This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

TGF: Impact of the Internet of Things Version 1.0

Committee Note Draft 01

16 October 2014

Specification URIs

This version:

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/cnd01/TGF-IoT-Impact-v1.0-cnd01.pdf (Authoritative)

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/cnd01/TGF-IoT-Impact-v1.0-cnd01.html

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/cnd01/TGF-IoT-Impact-v1.0-cnd01.doc

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/TGF-IoT-Impact-v1.0.pdf (Authoritative)

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/TGF-IoT-Impact-v1.0.html

http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/TGF-IoT-Impact-v1.0.doc

Technical Committee:

OASIS Transformational Government Framework TC

Chair:

John Borras (johnaborras@yahoo.co.uk), Individual

Editors:

Nig Greenaway (Nig.Greenaway@uk.fujitsu.com), Fujitsu Limited

Chris Parker (chris.parker@cstransform.com), CS Transform Limited

Related work:

This document is related to:

- *Transformational Government Framework Version 2.0*. Edited by John Borras, Peter F Brown, and Chris Parker. Latest version. http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.html.

Abstract:

This Committee Note provides an impact assessment of the new opportunities becoming available through the development of the Internet of Things (IoT) on

Transformational Government programs and the delivery of services by the public sector. It seeks to identify the issues that need to be addressed and makes recommendations on how best to tackle these and how the Transformational Government Framework (TGF) v2.0 can be utilized to ensure the optimum advantage is taken of these new opportunities.

Status:

This document was last revised or approved by the OASIS Transformational Government Framework TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.
Technical Committee members should send comments on this document to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at https://www.oasis-open.org/committees/tgf/.

Citation format:

When referencing this document the following citation format should be used:

[TGF-IoT-Impact-v1.0]

TGF: Impact of the Internet of Things Version 1.0. Edited by Nig Greenaway and Chris Parker. 16 October 2014. OASIS Committee Note Draft 01. http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/cnd01/TGF-IoT-Impact-v1.0-cnd01.html. Latest version: http://docs.oasis-open.org/tgf/TGF-IoT-Impact/v1.0/TGF-IoT-Impact-v1.0.html.

Copyright © OASIS Open 2014. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

 Copyright © OASIS Open 2014. All Rights Reserved.

1 Introduction

This Committee Note looks at the opportunities and challenges that the Internet of Things (IoT) opens up for public sector organizations. And it shows how use of the Transformational Government Framework [TGF v2.0] – an OASIS standard bringing together global best practices on the governance and delivery of transformational change – can help policy-makers embrace those opportunities and respond effectively to those challenges.

It is in three main parts:

- Section 2 places the Internet of Things in the context of previous waves of technological change and their application to public service delivery;
- Section 3 identifies six key impacts of the Internet of Things for public service delivery;
- Section 4 identifies how – for each of the six IoT impacts - the Core Patterns of the Transformational Government Framework provide a practical toolkit for policy makers and service delivery managers in the public sector looking to build IoT-optimized public services.

1.1.References (non-normative)

[TGF v2.0]

Transformational Government Framework Version 2.0. Edited by John Borras, Peter F Brown, and Chris Parker. 01 May 2014. OASIS Committee Specification 01. Latest version: http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.html

[TGF eHealth Profile v1.0]

Transformational Government Framework e-Health Profile Version 1.0. Edited by John Borras, Hans A. Kielland Aanesen and Nig Greenaway. 19 June 2014. OASIS Committee Note 01. Latest version: http://docs.oasis-open.org/tgf/TGF-eHealth-Profile/v1.0/TGF-eHealth-Profile-v1.0.html

Copyright © OASIS Open 2014. All Rights Reserved.

2 Context

As the challenges to organizations change over time, technology continuously evolves in an attempt to better address them. In particular, IT is ever developing new capabilities and extending its applicability to an increasing number of facets of business and personal life.

