International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(19 July 2019)

ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities

Technical Report D4.1

Framework for security, privacy, risk and governance in data processing and management

ITU-T

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. ITU-T Study Group 20 set up the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) at its meeting in March 2017. ITU-T Study Group 20 is the parent group of FG-DPM.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Technical Report D4.1

Framework for security, privacy, risk and governance in data processing and management

Summary

This Technical Report addresses concerns regarding data security, privacy and risk for data processing and management in IoT and Smart Cities and Communities require an appropriate governance framework. This report describes these concerns, the key components of the governance framework and the impact on related lifecycles and processes, in particular on risk management processes.

Acknowledgements

This Technical Report was researched and principally authored by Robert Lewis-Lettington (UN-HABITAT), Pasquale Annicchino (Archimede Solutions), Nathalie Feingold (NPBA), Antonio Kung (TRIALOG SA) and Xiaomi An (RUC) under the chairmanship of Gyu Myoung Lee (Korea, Rep.of).

Additional information and materials relating to this Technical Report can be found at: www.itu.int/go/tfgdpm. If you would like to provide any additional information, please contact Denis Andreev (TSB) at tsbfgdpm@itu.int.

Keywords

Smart Cities; Internet of Things, Smart City Architecture, Data Management; Security; Data Protection; Privacy; Governance; Risk Management.

Technical Report D4.1

Framework for security, privacy, risk and governance in data processing and management

CONTENTS

Technical Report D4.1

Framework for security, privacy, risk and governance in data processing and management

1. Scope

Recognising the heterogeneity of actors, interests, applications and dynamics within, and the rapid evolution of, the data processing and management for smart cities and communities ecosystem, this technical report:

- explains concerns for security and privacy for data processing and management in IoT and Smart Cities and Communities,
- describes the multi-dimensional viewpoint for security and privacy in data processing and management, and their impact on processes applied by IoT and Smart Cities and Communities stakeholders
- describes the risk management processes for data processing and management in IoT and Smart Cities and Communities, and
- describes a governance framework for data processing and management,

2. References

[FG-DPM TS D0.1]	Draft Technical Specifications D0.1 “Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary”.
[IEC Guide 120: 2018]	Security aspects - Guidelines for their inclusion in publications
[ISO 16091]	Space systems -- Integrated logistic support
[ISO 29100]	Information technology-Security techniques-privacy framework
[ISO 31000]	Risk management
[ISO/IEC 20547-3]	Big data Reference Architecture
[ISO/IEC 27000]	Information security management systems — Overview and vocabulary
[ISO/IEC 27001]	Information security management
[ISO/IEC 27002]	Code of practice for information security controls
[ISO/IEC 27005]	Information Security Risk Management
[ISO/IEC 27552]	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
[ISO/IEC 29100]	Privacy framework
[ISO/IEC 30141]	IoT Reference Architecture
[ISO/IEC 30145-1]	Smart City ICT Reference Framework: Smart City Business
[ISO/IEC 30182: 2017]	Smart city concept model – Guidance for establishing a model for data interoperability
[ISO/IEC AWI 30145-1]	Information technology -- Smart City ICT reference framework
[ISO/Guide 73:2009]	Risk management — Vocabulary
[ISO/IEC/IEEE 15288]	Systems and software engineering — System life cycle processes
[ISO/IEC PRF TR 27550]	Privacy engineering for system life cycle processes
[ITU directory]	Integrated Database ITU Terms and Definitions
[ITU-R M.1224]	Vocabulary of terms for International Mobile Telecommunications (IMT)

[ITU-T X. 1040 (10/2017)]	Security reference architecture for lifecycle management of e-commerce business data
[ITU-T X. 1601 (10/2015)]	Security framework for cloud computing
[ITU-T Y. 2060 (06/2012)]	Overview of the Internet of things

3. Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 Data [ISO 16091, 2018]: Information represented in a manner suitable for automatic processing

3.1.2 Data breach [ITU directory**]:** A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.

3.1.3 Data controller [ITU-T X. 1601 (10/2015)]: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.1.4 Data integrity [ITU-R M.1224]: The property that the data has not been altered or destroyed in an unauthorized manner.

3.1.5 Data processor [ITU-T X. 1601 (10/2015)]: In relation to personal data, this means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.1.6 Ecosystem [D0.1]: A network of interconnecting organisations, , forming a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability and sustainability. Digital ecosystem models are informed by knowledge of natural ecosystems, especially for aspects related to competition and collaboration among diverse entities.

3.1.7 Governance [adapted from, http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance]: sets the parameters under which management operates, including how power is distributed and shared, how policies are formulated, priorities set and stakeholders made accountable.
Note: Governance is about the definition of the strategic vision and direction, the formulation of the high-level goals and policies of an organisation and the overseeing of its management.

3.1.8 Internet of Things [Source: ITU-T Y. 2060 (06/2012)]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.9 Management [http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance]: Management is about running operations according to the established vision and policies, making operational decisions, and interfacing with governance bodies to allow for supervision.

3.1.10 Personal data [D0.1]: Any information relating to an identified or identifiable natural person ('Data subject');
Note: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

3.1.11 Privacy by default [adapted from GDPR, Article 25.2]: The implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Note: This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures ensure that by default personal data are not made accessible, without the individual's intervention, to an indefinite number of persons.

3.1.12 Privacy by design [adapted from GDPR, Article 25.1]: A methodology according to which, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of persons posed by the processing, at the time of the determination of the means for processing and at the time of the processing itself, the implementation of appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation in an effective manner and the integration of the necessary safeguards into the processing in order to meet regulatory requirements and to protect the rights of data subjects.

3.1.13 Risk [ISO 31000]: Effect of uncertainty on objectives.

3.1.14 Risk appetite [ISO/Guide 73:2009(en) Risk management — Vocabulary]: Amount and type of risk that an organization is willing to pursue or retain.

3.1.15 Security [IEC Guide 120, 12018]: Condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

3.1.16 Sensitive data [ITU-T X. 1040 (10/2017)]: Data with potentially harmful effects in the event of disclosure or misuse.

