaboration, to enable citizens to choose between policy options and improve social inclusiveness and sustainable growth. At the same time, governments need to understand the impact of technological choices on the privacy and security of both government and users. In order to maintain and enhance a trust relationship, governments are expected to take up the new opportunities provided by new technologies to spur open and participatory governance, while tackling the associated risks.

8. **Enabling joined-up approaches to deliver public economic and social value.** A second set of principles assist governments in taking the strategic decisions needed to move from 20th century connected societies (using technology to do things better or more efficiently) to 21st century interconnected societies (using technology for innovative problem-solving and public engagement). In the new context, the paradigm has widened from government as provider of services, solutions and responses, to encompass government as an enabler and convener for delivering public value. The newly evolving citizen-driven approach requires governments to organise themselves around citizen expectations and needs rather than their own internal logic and needs. This requires strategic coherence across ICT policies and strategies, supported by new governance frameworks that join up various actors and political commitment to new approaches, and bring down government silos.

9. Maximising the impact and results of ICT investments. The third set of principles helps governments ensure that their own capacities, norms, structures and risk management models, are aligned with their strategic ICT vision, and vice-versa. The multiplication of technological options and solutions provides answers to new and recurrent problems, but it can also pose new risks for governments if they are unprepared for the new technological reality. For example, in choosing between cloud computing and more traditional ICT systems and solutions. In order to do so, governments must first understand the risks involved, as well as their own needs, cost structures, capacities, legal and cultural barriers and existing business models.

10. In assisting governments in taking the strategic decisions needed to address the challenges listed above, the Principles support national e-government agendas in going beyond the goal of "doing more with less" (*i.e.* showing productivity gains of ICT investments, demonstrating that they help addressing staffing pressures), to a long-term perspective of using ICT and digital policies to deliver public value and to do things better, maximising returns on investment by involving new actors, new models and new relationships.

How does the PGC Recommendation complement other OECD instruments?

11. The changes in the digital governance context and the pervasiveness of technology in the delivery of public services are requiring new stakeholders across government to have a role in strategic decision making on ICT investments, technology use and deployment in the public sector. Key actors from co-ordinating units, sector ministries, and public agencies will find the Principles relevant to improve ICT effectiveness for delivering public value and strengthening citizen trust. In this regard, the Principles support a shared understanding within the public sector and with stakeholders on how to prepare for and get the most out of technological change. The Principles apply to all OECD member countries and provide also useful guidelines for non-member countries strongly concerned by challenges and good practices related to ICT use in the public sector, *i.e.* e-government.

12. The principles cannot be seen isolation. They are intended to be used in conjunction with other OECD policy guidance and tools. Specifically, the PGC draft Recommendation complements and provides a specific context for the application of:

C(80)58/FINAL - Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

C(95)21/FINAL - Recommendation of the Council on Improving the Quality of Government Regulation.

C(98)70/FINAL - Recommendation of the Council on Improving Ethical Conduct in the Public Service Including Principles for Managing Ethics in the Public Service.

C(2002)131/FINAL - Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security.

C(2007)68 - Recommendation of the Council on Electronic Authentication. C(2008)36 - Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information.

C(2008)105 - Recommendation of the Council on Enhancing Integrity in Public Procurement.

C(2008)35 - Recommendation of the Council on the Protection of Critical Information Infrastructures

C(2011)155 - Recommendation of the Council on the Protection of Children Online.

C(2011)154 - Recommendation of the Council on Principles for Internet Policy Making.

C(2012)86 - Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships.

C(2012)7 - Recommendation of the Council on International Mobile Roaming Services.

13. Each existing instrument contains guidance relevant for e-government. The Principles on digital government strategies offer guidance on how to make the most of digital opportunities to create public value and mitigate risks related to: quality of public service delivery, public sector efficiency, social inclusion and participation, public trust, and multi-level and multi-actor governance.

14. The Principles are organised in three pillars:

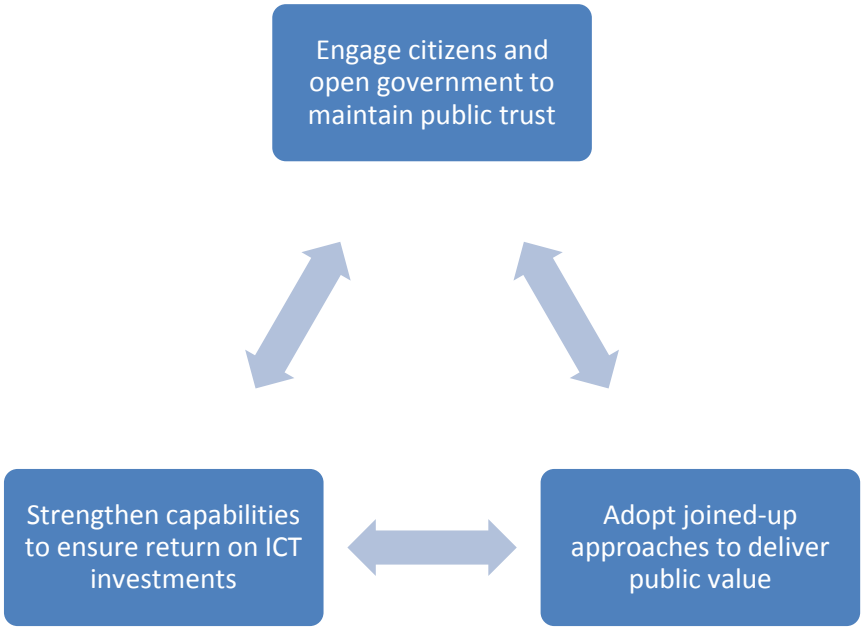
- ***Pillar I*: Engage citizens and open up government to maintain public trust.** This pillar underlines the actions needed to exploit the potential and minimise the risk of using technology, and new technologies in particular, for open, participatory and ubiquitous public sectors where institutional and non-institutional actors can engage and collaborate with governments.