Forty years ago, IT was largely a set of isolated capabilities that provided local benefits to those who could afford specialized and diverse equipment and the skills to exploit it. During the 1990s, the Internet provided a universal means of joining up these islands of activity and formed the basis for a worldwide IT platform capable of organic development by a wide range of organizations and individuals. One such development was the World Wide Web that provided the ability to link information. Another, during the 2000s, was Social Media that raised the level of interworking to provide person-to-person connectivity and facilitate collaboration between individuals and organizations. These have rapidly become a part of everyday life for the public and introduced consumer-led change to business and government organizations.

The latest wave of developments takes interworking still further by incorporating objects of all sorts into the network of IT services, information, organizations and people. This is the Internet of Things (IoT) that provides the potential for e-devices to be commonly built into infrastructure such as roads, vehicles, localities (e.g. smart cities), homes, livestock and even people (e.g. for measuring bodily functions). Many organizations, including governments, are realizing that there are financial, social and other benefits that are emerging though the use of networks of e-devices for the collection of data (e.g. the monitoring of people and their environment for health purposes) or raising alerts (e.g. when river levels rise). The hope is that these networks can provide better services to society at large - whilst realizing the economies that are necessary to support growing and aging populations, and also ensuring sustainability and meeting social, individual, corporate, environmental, neighbourhood, regional and global needs.

There is not yet an agreed definition of IoT, but the OASIS document Transformational Government Framework e-Health Profile [TGF eHealth Profile v1.0] offers the following:-

> *“a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes.*
>
> *Note: Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.”*

This definition does not radically conflict with those offered by others and, importantly, includes the interaction with other systems and people who can use the information generated by a set of ‘things’.

Such systems are already being developed by a wide range of players across all sectors. For example, smartness is currently being built into washing machines, TVs, refrigerators and other domestic products. These have various potential uses (and concomitant risks) and could use any

 Copyright © OASIS Open 2014. All Rights Reserved.

of a number of connections within the home, to achieve local and possibly internet-level transmission needs.

The widespread and diverse adoption of these technologies and the 'bottom up' development, that is necessary for the medium term development of the IoT, are key characteristics that need to be considered and managed now as near-term projects start to build an infrastructure that would be prohibitively expensive to replace.

Some very large projects are already starting to emerge - often as Smart City initiatives. The full impact of the possible future extent of IT-based support can begin to be understood by considering the work going on in Japan to rebuild complete areas following the earthquake and tsunami in 2011[1]. There, the opportunity presented by the necessity for large scale reconstruction is being taken to introduce building and home management systems (amongst other innovations) to provide a sustainable environment that contributes to society and people's lives. In this situation, they are, in most senses, starting from scratch and are able to agree and control the development of all systems. However, this is atypical and generally the development of a smart city or equivalent ecosystem will involve a number of organizations from a range of sectors who all need to work together and who also own existing services and systems that need to coexist and interoperate. In this scenario, building and home management systems will be fitted to new buildings and retrofitted to others.

However, further independently-supplied systems need to be able to leverage the capabilities that are already implemented. An example is an e-Health system that will contribute its own set of facilities but could usefully leverage home, building and city management systems in order to deliver its full potential. Without that capability, it would be necessary to implement much of those systems' facilities within the e-Health system leading to duplication and increased cost.

The IoT can be used to deliver many benefits but, as with any technology, it also has the potential to be abused. Examples of use and abuse are widespread and available in the media[2].

Thus, the longer term should be considered by taking a holistic approach to all developments that involve IoT aspects. This paper identifies some areas where the emergent IoT and its application can impact programmes in which government organizations play a major part. It then goes on to relate these to existing TGF patterns in order to help government and partner organizations deliver programmes that contribute to the future rather than constraining it by delivering tomorrow's legacy systems, today.

[1] The Fujitsu Scientific & Technical Journal 2014 - 4(Vol.50, No.2) "Smart Cities and Energy Management" - see http://www.fujitsu.com/global/about/resources/publications/fstj/archives/vol50-2.html

[2] The BBC News Article "Tomorrow's cities - the lamp-posts watching every move" 25th September 2014 http://www.bbc.co.uk/news/technology-28159732

 Copyright © OASIS Open 2014. All Rights Reserved.