3.1.17 Smart cities and communities (SC&C) [D0.1]: The effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for citizens.

Note: This definition aligns with the definition of smart city in [b-ISO/IEC 30182: 2017] and with the recommendation from the IEC/ISO/ITU Smart City terminology coordination task team.

3.2 Terms defined here

This Technical Report defines the following terms:

3.2.1 Collection limitation: The collection of personal information that is fair, lawful and that is limited to that which is necessary for the specific purposes;

3.2.2 Data minimization: The collection of personal data that is kept to a strict minimum.

Note: The design of programs, information and communication technologies, and systems begins with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability and likability of personal information is minimized.

3.2.3 Purpose specification: Purpose for which personal information is collected, used, retained and disclosed that is communicated to the individual (data subject) at or before the time the information is collected.

Note: Specified purposes should be clear, limited and relevant to the circumstances.

4. Abbreviations

AI:	Artificial intelligence
DPM:	Data processing and management
EU:	European Union
ICT:	Information and communications technology
IoT:	Internet of Things
GDPR:	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard

	to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ISO:	International Organization for Standardization
SC&C:	Smart cities and communities
TVRA:	Threat, Vulnerability and Risk Analysis
WIPO:	World Intellectual Property Organization

5. Security, privacy, risk and governance in data processing and management in the internet of things and smart cities and communities

5.1 Security concerns

Data security is a fundamental concern within smart and sustainable cities as technological developments present new and often still unsolved problems for smart cities. The growing body of data collected demands for specific capabilities and capacities in order to manage data streams coming from different sources. Data need to be managed and processed properly in order to maximize their value (both for citizens and for cities) in a secure manner. The large and interconnected network of devices generate issues ranging from social surveillance to vulnerabilities in the technical infrastructures to attacks (for instance in the case of traffic systems)[1]. In many parts of the world, policy makers and legislators are trying to address security issues also by improving the existing legal framework on liabilities. For instance, the European Commission is considering whether there is a need to revise the EU Directive on Product Liability in order to tackle legal problems arising from IoT, robotics and autonomous capabilities. In Japan, the Japanese Council on Investments has approved a set of guidelines on autonomous cars which are one the first legal framework at global level on this issue. As far as data security is concerned, cities are therefore called to preventive action in order to detect and map possible security threats in advance and act accordingly. Threats may also affect data integrity, confidentiality and accessibility. Violations of data security can therefore compromise the entire system and also the trust of citizens that without security will not trust the solutions deployed by cities. A minimum set of agreed security standards and practices for IoT products will be required and their developments will have to be based on a firm understanding of the risk that such systems pose today.

From the point of view of DPM in smart cities, data security must be ensured continuously entire the domain and throughout the life-cycle of the data in question. In order to guarantee security there should be no gaps in either protection or accountability. The protection of security here is also particularly relevant for the protection of privacy, as without the first the protection of the second cannot be guaranteed. Within the existing framework, cities should particularly be consistent with standards that have been developed for instance those on smart city business process framework (ISO 30145-1) which defines a specific process on safety, security and resilience which follows the following principles:

- holistic approach
- aggregation data from multiple sources to manage safety, security and resilience
- elaboration of deployment of data privacy standards
- separation between critical and non-critical services of the city so that services can be engineered accordingly
- disaster recovery plans that are regularly tested[2].

[1] R. Kitchin, M. Dodge, The (In)security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention, Journal of Urban Technology, 21, 2017, pp. 1-19.

[2] Create-IoT-Project, Legal IoT Framework (Initial), Deliverable 05.05, December 2017.

The diversity of deployed devices in smart cities makes therefore security a multi-dimensional problem. Other principles provide that smart cities should support the harmonised cyber-security framework, manufacturers and solution vendors should integrate security in their products[3].If appropriate standards will not be developed it will become increasingly more difficult to encourage end-users to rely on IoT solutions.

5.2 Privacy and data protection concerns

Data protection within the context of smart cities can be seen from different points of view. First of all, one has to bear in mind that when we look at smart cities they are subject to different legislation in many parts of the world and therefore their regulation is not uniform. If we take into account the European situation, starting from a user-centred point of view, and taking into account the GDPR, we can derive important principles of significant importance for smart cities[4]. The GDPR enshrines a set of fundamental principles and norms that are always to be taken into account in the context of smart cities. Among them: lawfulness; fairness; transparency; purpose limitation; Data minimisation; accuracy; storage limitation; integrity and accountability. The GDPR also provides detailed norms for the collection of consent. The GDPR is more prescriptive when it comes to the conditions for consent, however the new rules transpose into law what was already required by certain supervisory authorities. According to article 4(11) of the GDPR consent means any "freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR also details the requirement for the processing of personal data of underage persons and processing of special categories of data. The GDPR sets out obligations provides for obligations towards the facilitation of the exercise of the data subject's right to information such as access to personal data, rectification and erasure, right to data portability. The legal provisions also enable the data subject to restrict processing of his data under certain circumstances and detail processes for objection and seeks to protect the individual vis-à-vis automated decision-making mechanisms.

The GDPR will require smart cities:

- the use of privacy by design, privacy by default and the use of the Privacy Impact Assessment in the design and management of ICT solutions using personal data
- the appointment of data protection officers

We have basic principles to implement privacy by design measures within smart cities. Here we have different options:

- Ann Cavoukian seven principles: proactive not reactive; privacy as default setting, privacy by design, positive sum, security, transparency, user-centric
- ISO 29100 standard: consent and choice, purpose, collection limitation, data minimization, use limitation, accuracy and quality, openness/transparency/notice/, individual participation and access, accountability, security
- Other jurisdictions are also developing legislation focused at protecting privacy. For instance Japan approved the *Act on the Protection of Personal Information* which entered into force on May 30th 2017[5]. The new law created the Personal Information Protection Commission, expands the scope and definition of the notion of "personal information" also by adding the new category of "Sensitive Personal Information". Under the Act information handlers are

---

[3] ENISA, Cyber Security for Smart Cities. An architecture model for public transport, December 2105.