- ***Pillar II:* Adopt joined-up approaches to delivering public value.** This pillar focuses on the strategic importance of coherent ICT use across the public sector. As the infrastructure of the 21st Century, ICT systems, standards, and services enable joined-up and agile administrations capable of adopting whole-of-society approaches to create public value. A coherent approach to ICT requires organisational and governance frameworks that secure political support, and enable and facilitate collaboration.

- ***Pillar III*: Strengthen capabilities to ensure return on ICT investments.** This pillar highlights the conditions for ensuring success in ICT decision-making and management. The proliferation and complexity of ICT solutions can lead to failure of ICT projects, duplicative or ill-adapted systems or poor procurement decisions if governments fail to provide an architecture, an enabling environment and a participation framework for the use ICTs to deliver public value.

15. Once approved by the Council, the PGC commits to monitoring the implementation of the Recommendation and to report thereon to the Council no later than three year following its adoption and regularly thereafter, in consultation with other relevant OECD Committees.

Figure 1. The OECD Principles on Digital Government Strategies: Bringing governments closer to citizens and businesses.



Source: OECD.

Timetable for developing the policy instrument

March 2012	The PGC Network on E-Government mandated the OECD to develop an instrument on e-government.
April 2012	The PGC approved the development of the Principles.
May 2012-August 2013	Drafts 1-2 prepared in consultation with a Task Force of volunteering country delegates.
August – October 2013	Consultation with: - Task Force OECD Member countries - GOV
October 2013	Discussion of draft principles at E-Leaders 2013
December 2013	- Deadline for receipt of comments on the draft principles from OECD member countries - Consultation OECD wide stakeholders (e.g. Directorates, CISAC, BIAC, TUAC, etc).
March 2014	Presentation of the Draft to the Public Governance Committee
Q2 2014	Finalisation of the draft principles
Q3 2014	Final principles presented to the Council

DRAFT "OECD PRINCIPLES ON DIGITAL GOVERNMENT STRATEGIES: BRINGING GOVERNMENTS CLOSER TO CITIZENS AND BUSINESSES".

Pillar 1: Engage citizens and open up government to maintain public trust

Principle 1. Promote the use of ICT for greater transparency, openness and inclusiveness

- *Make ICTs a key part of the strategy to foster transparency, openness and inclusiveness of government processes and operations.*
- *Take steps to address existing digital divides and avoid emergence of new forms of digital exclusion.*

Principle 2. Encourage engagement and participation in a multi-actor context

- *Use ICT opportunities to be inclusive and engage with public, private and civil society stakeholders to create public value in the policy-making process and in service design and delivery.*
- *Establish a digital governance ecosystem.*
- *Create a data driven culture in the public sector.*

Principle 3. Establish the right conditions to strengthen confidence in digital government services

- *Take the necessary steps to strengthen public confidence on privacy protection and security.*
- *Establish criteria for balancing privacy and security considerations with the benefits of the Internet to its users (external and internal).*
- *Balance the need to be a provider of timely and reliable official information with the opportunities that come with sharing imperfect data.*
- *Review existing regimes for privacy and security and align them with related national and international efforts, including on measuring impacts.*

Pillar 2: Adopt joined-up approaches to deliver public value

Principle 4. Adopt a government-wide digital government strategy

- *Develop and adopt a strategy to ensure a coherent use of ICT within and across policy areas and levels of government in support of a common vision.*
- *Promote engagement of various stakeholders in providing input for the definition of the strategy.*
- *Seek complementarity, alignment and mutual reinforcement between digital government strategies and other public administration reforms and relevant sector strategies.*

Principle 5. Ensure leadership and political commitment

- *Secure top political level support and commitment to the national digital government agenda.*
- *Ensure that the vision statement embedded in the strategy is linked to broader public sector reform and policy objectives.*