3 Possible Impacts of IoT-based Services

The impacts on services that use of the IoT is likely to introduce include:-

- Unpredictable Futures
- New Partnership models
- Complexity for the Customer
- Data Privacy and Security
- Systems Management
- Network-related Issues

Each of these is discussed in turn in the following sub-sections.

3.1 Unpredictable Futures

As with earlier phases of IT development, the uses to which the latest technologies will be put and the way that they and the services that they enable will develop cannot be accurately predicted.

The IoT provides a number of disruptive technologies that will lead to the innovation, by all kinds of stakeholders, that is necessary to meet the challenges of the modern world. At the same time, the use of these technologies will generate new risks alongside those that always exist such as cataclysmic events, organizations' evolution, mergers and acquisitions and new consumer desires.

The sheer amount of data that services will generate introduces further risk factors such as the difficultly in turning it into actionable information. The volume will exceed the capability of humans to act appropriately upon it and lead to many decisions being taken automatically. This introduces the potential for some key factors to be missed leading to outcomes that are suboptimal or completely wrong.

At the same time, greater data volumes lead to increased risks of data leakage that could prove catastrophic.

However, waiting to see how the technology will turn out is not an option. Businesses and governments of all sizes have problems that have to be addressed, at least in part, in the short term and the IoT has the potential to provide some of the answers.

3.2 New Partnership Models

Services to a region or city as discussed above will need to be provided by a range of sectors and players within them. These will include government (all tiers), energy companies, transport authorities, health services, service companies, etc. as well as a range of suppliers to those organizations.

Copyright © OASIS Open 2014. All Rights Reserved.

Many systems (e.g. weather and disaster management) are regional and cross government jurisdictions. Thus, federation between sectors and their services will become increasingly important in the medium to long term.

However, the IoT is being built bottom up with a range of standards (often specific to a sector) and network types.

The foundations for collaboration and orchestration within and across sectors need to be considered early on. Relationships may become very complex with a single organization playing custodian, supplier and consumer roles within a service ecosystem.

Stakeholder organizations will all have their own objectives and channels to market and this provides them with a challenge. How do they manage their piece of the overall ecosystem and benefit from it whilst also contributing to the greater good of society at large?

Continuity of service over time is another issue that needs to be addressed in any service development as cessation of operations by any stakeholder for whatever reason would impact the overall service.

3.3 Complexity for the Customer

IoT-based services can have many component parts and may be provided by consortia consisting of several stakeholder organizations. This complexity is bound to confuse all but the most digitally literate customers.

From the end-user (citizen or business) perspective, any multiplicity of players could give rise to several inter-related contracts and support mechanisms. Whilst variety, choice and competition are desirable market characteristics, straightforward customer access to a small number of (aggregated) systems and seamless support for them is a necessary prerequisite to service success.

Customers will wish to change suppliers. This needs to be as seamless as possible and not result in service interruptions as they will have come to depend upon the service and service interruptions could have potentially disastrous results.

3.4 Data Privacy and Security

Data privacy is vital. Citizens and businesses need to trust the service and must understand the benefits that they gain in return for allowing aspects of their information to be shared.

On the supplier side, there is an understandable desire to leverage the information made available to them for service improvement and marketing purposes. This needs to be very transparent, in order to retain trust, and be rigorously enforced to ensure good practice. Examples such as the recent NHS care.data situation in the UK and the general dislike by Facebook users of the new Facebook Messenger demonstrate the fragility of trust with citizens withholding assent and migration to a range of alternative messaging applications, respectively.

 Copyright © OASIS Open 2014. All Rights Reserved.

Such secondary use of information needs to be transparent and not be hidden in long complex service agreements that virtually no one has the time to read, let alone understand.

The retention (and possible transfer) of raw information following a customer switching to an alternative supplier needs to be addressed in service agreements.