[4] For a general scenario of legal framework see Create-IoT-Project, Legal IoT Framework (Initial), Deliverable 05.05, December 2017.

[5] Japan has enacted also other specific laws on the collection and processing of personal information. Among them: Act for the Protection of Personal Information Held by Administrative Organs; Act for the Protection of Personal Information Retained by Incorporated Adminisrative Agencies, etc.; Ordinances for the protection of personal information ser by each municipalities.

required to take necessary and appropriate measures to ensure the security of personal information. The measures that will be deemed appropriate to the case will depend on the nature, scope, context and purpose of use or processing of personal data and also the risks for rights and freedoms of individuals. In other parts of the world several countries are developing personal data protection legislations. For instance, there is nounified approach in the African continent where some countries have comprehensive personal data protection legislations and others have no legislation or contitutional protection. There are 14 countries which have enacted data protection legislation and the African Union has adopted the AU Convention on Cybersecurity and Data protection which still has to enter into force[6]. Also in South America different countries have enacted data protection laws: Argentina[7]; Costa Rica[8]; Mexico[9]; Perù[10]; Uruguay[11]. Brazil has approved a comprehensive data protection on August 14th 2018 to boost the adoption of IoT solutions and the development of smart cities in the country[12]. The law has become effective in February 2018. Key features of this new law are: the establishment of a national data protection authority, the introduction of the data protection officer, legal basis for data processing, consent requirements, notification of data breaches, privacy by design and privacy impact assessment, data transfer restrictions.

As we can see, many states are developing laws and regulations aimed at protecting the privacy of individuals. Privacy and data security-failures, in fact, are to be considered as one of the most important problem that can occur in smart cities. As the most important component in the development of smart cities are data and their use, one has to be particularly careful in their management, in fact: "IoT landscape heavily leverage on personal data to deliver services and increase consumers' welfare, personal data protection and security are key elements in the "value creation chain" of IoT"[13]. In this scenario the use of IoT devices in smart cities is not new, but makes more complex the subject's control over his own personal data and becomes more difficult to identify the legal grounds for personal data processing. The presence of multiple devices, data sources and entities processing personal data has also an effect on the acquisition of the data subject's consent which in the context of smart cities, under EU law, may constitute a legal basis for personal data processing of IoT deployments. There is therefore a direct relationship between IoT architectures in smart cities and privacy protection and this is the reason why an approach of privacy by design should be encouraged.

According to the GDPR, which is probably the most advanced legislation at the global level, many cities will need to comply with legal accountability obligations to European Data protection law. As data controllers, cities will be required to implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures when necessary. In each case cities will be called to evaluate which measures will be appropriate. This will depend on the nature, scope, context and purpose of the processing and also the risks for rights and freedoms of individuals. Regulators around the word are also embracing the concept of accountability as a key principle in data process management (privacy regulators in Canada, Hong Kong, Australia have issued "*Accountability Guides*" or "*Privacy Governance Frameworks*" in order to assist the private sector).

Basic frameworks to deal with IoT solutions, also in the context of smart cities, have been recently elaborated. Hyper-connectivity in fact entails a great deal of risks and calls for the development of a

---

[6] For a comprehensive overview see A.B. Makulilo, African Data Privacy Law (Springer: 2016).

[7] Personal Protection of Personal Data (Federal Law 25.326/2000).

[8] General Law on the Protection of Personal Data (Federal Law 8.968).

[9] Federal Law on Personal Data.

[10] Data Protection of Personal Data (Act 29.733/2011).

[11] Protection of Personal Data (Act 18.331/2008).

[12] IAPP, The hot topics warming up Brazil's data protection debate, 13/2/2018, available at: https://iapp.org/news/a/the-hot-topics-warming-up-brazils-data-protection-debate/.

[13] Create-IoT-Project, Legal IoT Framework (Initial), see supra at footnote***.

proper legal framework. The regulatory ecosystem of course will vary according to the different kind of activities in place. For what may concern data protection and privacy the Article 29 Working party has specifically raised the issue of privacy and security issues raised by the IoT.

5.3 Risk issues in data processing and management

Many unknown unknowns stem from data management and processing in IoT and SC&C, with a direct impact on the ecosystems's resilience and stability. As said in the following quote:
"Security is hard. Even in small organizations with well-understood network infrastructures, keeping intruders out cannot be guaranteed. Imagine a large, diverse infrastructure where a variety of bureaucracies and critical infrastructure components share complex interconnections with, perhaps, no overarching cybersecurity architecture. This is what your city probably faces."[14]
This uncertainty generates a variety of risks that should be identified and managed through a risk management process to ensure a safe development of cities. To this purpose, existing standards and methodologies[15] could be adapted to the specific needs, contexts and complexities of cities, communities and projects. Among these risks, privacy and security represent a significant threat. But as shown in Figure 16, a new paradigm calls for faster implementation of a dynamic risk management approach, able to anticipate risks, cyber risks and threats through an ongoing process.

Data-based decisions

Smart cities entail a growing number of data-based decisions related to a wide range of topics (energy, traffic, tax, safety, insurance, etc.) and stakeholders (citizens, cities, companies, etc.) hoping for effective, fair and unbiased decisions that will result in operational efficiency, sustainable economic growth and social justice. The efficiency of the decision-making process depends on technical and non-technical parameters such as algorithms, data quality and governance – each of which could be a source of bias or error. What, then, are the economic, social or environmental consequences of wrong decisions, bias or errors due to poor quality data, misinterpretation or an inability to use the data effectively?

New business models

The business models of a growing number of companies rely on data. We can then wonder if those business models are resilient to face data issues and uncertainty linked to new technologies (blockchain, AI…), if people (citizen, civil servant, business employees…) skills adjusted to the actual and future needs induced by digitalization[16], and in a more general manner, if corporate governance adapted to the changing economic world.