Principle 6. Establish effective organisational and governance frameworks

- *Identify clear responsibilities within the public administration to ensure overall co-ordination.*
- *Establish organisational mechanisms and governance frameworks to co-ordinate use of ICTs within and across levels of government.*
- *Establish a framework for interoperability.*
- *Adopt mechanisms that enable proper "check and balances" to reinforce accountability.*
- *Strengthen international co-operation to better serve citizens and businesses across borders.*
- *Share knowledge to learn from success stories, but also from failures.*

Pillar 3: Strengthen capacities to ensure return on ICT investments

Principle 7. Articulate the business case for ICT projects to sustain funding and implementation

- *Manage ICT projects through strong and clear business cases.*
- *Encourage and manage stakeholder participation in the articulation of business cases.*

Principle 8. Reinforce institutional capacities to manage and monitor implementation

- *Introduce structured approaches to manage implementation of ICT projects and to minimise risks.*
- *Pursue a framework for evaluation and measurement of value creation.*
- *Seek to reinforce the capabilities of public sector workforce and mobilise partnerships with the private and non-governmental sectors as necessary.*

Principle 9. Focus on strategic decisions on the use of ICT resources

- *Appraise current assets to take strategic decisions on the use of ICT resources.*
- *Ensure that national procurement strategies match options for procuring ICT services and products to government needs and capability*

Principle 10. Review and update legal frameworks to adapt to changing contexts.

- *Examine legal and regulatory framework and strive for clarity and consistency.*

Pillar 1: Engage citizens and open up government to maintain public trust

16 The emergence of new technologies like social media and mobile technologies, and technology driven approaches, e.g. Open Government Data, are providing opportunities to maintain or improve trust through new, more direct interactions with citizens and businesses. By using popular digital channels, that citizens and businesses frequent, and by sharing resources publicly, governments can better respond to new public demands in terms of services, policy making and forms of engagement, arising in particular from a new generation of digital natives.

17. Public engagement is a critical component of open and accountable government, both for building trust as well as for creating public value. "Crowd-sourced solutions" – where content and input are sourced from a range of users and actors who have particular knowledge and interests not possessed by the governments – open up the possibility for finding solutions that are not only better adapted and more innovative, but also less resource-intensive than for governments to develop themselves. Informed consultation and participation can lead to new forms of collaboration and to the identification of joint solutions and services that better respond to users' needs. Digital forms of public engagement can contribute to strengthening the support for public institutions and the trust relationship between governments and citizens, but challenges emerging from the involvement of non-government actors in public affairs need to be addressed.

18. Over three decades of intensive use of ICT in the public sector have, in many instances, led to a so called "digital divide", which separates those who are capable of fully embracing technological opportunities and the "have nots" who are excluded from the benefits of online services and information. The emerging use of Web 2.0 (social media, mobile applications) by the public sector, if not properly implemented, can create new forms of digital divide. As a significant barrier to e-government success, the digital divide – both in the society and within the public administration - continues to be an issue to be addressed, and governments need to watch out for the emergence of new forms of digital exclusion.

Principle 1. Promote the use of ICT for greater transparency, openness and inclusiveness

19. *Make ICTs a key part of the strategy to foster transparency, openness and inclusiveness of government processes and operations.* Governments should start by including open and inclusive processes as one of the main goals of their national digital government vision in order to improve governments' accessibility, transparency and accountability. Governments should adopt legislations that recognise citizens' right to access, use and re-use public sector data, information, records and content. The development and adoption of fair and clear licenses for the re-use of public sector information based on open models are key to unleash open government data potential. Governments should review many of the laws, enacted primarily in the 20th century, to recognise different needs brought about by new technologies (e.g. social media, mobile government) and technology-driven approaches (e.g. open government data) and to accommodate intensified public expectations of accountability and transparency. Governments should also consider adopting open standards to support inclusiveness, and public records management systems that provide stronger basis for accountability.

20. *Take steps to address existing digital divides and avoid emergence of new forms of digital exclusion.* Governments should facilitate disadvantaged groups of users with targeted interventions aimed to increase their inclusiveness (e.g. fighting all sorts of access divide). Actions should address issues of ICT literacy in the society, raise awareness on existing online opportunities, develop IT skills in the society and among civil servants, and increase the comfort and familiarity of all segments of the population with using technology and online channels to interact with governments. E-Government strategies should be gender-balanced and take into account different contexts in which men and women live and operate to avoid unanticipated negative effects in terms of exclusion. New technologies (e.g. m-government) are

facilitating Internet access, and governments should adopt multi-channel service delivery strategies to seize all available channels to improve online access to as many users as possible while respecting the choice of those citizens who prefer offline channels. A focus on ease-of-use when developing ICT services can also support the increased use of online channels by citizens. As highlighted by Principle 4, governments should ensure coherence of e-government programmes and strategies with Information Society strategies to ensure access to online channels and developments of an ICT skilled society.