Cyber security also needs to be considered. There have been localized malicious attacks on some home management systems but the threat increases exponentially in larger systems. The current issues with unsecured Wi-Fi connections will seem insignificant compared to (e.g.) interference with any element of an e-Health or power supply system.

3.5 Systems Management

Many of the devices (and the data that they generate) will not be in the direct control or ownership of the public sector and the management of sensors and other devices within the community raises new challenges. Device failure or exhaustion of battery power might be mildly inconvenient in many cases but in others could be fatal (e.g. in an e-Health system). It is also important to recognize that services and the components within them will need to evolve over time.

The increased use of ICT by exploiting IoT technologies will have an impact on emissions and power usage. This may be positive when other factors, such as a service reducing power costs and impacts elsewhere, are taken into account but the overall impact of all changes on the environment needs to be understood.

Policies on asset management, monitoring, maintenance, upgrades, replacement, modification, status reporting, etc. of devices need to be open and available to all.

3.6 Network-related Issues

Network coverage may well be an issue. There is no single answer to connectivity and a range of alternative architectures might be needed to provide appropriate coverage for IoT and other services (sometimes even implementing several to serve the same location).

Different types of network (cabled, wireless, mobile or mesh) may be required depending on the service requirements (and more than one is likely to be necessary to support a single service – e.g. a cabled wireless backbone within a property). Some technical standards already differ for implementations within offices, industrial sites, homes, data centre and other uses.

Interference between systems (e.g. between home management systems in neighbouring properties), needs to be eradicated. This is not just a spectrum issue but could also occur at the application service level as these systems will need some level of configuration. This may be initially set up by a service provider but individuals will need to configure new devices as they subsequently acquire them. This raises the potential for accidental or malicious invasiveness into other systems.

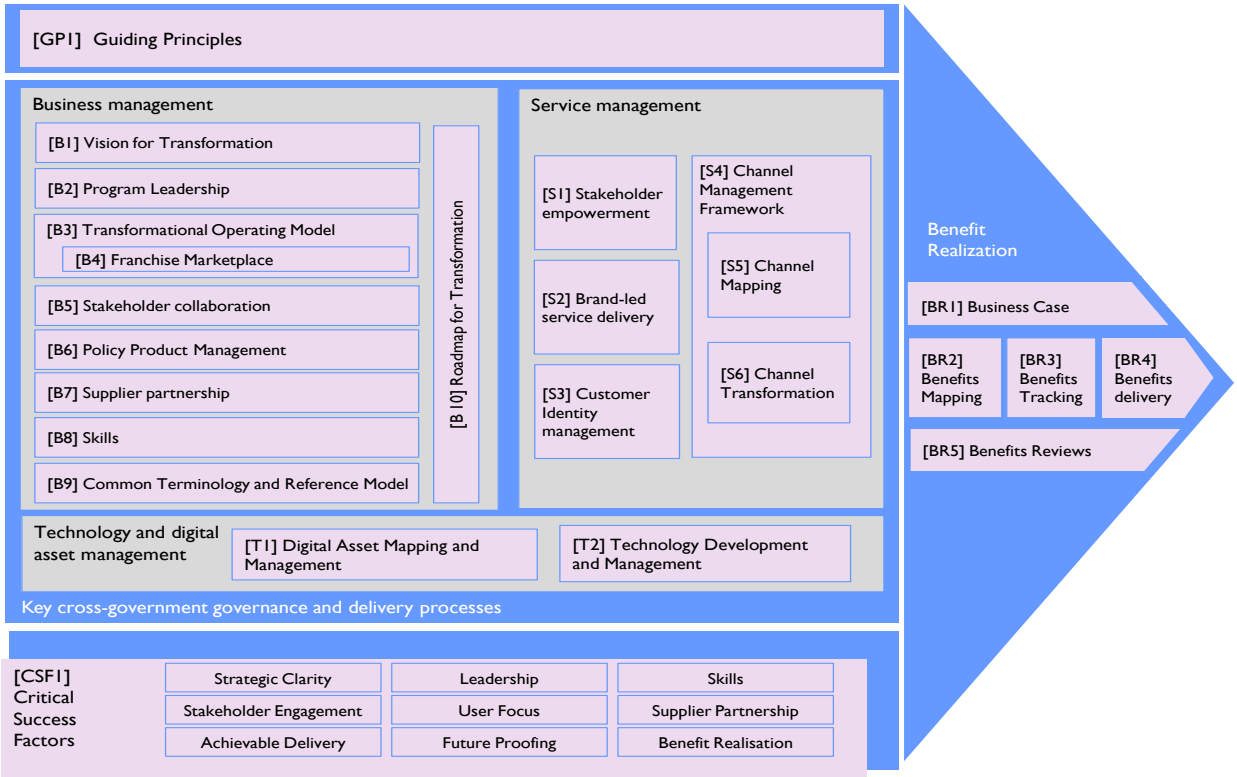
Interference also carries the risk of impacting the availability, performance or usability of a system.