Digitalization also challenges the valuation models that shape corporate finance. The WIPO study shows that today, almost a third of the value chain is based on intangible capital[17], including databases, digital skills, technology, tools flexibility, data management process, ability to extract value from data and in a general way, anything that represents a know-how or an advance in the field of data management. Are business models and valuation resilient in this new era of technology? What are the consequences on business models and valuation of wrong decisions or errors due to poor

---

[14] Pen Testing a City, Gregory Conti (West Point), Tom Cross (Drawbridge Networks), and David Raymond (Virginia Tech)).https://www.blackhat.com/docs/us-15/materials/us-15-Conti-Pen-Testing-A-City-wp.pdf

[15] For example, existing standards and methods include, (i) The International Organization for Standardization (ISO) publishes ISO31000 standard on Risk management, (ii) Enterprise Risk Management by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, www.coso.org), (iii) an industry-level example – Operational Risk Framework, Basel Committee on Banking Supervision https://www.bis.org/publ/bcbs195.pdf, (iv) a country-level example from Switzerland, based on the NIST Cybersecurity Framework Core – *Minimum standard for improving ICT resilience*, Bern 2018, Federal Department of Economic Affairs, Education and Research (EAER), Federal Office for National Economic Supply (FONES).

[16] The Geneva Initiative on Capacity Development in Digital Policy. https://digitalswitzerland.com/2017/12/27/geneva-initiative-capacity-development-digital-policy/, https://igf2017.sched.com/info. The European project DigComp offers a useful framework: Digital Citizenship Education Volume 1 : Overview and new perspectives, octobre 2017 (p.23).

[17] Intangible Capital in Global Value Chains, World Intellectual Property Report 2017

quality data and inability to properly use the data? What are the consequences of data issues on customer relationship and reputation[18]? Are companies able to maintain high reporting capabilities / ability to capture the big picture of their activities within the interconnected environment generated by smart cities and IoT?

Moreover, the actual concentration of the global economy around a limited number of services, hardware and technology providers raises the questions of concentration risk, and of technological and data dependencies. For example, what could be the impact of a massive blackout (electricity, transportation, banking, etc.), obstacle resulting from economic competition or bankruptcy of a major service provider. Answers to basic questions such as "what time to return to normal?", "what happens during a blackout to maintain the activity?", or "can we still work with old systems?" [19] should be forecasted.

Finally, the current economic pressure on innovation could generate unexpected future costs. As stated by Sculley, Holt, Golovin, et al., "it is dangerous to think of these quick wins as coming for free". This encourages us to consider technological debt as a risk.

New borders of law

Legal issues are generated by data processing and management in IoT and SC&C, in a context of heterogeneity of stakeholders (public/private, cities/citizen, companies/startups…) and cutting-edge technologies (cross-border projects, data transferability and ubiquity, system openness, cloud etc.) :

- Jurisdiction issues related to legal framework of data processing and storage on public/private cloud, data transfer and cross border flows;
- Legal and governance issues associated with data ownership, data lock-in, seamless portability of the data among cloud service providers (e.g. mobile number portability);
- Real-time processing (5G, edge technology, real-time analytics, autonomous machines etc.) generating an acceleration of decision that can now be taken instantly through the delegation of decisions to algorithms and machines. This raises questions about algorithm ethics, control, fiability etc.;
- Subcontracting (cloud, outsourcing etc.).

Connectivity and Openess

The fact that Smart Cities and IoT are characterized by the use of "data for everything" and that devices, objects, tools, sensors, monitoring tools (…) can be opened and/or connected with other devices, tools, systems (…) generate huge data flows and data exchanges. This very high level of connectivity may generate a virality of threats: bad quality data contagion, dissemination of erroneous information resulting in panic, or dissemination of fake news [20].

Moreover, the fact that Smart Cities and IoT are characterized by the interaction of heterogeneous stakeholders/systems/devices can cause a quick and massive impact on the Ecosystem as a whole, problems migrating from one environment to another. At a highest level, one isolated problem can lead to a massive, general consequence on the whole ecosystem, generating a Systemic risk.

Such a risk is well studied and framed in the banking Industry, where Systemic risk is monitored and defined[21] as "The risk that the inability of one or more participants to perform as expected will cause other participants to be unable to meet their obligations when due." It could be interesting to translate

[18] Basel Committee on Banking Supervision (BCBS), 1989.

[19] https://www.club-ebios.org/site/presentations/ClubEBIOS-2015-09-08-PERTUS.pdf

[20] The GIP Digital Watch observatory for Internet governance and digital policy, Top digital policy developments in 2017. https://dig.watch/

[21] A glossary of terms used in payments and settlement systems, Committee on Payment and Settlement Systems, BIS

such a risk in the SC&C and IoT environment, where interconnexion, data flows, mutualization of services, devices or sources of energy can cause contagion of problems and failures.

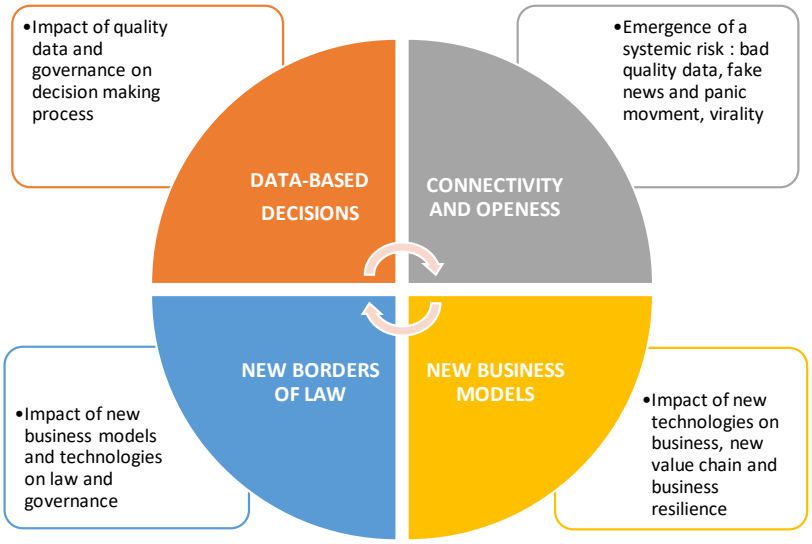

Figure 1 – Risks generated by Smart Cities and IoT specific context – a new paradigm

As we just described, risks generated by data processing and management in IoT and SC&C are numerous and varied. They embrace privacy and security risk, but also numerous other critical risks that stem from the tremendous use of data everywhere and at every stages of Smart Cities and IoT use. Probability of occurrence and magnitude of such risks must be evaluated, and responsibilities should be clarified in case of occurrence to determine who holds the risks and at the end, pay the costs of uncertainty. To this purpose, Section 6 describes how put in place a risk management methodology to ensure a safe growth and sustainability of Smart Cities and IoT.