Principle 2. Encourage engagement and participation in a multi-actor context

21. *Use ICT opportunities to be inclusive and engage with public, private and civil society stakeholders to create public value in the policy-making process and in service design and delivery.* Governments should consider different options to use technology to motivate and encourage public participation in policy making and services co-design and co-delivery. This includes digital initiatives to increase political engagement, use of blogs to capture feedback, uptake of social media channels, and development of mobile applications. While grasping these new opportunities, governments should properly address issues concerning citizens' rights, organisation and resource allocation, adoption of new rules and standards, development of institutional capacities to take up these new opportunities and need to facilitate engagement of all age groups and population segments. Similarly, governments should take into account respect of formal responsibilities and procedures (e.g. adoption of guidelines clarifying role and procedure for establishing and managing official government accounts on social media).

22. *Establish a digital governance ecosystem.* In order to assist in identifying and better serving specific segments of the population, governments should identify and engage new and emerging actors (e.g. non-governmental organisations or citizens' associations) involved in the provision and use of ICT-enabled platforms and/or services. They should also partner with civil society entrepreneurs and the private sector to establish trusted third parties to stand between governments and data providers, on the one hand, and citizens, on the other. This includes the identification of business cases and funding models to motivate the actors' involvement to balance supply and demand-driven approaches; the adoption of policies to enable the establishment of ecosystems around universal issues; and creating a framework and culture of collaboration, both within the public sector and with external actors.

23. *Create a data driven culture in the public sector.* Governments should adopt strategies and guidelines for an open government data regime; and should increase the amount of evidence, statistics and data concerning their operations, processes and results to increase openness and transparency but also to incentivise public engagement. Governments should ensure that data and evidence are trustworthy and take steps to prevent misuse and protect data integrity. Actions should be taken to strengthen a culture of access and use of data to spur participation in policy making, creation of public value, service design and delivery. A critical step for creating this culture should be acquiring new capabilities and defining new roles that allow the government to take advantage of the huge amount of public sector information of the public sector. Data hygienist, data explorers and data scientists are among the roles not yet generalised in the public sector (see also Principle 8).

Principle 3. Establish the right conditions to strengthen confidence in digital government services

24. Strengthen public confidence on privacy protection and security. This is essential as more services and information become digital, as use of new technologies increases and new forms of collaboration are established with private and non-governmental partners. The wide diffusion of Internet-based systems and services is changing the landscape of security threats, actual and perceived. Governments today are assessing and managing risks that are amplified by technological trends like cloud computing, cross-border data flows, "BYOD" (bring your own device) policies, use of social networks and others. The sensitive nature of parts of government-processed information requires close linkages between

digital government strategies and national "cybersecurity" strategies as they have emerged over the past decade. In establishing these linkages, governments need to ensure that security measures respond to business needs and are not limited to technological "fixes", but are embedded into organisational and management thinking about how to increase confidence in government services, e.g. "building-in security by design". This ensures that security is considered from the outset and not a costly afterthought; and limits risk of interruptions in online service delivery.

25. *Establish criteria for balancing privacy and security considerations with the benefits of the Internet to its users (external and internal).* Citizens are unlikely to interact with governments via online channels without confidence that their privacy is protected and that their information is securely processed. This can be a significant barrier to fully capturing the benefits of digital government services, e.g. resulting in low uptake of online services. Ensuring security and privacy is costly, but risk of breaches and associated loss of trust and reputation can be pricier. This is important for the growing number of government services that are facilitated by digital identities, single sign-on or other digital identification, authentication and control mechanisms. Governments need to enable both trust *and* innovation. Persuasive government action in this area also can accelerate adoption and diffusion of good practices in the private sector.

26. *Balance the need to be a provider of timely and reliable official information with the opportunities that come with sharing imperfect data*. Governments need to ensure that data provided is trustworthy and avoid risks of data misuse and manipulation, particularly as more government data is made available as "open government data" (i.e. accessible, usable and re-usable) also to non-institutional actors to produce value (see also principle 2). At the same time, the "strive for perfection" should not always prevent publication of data, although data quality should be ensured. Governments are starting to recognise the opportunities of collaboration with external stakeholders to improve quality of government data and information.

27. *Review existing regimes for privacy and security and align them with related national and international efforts, including on measuring impacts*. Individual laws and policies may no longer be enough to effectively safeguard individuals' right to privacy and government organisations' security. Digital government strategies should be closely linked to overarching national strategies for privacy protection (cf. *OECD 2013 Privacy Guidelines*) and IT security (cf. *OECD 2002 Guidelines for the Security of Information Systems and Networks*). [National E-Leaders should co-ordinate domestically on the current revision of the *OECD 2002 Guidelines* so that it takes due note of the benefits and needs of digital government strategies in this area.] Additionally, regulatory regimes need to be complemented by a combination of business, management and technical measures to provide oversight, enforcement and guidance and thus nurture a new culture conducive to safeguards for privacy and security. These measures include policies, procedures, organisational structures and software and hardware functions. Finally, digital government strategies should use empirical evidence to illustrate the degree to which they achieve privacy and security-related objectives[2].