 Copyright © OASIS Open 2014. All Rights Reserved.

4 Using the TGF

The Transformational Government Framework (TGF) provides a set of patterns that together provide guidance on, and good practice for, the development, agreement and delivery of government programmes. They are relevant to all stakeholders in such programmes, including policy developers, those responsible for service design, commissioning and delivery, elected leaders, government executives, private sector partners, suppliers, voluntary sector organizations and community representatives.

The patterns are shown in the overall TGF model:-



The TGF patterns are fully described in the TGF standard documentation [TGF v2.0].

This section addresses each of the impacts of the IoT introduced in section 3 and identifies the TGF patterns that have the most guidance to offer in addressing them. This cannot be exhaustive and is limited to the main considerations identified within this document. All of the TGF patterns should be considered throughout the enactment of government programmes - including parts that are wholly delivered and managed by the private sector. This is particularly true for the Guiding Principles [GP1], Critical Success Factors [CSF1] and Benefit Realization [BR1]-[BR5] patterns that apply throughout all aspects of any TGF program.

Copyright © OASIS Open 2014. All Rights Reserved.

Thus the remainder of this section concentrates upon applicability of the key Business, Service and Technology/Digital Asset Management patterns.

4.1 Unpredictable Futures

The major impacts introduced by the IoT in this area are technical. However, business innovation may also introduce disruptions. As described earlier, technology will always change. The TGF addresses future-proofing by means of an open governance approach that is technology-independent including the use of programme principles.

IoT Impact	Relevant TGF Pattern(s)
Disruptive technologies	Supplier Partnership [B7], Skills [B8], Roadmap for Transformation [B10], Resources Mapping and Management [T1], Technology Development and Management [T1]
Data volumes	Transformational Operating Model [B3], Resources Mapping and Management [T1], Technology Development and Management [T1]
Automated decision making	Transformational Operating Model [B3], Policy Product Management [B6], Skills [B8], Common Terminology and Reference Model [B9], Roadmap for Transformation [B10], Customer Identity Management [S3], Technology Development and Management [T1]
Risk of data leakage	Transformational Operating Model [B3], Customer Identity Management [S3], Resources Mapping and Management [T1], Technology Development and Management [T1]

4.2 New Partnership models

The TGF is based on collaboration between the full range of stakeholders. As technology becomes pervasive in consumer and public ‘spaces’, this facet is one to which explicit ongoing attention must be paid.

IoT Impact	Relevant TGF Pattern(s)
Services not bounded within a specific jurisdiction	Vision for Transformation [B1], Program Leadership [B2], Transformational Operating Model [B3], Franchise Marketplace [B4], Stakeholder Collaboration [B5], Supplier Partnership [B7], Common Terminology and Reference Model [B9], Stakeholder Empowerment [S1], Brand-led service delivery [S2], Customer Identity Management [S3], Channel Management Framework [S4]

Copyright © OASIS Open 2014. All Rights Reserved.