5.4 Governance issues in data processing and management

Data in smart cities applications can represent enormous liability, asset, systemic and reputational risks in terms of safety, security, privacy and other aspects. For instance, replacing the content of surveillance cameras by fake data, or accessing the personal health data of a city inhabitant could raise major issues in case of data breaches. Similarly, the governance of data can play a significant role in facilitating interoperability, e.g. through the establishment of common standards. It can also be important in the creation of value and in monetization by clarifying rights and obligations, including user rights or ownership. The ethics of data processing and management is a significant concern in the collection, processing, packaging, application and monetization of data. Ethical concerns are driven by limited trust among actors, complex indirect relationships, concerns over bias in algorithms and asymmetrical access to information and resources in data processing and management. Such a scenario is typical of those that benefit from clear and broadly supported governance frameworks. There is, therefore, a need to provide guidelines and procedures for the governance and management of these data assets and to facilitate the exchange of best practices and expertise among cities. Applied to the governance of data security and privacy in smart cities, the following must be taken into account:

- governance frameworks are established by a combination of authorities, including international agreements and practices, national governments and the local governments in smart cities;
- the management of data within a governance framework is provided by a complex ecosystem of stakeholders (that could include public and private organisations, as well as suppliers).

For convenience, we use a definition of governance adapted from UNESCO and that focuses on strategic decision-making authority and the establishment of rights and responsibilities. This distinguishes governance from the management of data processing and management. The goals for data governance include, but are not limited to, the following:

- Create a data-driven and evidence-based informed culture.
- Avoid over-regulation and constraints on, or distortions to, the appropriate development of the sector.
- Promote equity, inclusion and transparency in the data economy.
- Continue and strengthen the data governance programme by adopting a collaborative innovation community capacity building ideas.
- Provide effective ways of enabling appropriate data privacy and security protection.
- Provide self-service business intelligence capabilities.
- Adopt suitable and effective data management tools.
- Redefine the roles of data-related analytics to provide better insights and predictions.

The benefits of a good data governance framework include the following:

- Reduce the costs of the creation, maintaining, disposition, storage and use of data.
- Improve the quality of data assets from cities and communities by making it trustworthy, accessible, available, usable and traceable.
- Enabling digital continuity of data to information to knowledge to smart action.
- Enhance revenue from the processing and monetization of data.
- Improve the value and diversity of direct and indirect benefits to citizens from data processing and management

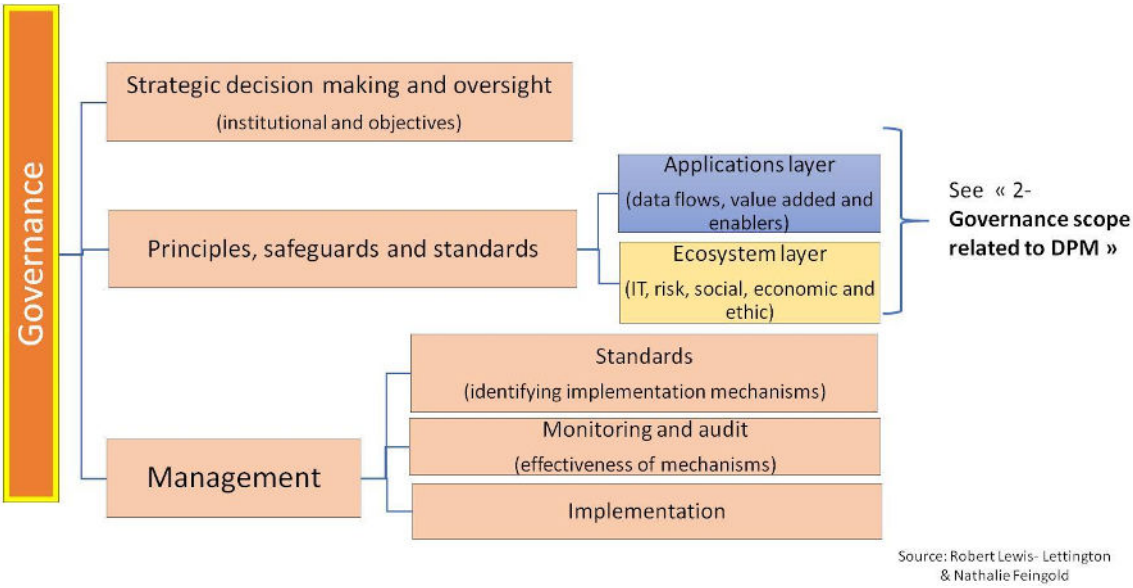

Figure 2 – Governance framework for DPM in SC&C

Figure 2 provides a framework for governance of DPM in SC&C described in thematic terms. It emphasizes the distinction and relationship between the governance and management elements. The governance element includes strategic decision making, which establishes the rights and responsibilities of DPM actors, and the setting of high-level objectives. The diversity of concerns is

an important feature, particularly the need to consider both ecosystems and applications layers of DPM activities. The management element includes the day to day implementation of the conclusions reached in the governance element. Good governance is achieved by equity and inclusion in the governance element and by clear monitoring and accountability mechanisms between the governance and management elements.