Pillar 2: Adopt joined-up approaches to deliver public value

28. Public sector ICT usage has matured in OECD countries and has become mainstream to the point that the use of digital tools is integrated into the daily work of public administrations. This continuously provides new opportunities for collaborative work and for the delivery of seamless and integrated services. A number of different actors, within and across levels of government, need to share data and information and to work together in new ways to solve problems from a constituents' perspective. Old organisational settings and arrangements are often inadequate and need to be rethought in a context where actors are not only connected, but increasingly interconnected, and administrations need to join up.

29. OECD countries are also finding that increasingly their public sectors are becoming just one player in a new form of 'open-source governance' in which they may be asked to play the role of arbiter, co-ordinator, partner, funder, and regulator for the activities of others in delivering public value. In this context, digital government has become essential for the sharing of tasks and information amongst stakeholders at different levels both inside and outside governments.

30. In order to meet these new challenges, governments need a government-wide vision to help maintain consistency, coherence and a common sense of purpose for ICT deployment in the public sector, and in some instances, a pan-government vision (e.g. for cloud security and the notion of cross recognition of certification and accreditations).. A digital government strategy for the public sector as a whole serves to prioritise specific objectives (improving quality of public services, enhancing public sector efficiency, increasing public engagement in policy making); to harmonise ICT investments (interoperability frameworks); and to ensure related changes in the supporting environment (organisational change, co-ordination, Public Private Partnerships (PPPs), selection of outsourcing models, risk management, HR development, updates of the legal and regulatory framework).

31. Effective digital government agendas depend on input from a variety of stakeholders. Many ICT investments have only yielded limited results due to policies that do not sufficiently reflect internal and external stakeholders' views and knowledge. As a result, they are poorly implemented and lack policy coherence (e.g. due to the multiplication of sector strategies). Given the cross cutting nature of ICTs and the proliferation of multifaceted challenges that require joined-up interventions and cross-cutting actions, effective linkages and alignment across ICT-related strategies is now critical for the successful design and implementation of public policies.

32. Support of political leaders is pivotal to diffuse the government-wide vision necessary to sustain public sector ICT use and to link it to broader national strategic and reform objectives. A vision alone, however, is not enough. The objective of public ICT initiatives is to foster networked societies and collaborative governments where all actors are given the opportunity to exploit, access and harness services and information anywhere and at any time. This may require important changes in the "ways of doing work" in the public sector.

Principle 4. Adopt a government-wide digital government strategy

33. *Develop and adopt a common vision and strategy to ensure a coherent use of ICT within and across policy areas and levels of government in support of a common vision.* The strategy should include a vision statement highlighting broad national objectives and expected outcomes. Based on the assessment of the national context, of the level of sophistication of ICT deployment in the public sector and of the overall societal uptake of online opportunities, the strategy should be complemented by an action plan. This should include specific goals and targets which can help administrations set a course of action, orient individual initiatives towards common national policy goals to capture synergies and avoid overlaps and waste. A timeframe for implementation should include the definition of measurable indicators and a timeline to monitor progress forthrightly and make mid-course corrections.

34. Promote engagement of various stakeholders in providing input for the definition of the strategy. Bringing in input of users of public services (citizens and businesses), service providers (sector ministries and agencies), non-governmental organisations, and government employees should be seen as an essential prerequisite to defining digital government visions that are not only "supply" driven, but that address constituents' needs and challenges, i.e. demand-driven. This serves to ensure ownership of the strategy and its translation into realistic plans.

35. Seek complementarity, alignment and mutual reinforcement between digital government strategies and other relevant sector strategies and relevant sector strategies. The government should provide the institution or authority formally responsible for digital government co-ordination with the mechanisms to align strategic choices on ICT investments and deployment in various policy areas (e.g. Information Society Strategy, Information Economy Strategy, Public Sector Reform Programmes, e-health, e-procurement). This helps ensure sustainable approaches consistent with the national vision, facilitates joint investments and initiatives to achieve results, and highlights the potential contribution of ICT to policy objectives and broad public sector reforms.

Principle 5. Ensure leadership and political commitment

36. *Secure top political level support and commitment to the national digital government agenda*. The strategy embedding a vision and its rationale, and the validation of digital government as enabler for broader policy outcomes should be supported by administrations across all levels of government (if necessary, it should be supported by funding mechanisms and legal frameworks – see also Pillar 3). Policy makers in charge of co-ordinating ICT use in the public sector should involve and secure commitment of the top political leadership - e.g. Head of Government as the champion of change, involvement of the top political leadership of appropriate hierarchical level in key stages of implementation of high-priority ICT initiatives and key strategies. Required changes necessary in the implementation of major ICT projects should be communicated rapidly to ensure that all key leaders and managers accept responsibility for the implementation of needed changes.

37. *Ensure that the vision statement embedded in the digital government strategy is linked to broad public sector reforms and policy objectives.* A common strategy embedding a common vision is not a goal in itself and should be seen as a means to achieve policy priorities. Policy makers responsible for digital government should link the government-wide digital government vision with broader public sector strategic reform objectives to secure commitment of political leadership, promote inter-ministerial co-ordination and collaboration, and facilitate engagement and co-ordination of relevant agencies across levels of government.