IoT Impact	Relevant TGF Pattern(s)
Stakeholder roles and collaboration	Vision for Transformation [B1], Transformational Operating Model [B3], Franchise Marketplace [B4], Stakeholder Collaboration [B5], Policy Product Management [B6], Supplier Partnership [B7], Skills [B8], Common Terminology and Reference Model [B9], Stakeholder Empowerment [S1], Customer Identity Management [S3]
Individual stakeholder objectives	Vision for Transformation [B1], Program Leadership [B2], Stakeholder Collaboration [B5], Stakeholder Empowerment [S1]
Continuity of service	Program Leadership [B2], Transformational Operating Model [B3], Franchise Marketplace [B4], Supplier Partnership [B7], Skills [B8], Roadmap for Transformation [B10],Resources Mapping and Management [T1], Technology Development and Management [T1]

4.3 Complexity for the Customer

The TGF espouses a citizen-centric approach. This tenet is vital for systems that reach so far into the consumer/user space as those made possible through IoT-powered solutions.

IoT Impact	Relevant TGF Pattern(s)
Many component parts leading to complexity for the customer	Transformational Operating Model [B3], Franchise Marketplace [B4], Stakeholder Collaboration [B5], Common Terminology and Reference Model [B9], Brand-led service delivery [S2], Customer Identity Management [S3], Technology Development and Management [T1]
Inter-related contracts and support mechanisms	Vision for Transformation [B1], Program Leadership [B2], Transformational Operating Model [B3], Franchise Marketplace [B4], Stakeholder Collaboration [B5], Policy Product Management [B6], Supplier Partnership [B7], Skills [B8], Common Terminology and Reference Model [B9], Stakeholder Empowerment [S1], Brand-led service delivery [S2], Customer Identity Management [S3], Channel Management Framework [S4], Channel Mapping [S5], Channel Transformation [S6], Resources Mapping and Management [T1], Technology Development and Management [T1]

Copyright © OASIS Open 2014. All Rights Reserved.

IoT Impact	Relevant TGF Pattern(s)
Customer requirement to change suppliers	Franchise Marketplace [B4], Stakeholder Collaboration [B5], Supplier Partnership [B7], Stakeholder Empowerment [S1], Customer Identity Management [S3], Resources Mapping and Management [T1], Technology Development and Management [T1]

4.4 Data Privacy and Security

The TGF identifies the need for identity and privacy management. These requirements can be exacerbated when multiple organizations are contributing towards a service that aggregates offerings from a number of sectors. The nature of IoT systems can increase the risk factors to a system still further.

IoT Impact	Relevant TGF Pattern(s)
Engendering customer trust	Program Leadership [B2], Stakeholder Collaboration [B5], Brand-led service delivery [S2], Customer Identity Management [S3]
Supplier leveraging of information	Transformational Operating Model [B3], Supplier Partnership [B7], Stakeholder Empowerment [S1], Customer Identity Management [S3]
Transparency of information usage	Transformational Operating Model [B3], Stakeholder Collaboration [B5], Supplier Partnership [B7], Brand-led service delivery [S2], Customer Identity Management [S3]
Management of data following a customer switch of supplier(s)	Transformational Operating Model [B3], Franchise Marketplace [B4], Stakeholder Collaboration [B5], Supplier Partnership [B7], Common Terminology and Reference Model [B9], Stakeholder Empowerment [S1], Brand-led service delivery [S2], Customer Identity Management [S3], Channel Management Framework [S4], Channel Mapping [S5], Resources Mapping and Management [T1], Technology Development and Management [T1]
Resilience against malicious attack	Transformational Operating Model [B3], Policy Product Management [B6], Skills [B8], Customer Identity Management [S3], Resources Mapping and Management [T1], Technology Development and Management [T1]

Copyright © OASIS Open 2014. All Rights Reserved.

4.5 Systems Management

The TGF addresses how changes to the way in which technology and digital assets are managed to accelerate, de-risk and lower the cost of transformation programs. These principles need to be applied to components that are deployed in customer and public spaces.