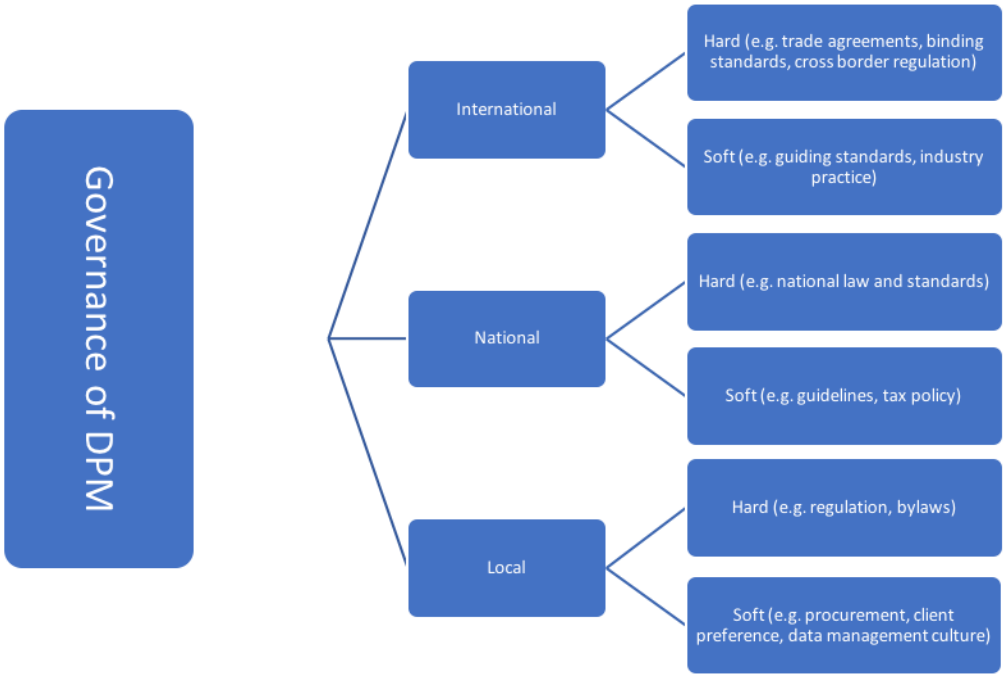

Figure 3. Jurisdictional framework for the governance of DPM in SC&C

Figure 3 describes the diversity of geographic, or jurisdictional, inputs into a governance framework. No actor, whether public or private, is truly independent in the governance of DPM for SC&C. They each need to map and consider the binding (hard) obligations and influences (soft) that apply to their particular activity and wider context. In well developed markets, local and national inputs into a governance framework are usually relatively well understood and easily identifiable, even if they are sometimes complex. International inputs are often more challenging, not least because of the transboundary nature of many DPM activities, even when focused on smart cities and communities. For example, many cloud based systems may depend upon the use of servers in multiple locations and that may make an activity subject to the laws of more than country. Similarly, some regulatory approaches to privacy focus on the legal status of the individual, and not the location of a transaction, and, therefore, may make the identification of applicable law more challenging.

6. Processes for security and privacy in data processing and management in the internet of things and in smart cities and communities

6.1 Collaboration processes for security and privacy

6.1.1 Collaboration in SC&C processes

Smart cities play a key role in digital ecosystems. While standards such as ISO/IEC 30141 (IoT Reference Architecture) or ISO/IEC 20547-3 (Big data Reference Architecture) explain roles that can be played in an ecosystem (e.g. a big data provider, big data application provider, big data consumer, an IoT user, IoT service provider, IoT service developer), smart cities typically play a management role.

ISO/IEC 30145-1 (Smart City ICT Reference Framework: Smart City Business) defines a process called “Safety, Security and Resilience”. The purpose of this process is to ensure that the City becomes, through the usage of innovative ICT, more safe and secure for its stakeholders and more resilient to natural and other disasters.
Security and privacy can involve global assets shared by organisations within an ecosystem. In that case their security and privacy processes must be globally coordinated as shown in Figure 1:

- each organization carries out its own security and privacy processes;
- an overall management of each organizations’ security and privacy processes ensures consistency of each individual process.

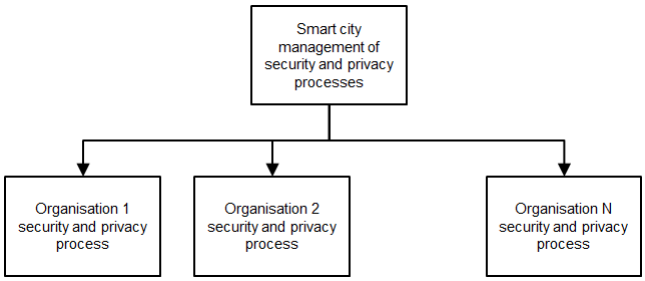

Figure 4 – Smart city management of security and privacy process

The type of management can take different forms. It could imply a strong involvement of the city authority, or it could carried out in association with third parties. Here are examples of security and privacy management approaches

- organizations involved in the operation of a transport service apply security and privacy processes that are directly coordinated by a city authority;
- organizations involved in the operation of a healthcare service apply security and privacy processes that could be coordinated by a national health authority, which in turn liaises with the city authority; and
- organizations involved in the operation of a weather broadcast service apply security and privacy processes that could be coordinated by a private company, which in turn reports to the city authority.

6.1.2 Guidance for organisations and ecosystems

Smart city management is needed on the data sharing chain. For instance an IoT system operator can collect data that is provided as a dataset to a service provider which in turn combines it with other sources of data and provides it to a data consumer. As shown in Figure ,**Error! Reference source not found.**

- each organization carries out its own data sharing process;
- an overall coordination of each organizations’ data sharing processes ensures the security and privacy of the data processing chain.