Principle 6. Establish effective organisational and governance frameworks

38. *Identify clear responsibilities to ensure overall co-ordination.* A institution or authority responsible for co-ordinating public sector deployment of ICTs should be in place with the key mandate to co-ordinate change, ensure co-operation across levels of government and sectors, and coherence of main relevant strategies, develop common policies and standards (e.g. on open standards and open source), drive the adoption of national interoperability frameworks for data exchange and interoperability across independently operated applications and the responsible agencies, and facilitate synergies and sharing of lessons across policy domains.

39. *Establish organisational mechanisms and governance frameworks to co-ordinate use of ICTs within and across levels of government.* Governments should periodically review their governance architectures and redesign them if necessary to break down silos, and adopt structures that are more flexible and oriented towards integrated policy making to enable the pooling of resources and services, re-engineering of processes, adoption of common standards that support high integration, interoperability of systems and service-oriented architectures.

40. *Establish a framework for interoperability.* Interoperability is essential for integrated and coherent service delivery and policy making. It is an important step in simplifying procedures and data collection for citizens, and in reducing duplication and error within the public sector. It can help improve collaboration across and within public administrations, making procedures quicker, simpler and cheaper

for all parties concerned, in particular when transactions need to be done cross-border and/or cross-sector. Governments should therefore take all necessary steps (e.g. technical and legal) to enable interoperability across governments and sectors.

41. *Adopt mechanisms that enable proper "check and balances" to reinforce accountability.* A system that foresees "check and balances" (e.g. internal, peer and parliamentary oversight, public oversight) of governments' decisions on public IT spending increases the level of accountability and public trust, and can help to improve decision-making and management in an area that is at high risk of project failures, delays, etc.

42. Strengthen international co-operation to better serve citizens and businesses across borders. Whenever possible, governments should consider the impact of their digital strategies and services on other countries. This is particularly important for trans- border regions and municipalities where commuting, working and investing across borders is already a reality. Even when interoperability and full-scale integration across borders might not be an immediate objective, many benefits can emerge from early sharing and co-ordination of digital strategies and plans internationally, e.g. identify existing practices to address comparable issues, design interoperable infrastructures for data exchange and cross-border public service delivery, achieving scale and efficiency effects for jointly implemented projects.

43. Share knowledge to learn from success stories, but also from failures. Sharing good experiences and learning from success stories can provide good anchors for improving future government IT projects. But in a field so closely related to innovation and exposed to rapid technological changes, and hence more exposed than others to failures, it should be regarded as acceptable to openly discuss and learn also from less successful practices. Many unsuccessful practices can be corrected and errors avoided by closely studying budget or time overruns, use of products that are out of scope or focus, non-satisfactory user experiences, etc. Data on both successes and failures should be made openly available so that international and national partners – from inside and outside of governments – can improve their practices and results.

Pillar 3: Strengthen capacities to ensure return on ICT investments

44. The planning and implementation of ICT projects is becoming increasingly complex in terms of budget magnitude, actors involved, and the choice of new technologies and delivery arrangements. They are also likely to impact many areas and functions of government, as well as government reform initiatives. The sequencing and management of these complex ICT projects and operations require interdisciplinary skills, and implementation of ICT projects is increasingly dependent on new business models and forms of collaboration within and between government organisations and with parties outside governments, both businesses and citizens. In many instances, results of ICT investments have been either insufficient or poorly managed, and benefits have not been fully realised. The current context is increasing the difficulty of managing and monitoring implementation, as it is more and more complicated to define roles and responsibilities upfront, adapt to changing skills needs and monitor performance. This is why governments need to be rigorous in adopting models and approaches that strengthen discipline in planning and monitoring in order to reduce the risk of project failure.

45. Without a sound measurement approach to sustain a systematic evaluation of costs, benefits, risks and outcomes of projects, it is increasingly hard for policy makers to make the investments required to achieve the overall digital government vision. Appropriate business cases and evaluation and measurement frameworks are essential to assess the merits of individual initiatives to meet the targeted objectives, and to monitor and improve implementation. The consequences of not meeting business cases include failure to achieve return on investments, cost overruns and project failure; while primary benefits of strong business cases include: a consistent framework for comparing investment decisions, a better understanding of the

drivers of project efficiency or factors to enhance return on investments, a better view of costs, benefits and beneficiaries, and a contribution to evaluating the efficiency and effectiveness of e-government.

46. In a context of multiple ICT projects and related responsibilities spread horizontally across many actors, facilitating a government-wide understanding of ICT needs and assets is needed to help governments make informed decisions on ICT use and spending, whether it be insourcing or outsourcing ICT solutions for an array of support and core activities, or exploring options to maximise the value of ICT investments, reduce computing costs, and enable the creation of personalised content and services. Public bodies can opt for shared IT service centres; concentrated responsibility for certain type of data or government process management in one ministry or agency (e.g. identity, authentication, registration, licensing); or cloud computing – which enables the distributed sharing of resources, software, data and/or processing capacity to users and computers on demand.