IoT Impact	Relevant TGF Pattern(s)
Management of devices not under direct control of service providers	Transformational Operating Model [B3], Stakeholder Collaboration [B5], Supplier Partnership [B7], Brand-led service delivery [S2], Customer Identity Management [S3], Channel Mapping [S5], Resources Mapping and Management [T1], Technology Development and Management [T1]
Device life	Supplier Partnership [B7], Roadmap for Transformation [B10], Brand-led service delivery [S2], Resources Mapping and Management [T1], Technology Development and Management [T1]
Power usage, emissions, sustainability	Vision for Transformation [B1], Transformational Operating Model [B3], Stakeholder Collaboration [B5], Policy Product Management [B6], Technology Development and Management [T1]
Asset policies	Transformational Operating Model [B3], Resources Mapping and Management [T1], Technology Development and Management [T1]

4.6 Network-related Issues

The TGF recognizes the need for a top-level vision and architecture for future technology use. This needs to be applied across all suppliers within a system and needs to address physical features of the environment in which service components are deployed. The use of IoT technologies necessitates an emphasis on sensors and devices and the means by which they interact with each other and with other system.

IoT Impact	Relevant TGF Pattern(s)
Network architectures	Roadmap for Transformation [B10], Resources Mapping and Management [T1], Technology Development and Management [T1]
Interference between systems	Transformational Operating Model [B3], Stakeholder Collaboration [B5], Policy Product Management [B6], Supplier Partnership [B7], Customer Identity Management [S3], Resources Mapping and Management [T1], Technology Development and Management [T1]

Copyright © OASIS Open 2014. All Rights Reserved.

IoT Impact	Relevant TGF Pattern(s)
Configuration in end-user environments	Transformational Operating Model [B3], Stakeholder Collaboration [B5], Supplier Partnership [B7], Stakeholder Empowerment [S1], Brand-led service delivery [S2], Channel Management Framework [S4], Channel Mapping [S5], Resources Mapping and Management [T1], Technology Development and Management [T1]

 Copyright © OASIS Open 2014. All Rights Reserved.

5 Conclusion

While the Internet of Things raises great opportunities for innovation and service transformation, it also raises significant challenges. These challenges are not necessarily entirely new, but they extend the scale and complexity of many challenges that public sector organisations are often already struggling with. Examples are:

- partnership relationships moving from primarily 'one to one' to federated 'many to many' relationships;
- an unprecedented explosion in the volume of data to manage and make decisions from – with decision-making increasingly becoming automated at the same time;
- increasing complexity of networks, devices and apps arising from the burgeoning availability of sensors;
- exposure to a greater vector of security and privacy risks arising from the sheer number of parties and connections involved in service delivery.

This set of changes will not impact all parts of the public sector simultaneously. The IoT is not one wave of technological change, but many overlapping waves that are impacting at different rates in different sectors and markets. So progress towards the IoT is likely to be lumpy not linear, but this means that forward strategy development and capacity planning is essential for all public bodies. And getting it wrong can quickly impact organizational operations and reputation.

As shown through the mapping conducted in Section 4 of this Committee Note, the Transformational Government Framework provides public sector leaders with the toolkit needed to establish an effective governance regime for IoT in the public sector.

Copyright © OASIS Open 2014. All Rights Reserved.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Hans A Kielland Aanesen, Individual Member
John Borras, Individual Member
Peter F Brown, Individual Member
Geoff Clarke, Microsoft Corporation
Nig Greenaway, Fujitsu Ltd
Gershon Janssen, Individual Member
Chris Parker, CS Transform Ltd
Colin Wallis, New Zealand Government
Joe Wheeler, MTG Management Consultants, LLC
Mark Woodward, Individual Member

 Copyright © OASIS Open 2014. All Rights Reserved.

Appendix B. Revision History

Revision	Date	Editor(s)	Changes Made
01	8 July 2014	John Borras	Initial draft.
02	21 July 2014	John Borras	Further input from TC members
03	15 October 2014	Nig Greenaway Chris Parker	Major rewrite and re-structuring.

Copyright © OASIS Open 2014. All Rights Reserved.