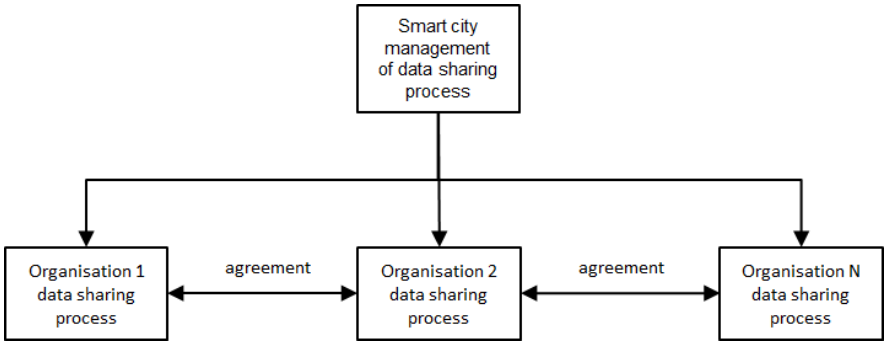

Figure 5 – Smart city management of data processing chain

The following guidance is provided:

- at the ecosystem level
    - identify the data processing chain operational requirements (such as velocity, veracity for a big data application, or scalability, provenance for an IoT service);
    - identify the security and privacy protection requirements of the data processing chain, such as data confidentiality, integrity, availability, unlinkability, transparency, intervenability;
    - identify specific requirements associated with each organisation role; and
    - establish security and privacy coordination schemes in the ecosystem, including measures for compliance, assurance and audit of practice.
- at the organization level
    - identify the specific organization operational requirements;
    - identify the specific organization security and privacy protection; and
    - establish data sharing process in accordance with the smart city management scheme.

6.2 Lifecycle processes for security and privacy

6.2.1 Security-by-design and privacy-by-design

Lifecycle processes must integrate a combined security and privacy by design approach. Security and privacy-by-design can be defined as the institutionalisation of the concepts of privacy and security in organisations and integrating them in the design, and life cycle of systems. Security-by-design focuses on objectives associated with:

- the protection of ICT assets;
- attributes such as confidentiality, integrity, availability (described in Table 3).

Privacy-by-design focuses on objectives associated with

- the application of principles for privacy-by-design and privacy-by-default, as listed in Table 1 (from Ann Cavoukian[22]), or in Table 2 (ISO/IEC 29100[23]);
- attributes such as unlinkability, transparency, intervenability (described in Table 3).

Proactive not Reactive; Preventative not Remedial
Privacy as the Default Setting
Privacy Embedded into Design
Full Functionality — Positive-Sum, not Zero-Sum
End-to-End Security — Full Lifecycle Protection
Visibility and Transparency — Keep it Open
Respect for User Privacy — Keep it User-Centric

Table 1: Privacy-by-design Principles from Ann Cavoukian

Consent and choice
Purpose legitimacy and specification
Collection limitation
Data minimization
Use retention and disclosure limitation

[22] Ann Cavoukian. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[23] ISO/IEC 29100 - Privacy framework is freely available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Accuracy and quality
Openness
Transparency and notice
Individual participation and access
Accountability
Information security
Privacy compliance.

Table 2: Privacy Framework Principles (ISO/IEC 29100)

Attribute		Description	Examples
Security protection attributes[24]	Confidentiality	Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.	Protected transmission of collected data, protected access with suitable authentication schemes, protected processing of data, and protected storage.
	Integrity	Ensures the accuracy and completeness of data over its entire life cycle.	Protection of integrity during transmission, processing of data, as well as at storage level
	Availability	Ensures accessibility and usability upon demand by an authorized entity	Preventing service disruptions due to power outages, hardware failures, or security denial of service attacks.
Privacy protection attributes[25]	Unlinkability	Ensures that a user may make multiple uses of resources or services without others being able to link these uses together	A user has two vehicles collecting data.
	Transparency	Ensures that an adequate level of clarity of the processes in privacy-relevant data processing is reached so that the collection, processing and use of the information can be understood and reconstructed at any time.	Understandable documentation covering technology, organization and responsibilities accessible to the user
	Intervenability	Ensures that users, data controller, data processors and supervisory authorities can intervene in all privacy-relevant data processing	processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions

Table 3: Security and Privacy Attributes

The integration of security and privacy has an impact on the overall lifecycle process. ISO/IEC 15288[26] describes the following categories of process:

- agreement processes (e.g., the supply process);
- organizational project-enabling processes (e.g., the quality management process);
- technical management processes (e.g., the risk management process); and
- technical processes (e.g., the system requirements definition process).

Table 4 shows the processes where the security and privacy for data processing must be integrated.

Type of process (ISO/IEC 15288)	Selected system life cycle processes (ISO/IEC 15288)	Security and Privacy engineering for data processing managment
Agreement processes	Acquisition process	

[24] From ISO/IEC 27000 Information security management systems — Overview and vocabulary

[25] From ISO/IEC 27550 Privacy engineering

[26] ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes

	Supply process	Negotiation of security and privacy capabilities between data processing stakeholders
Organizational project-enabling processes	Knowledge management process	Using this security and privacy framework
Technical management process	Risk management process	Managing a combined security and privacy risk analysis process Integration of resulting organisational and technical measures
Technical processes	Stakeholder needs and requirements process	Architecture description
	System requirements definition process	Carrying out a combined security and privacy risk analysis process Identifying mitigation measures
	Architecture definition process and design definition process	Designing mitigation measures

Table 4 - Selected system life cycle processes

The security-by-design and privacy-by-design process capability allow for the design and development of security and privacy capabilities. Several catalogs are available, such as standards such as ISO/IEC 27001 and ISO/IEC 27552 or the LINDDUN catalog[27] describes a catalog of security and privacy controls/capability. Figure 3 provides a usage and functional view based on the LINDDUN catalog.

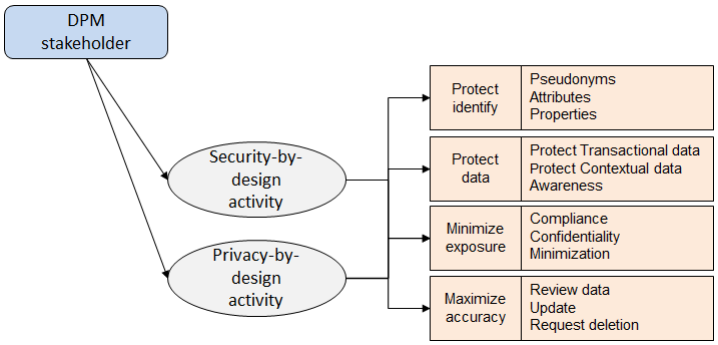

Figure 6 –Security and Privacy High Level Functional View

6.2.2 Guidance for organisations and ecosystems

Smart city management is needed on the lifecycle process. For instance,

- Organisations could agree on the use of similar controls, e.g.
  - an agreed level of protection for data at rest,
  - an agreed level of integrity and authentication for data in motion,
  - an agreed level of availability for data processing,
  - an agreed level of de-identification of data,
- organisations could agree on coordination for incident management, e.g.
  - an agree level of incident preparedness,
  - a common alert mechanism on security breaches (e.g. tampering detection) or on privacy breaches (e.g.re-identification detection).