47. The effects of rapid technological change such as mobile applications, cloud computing, open government data, service oriented architectures and social media are changing the nature of ICT projects which are less monolithic and more integrated than before and require quick answers from the government. The development of ICT projects cannot rest anymore on waterfall methodologies based on stable specifications. Agile development methodologies with open specifications and based on quick-wins and incremental achievements are the cornerstones of responsive, agile and resilient governments. Funding models for ICT projects and its procurement rules should evolve to support these new development methodologies, and skills need to be adapted. This will enable governments to take up new opportunities in the rapidly changing technological environment, and avoid government rigidity.

48. Conventional and outdated procurement procedures often fail to fully exploit new technological opportunities because they are too rigid to allow iterative design processes, constant user feedback, project specifications that adapt along the development of digital processes and approaches (e.g. open government data) and nurture public sector innovation.

49. ICT projects impact civil servants' needs in three areas: new skill requirements, changes to existing roles, and transformation of organisational culture and rules. Inadequate skills and frail project management capacities may lead to insufficient focus on implementation, missing opportunities to integrate systems and operations of individual agencies and risk of waste of resources.

50. The success of digital government initiatives and processes are highly dependent on government's role in ensuring a proper legal environment for their operation. Impact depends on the diffusion and affordability of access to the ICT infrastructure, which in turns is subject to the regulatory framework governing telecommunication and other ICT-related issues (e.g. those concerning data such as interoperability, the right of citizens to obtain government data in open formats and control access to personal information).

Principle 7. Articulate the business case for ICT projects to sustain funding and implementation

51. Manage ICT projects through strong and clear business cases. In order to identify the impact of ICT initiatives, justify public investments and manage risks, it is essential for governments to prepare detailed business cases for all ICT projects above a certain budget threshold. A sound business case should: highlight clearly where the value is (indicating not only expected economic value, e.g. cost-effectiveness, targeted savings, but also targeted outcomes non-quantifiable on a monetary basis, such as social value, scope and coverage of expected benefits for citizens and improvement of the quality of public services, participatory government solutions); spot potential risks magnitude; identify timeframes for results achievement; indicate how financial resources are being spent; and suggest follow up mechanisms on use of final services. The use of business cases fosters an organisational culture for disciplined projects

planning, and provides consistent criteria to guide evaluation and monitoring of the costs and benefits of ICT projects for overall digital government planning and investments. Also, it helps the alignment of individual projects with the priorities of the institution and government's reform agendas. The business case should include clear responsibilities and roles for all relevant actors, and outline the consequences for failure to meet agreed milestones.

52. Encourage and manage stakeholder participation in the articulation of business cases. Business case building should be viewed as part of a "project management process". Therefore to achieve key results, governments should adopt participatory strategies and mechanisms to involve all stakeholders in the definition of the business case including users of final services, different levels of governments that will be involved in or affected by the project, as well as the contractual actors. The risk of not involving key stakeholders is that key perspectives and needs are not been taken into account thus leading to failures in implementation, cost overruns, insufficient sequencing of projects and missed benefits. The nature and quality of business case management will be impacted by the tools and techniques that are used, the skills and competencies employed, and the norms and values that are brought to the process. Clarity on stakeholders' motives and arguments is for instance important to ensure trust in the participatory process.

Principle 8. Reinforce institutional capacities to manage and monitor implementation

53. *Introduce structured approaches to manage implementation of ICT projects and minimise risks.* Given the proliferation of ICT projects outside the scope of the main digital government strategy, and given the mainstreamed use of ICTs, governments should adopt mechanisms to ensure that the Centre of Government has a comprehensive picture of on-going initiatives (e.g. overview of portfolio of large ICT projects) and updated feedback on effective and efficient implementation, to avoid duplication of existing systems and datasets and minimise project management risks. Governments should for instance establish centralised review mechanisms for all projects above a certain budget threshold, and adopt common methodologies for project management that minimise risks of inefficiency (e.g. projects that overrun, overspend), duplication, and/or failure, while still allowing room for innovation. Models to identify who is accountable for managing parts of the process and taking decisions concerning implementation, who should provide input or resources to the activity and who should be kept informed on results need to be adopted as they can help in monitoring implementation, spotting problems and taking corrective measures. Centralisation of the reviewing mechanisms should sustain alignment with the objectives of the national digital strategy and achievement of economies of scale, while giving enough room for agility and avoid an excessive bureaucratisation of ICT projects development. Furthermore, the commoditisation of technology means that the role of ICT leadership should be closer to orchestration of capabilities than to the classic command-and-control model in order to provide quick answer to the societal challenges.

54. *Pursue a framework for evaluation and measurement of value creation.* Monitoring and evaluation of ICT projects across government requires clear actors (e.g. e-government co-ordination units, Ministries of Finance, inter-ministerial bodies), with clear responsibilities and mandates (e.g. approval of business cases for ICT projects above a certain budget threshold as mentioned in paragraph above). They should work in association with other monitoring and performance agencies responsible for individual projects and sector or organisation performance. The evaluation of ICT projects should not be isolated from the evaluation of the policies supported by the projects. Regardless of the ICT governance model (including more decentralised responsibilities), governments should ensure adoption and uniform application of standards, guidelines, codes for process reengineering, procurement, compliance with interoperability frameworks, and adoption of performance evaluation tools for regular reporting. Governments should invest in increasing the amount of evidence and data captured in the course of project implementation and create incentives to make greater use of existing data to monitor projects performance. The framework should set criteria for conditional release of funding, financing mechanisms that commit projects to achieving benefits, and peer/gateway review procedures.

55. *Seek to reinforce the capabilities of public sector workforce and mobilise partnerships with the private and non-governmental sectors as necessary.* Governments should regularly evaluate the impact ICT emerging technologies, trends and projects have on staff, assess skill gaps and ensure development of new types to enhance organisational learning and match fast changes taking place. The public sector work force needs to be able to count on flexible skills and competencies. These include skills for the advanced use of new technologies (social media and mobile technology) in carrying out internal tasks, deliver services and engage with outside actors; those on ICT project management; and those sustaining use of data for policy modelling, evaluation, data analytics and data mining to sustain policy simulation, target improvements in service delivery, monitor public policies' and programmes' impact. In order to ensure availability of adequate skills, governments should leverage the strengths of partners in the private and non-governmental sectors as necessary and be innovative in the ways they tap into high-skilled labour market. Arrangements to develop an adequate public sector workforce include recruiting and involving young professionals, creating "centre of excellence", providing professional and vocational training, establishing exchange programmes and win-win relations between the public sector and technology leaders. Strategies for ICT skills should be developed in line with other policies dealing with public sector work force mobility and ageing.

Principle 9. Focus on strategic decisions on the use of ICT resources

56. *Appraise current assets to take strategic decisions on the use of ICT resources.* In order to select the appropriate mix of ICT solutions, governments should have a good knowledge of their existing assets (e.g. including skills inventory, ICT inventory and age of existing assets to know where they are in their life cycle, a service inventory of the public sector, current contracts, inter-agency agreements). This can guide future investments and prioritise strategic decisions on resource allocations (e.g. choices on consolidation, reengineering of processes and technologies in the back-end, establishment of one-stop-shops to deliver services, selection on how to procure and contract ICT services and products, skills development or reallocation to support new procedures, processes and service delivery modes). Failure to treat these aspects accurately exposes governments to efficiency shortcomings and important financial risks.

57. *Ensure that national procurement strategies match options for procuring ICT services and products to government needs and capability.* Governments should opt for the way of procuring ICT services and products that increases efficiency, supports innovation and sharing, and best sustains objectives stated in the vision. Outsourcing, cloud computing, shared IT service centres and Public Private Partnerships (PPPs), are all possible options to enable agility, efficiency and value for money if properly supported. To use these options, it is necessary to identify common needs across the public sector, changes in procurement and contracting rules, and clear frameworks for setting responsibilities (see also Principle 8 and the measuring of costs and benefits of different options over the life time of a project and based on the public sector financing, capacities, etc). Additionally, governments should update procurement and contracting rules to make them compatible with modern ways of deploying technology such as cloud computing, new forms of PPPs and service contracts with the private sector.

Principle 10. Review and update legal frameworks to adapt to changing contexts.

58. *Examine legal and regulatory framework and strive for clarity and consistency.* This is essential in order to eliminate barriers to providing information and services online; to ensure that the legal and regulatory environment is not at odds with new technological opportunities and with the demands of increasingly connected societies; and to prevent risks associated with the use of the Internet and technologies, e.g. cybercrime, fraud in e-payments, misuse of open government data, breach of security (see also Principle 3). This requires simplifying regulatory requirements, clarifying legal validity of digital communication channels and acceptance of digital identification, authentication and payments; ensuring

legal equivalence of paper-based and online processes and signature; streamlining of procedures; facilitating sharing of data and resources across agencies to sustain integration and bridging the digital divide (e.g. bringing down barriers between citizens and governments to interact online). These issues are more effectively addressed on a government-wide basis by national laws, policies, architectures and legal and regulatory frameworks. Regular "compatibility checks", periodical reviews of legal and regulatory frameworks, and when necessary, amendments or new laws are needed to sustain effective implementation of ICT projects, legal stability for all stakeholders involved and particularly important in areas where digital government transactions are likely to have high value and or high level of sensitivity, e.g. e-payments, e-ID, e-authentication, e-procurement and procurement of IT solutions.

[1] Cf. UK Cabinet Office (November 2012), "*Government Digital Strategy*".

[2] Cf. OECD (2012), *Improving the Evidence Base for Information Security and Privacy Policies*.