27 https://linddun.org/solutions.php

As shown in Figure 1:

- each organization carries out its own security and privacy lifecycle process;
- an overall coordination of security and privacy lifecycle ensures a consistent treatment of the assets to protect.

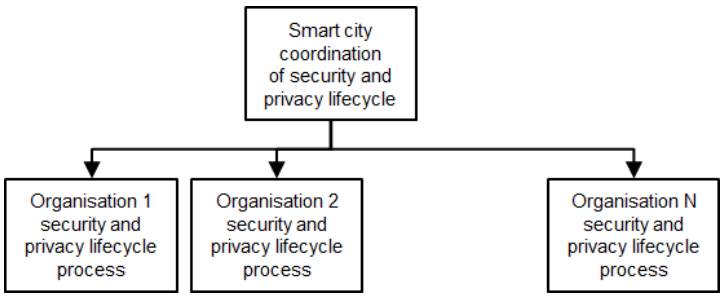

Figure 7 – Smart city management of security and privacy lifecycle.

The following guidance is provided:

- at the ecosystem level,
  - identify the processes in the ecosystem lifecycle where coordination is needed (assurance, compliance verification, incident management, audit).
  - Identify the controls that are implemented in the ecosystem further to the risk analysis coordination.
  - establish control coordination schemes in the ecosystem, including measures for compliance, assurance and audits of controls.
- at the organization level
  - identify the processes in the system lifecycle where security and privacy concerns need to be integrated.
  - identify the controls that are implemented in the system further to the risk analysis process;
  - establish the lifecycle process in accordance with the smart city management

6.3 Risk management in data processing and management

Data processing and management in Smart Cities and IoT generate uncertainty, many unknown unknowns that may constitute a threat to the stability of the system, the efficiency of the operations, or the wealth, the health or the dignity of the persons. Thus, it is the responsibility of the ecosystem to identify and measure the risks linked to data processing and management, and to manage it.

Risk is a cross-cutting element that relates to security and privacy but also has a broader relevance that needs to be addressed.

Regarding security and privacy, dedicated methodologies can be used. But more generally, global risk methodologies should be embraced to ensure a full securing of the ecosystem and an optimal forecasting and management of all the different risks.
Whatever the methodology, projects under construction should be challenged in the light of identified risks and threats to ensure their success in term of economics, social and societal growth.

6.3.1 Security and privacy risk analysis

Figure 4 depicts the relations between the components of a security and privacy risk analysis; the risk sources, the breaches and the consequences. Risk sources include:

- Personal data processing risks arising from the operations of the system itself such as distortion, surveillance, or unanticipated revelation

- risks caused by potential threats and vulnerability of a system, such as an unauthorized access to data.

Consequences that might arise as a result of privacy risks include:

- impact on citizens' privacy, such as exclusion, stigmatization, economic loss, control, influence or blackmail;
- impact on the operations and business of an organization, such as the impossibility to run the business

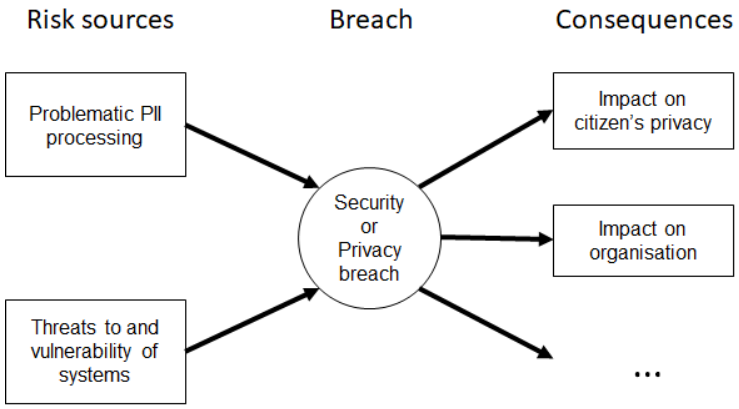

Figure 8 – Security and Privacy Risk Sources, Breaches and Consequences

Several methods are possible. The example below (Table 5) is based on the TVRA method[28]. TVRA focuses on security. We have extended it to cover both security and privacy.

TVRA Method process	Extension to data processing security and privacy risk
Identification of target of evaluation	Selection of data processing stakeholder
Identification of objectives	Identification of security and privacy objectives objectives
Identification of functional security requirements	Identification of functional security and privacy requirements
Systematic inventory of assets	Systematic inventory of assets
Systematic identification of vulnerabilities	Systematic identification of vulnerabilities using STRIDE[29] and LINDDUN[30]
Calculation of the likelihood of the attack and its impact	Calculation of the likelihood of the attack and its impact
Establishment of risks	Establishment of risks
Security and privacy countermeasure identification	Security and privacy countermeasure identification using categorisation of controls as used in ISO[31]
Countermeasure cost-benefit analysis	Countermeasure cost-benefit analysis
Specification of detailed requirements	Specification of detailed requirements

Table 5 – Risk Analysis Process

To go further, ISO/IEC FDIS 27005:2010(E) provides a detailed overview of different Information security risk assessment approaches[32].

---

[28] TVRA: Threat, Vulnerability and Risk Analysis. ETSI document. http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf

[29] STRIDE threat model; https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[30] LINDDUN privacy threat analysis methodology, https://www.linddun.org/

[31] These categories are used in ISO/IEC 27002 (Code of practice for information security controls), 27552 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines), 29151 (Code of practice for personally identifiable information protection).

[32] ISO/IEC FDIS 27005:2010(E) : p19 and p20 and Annex E (informative)

6.3.2 Risk management

To ensure a global risk management approach, covering most of the potential risks generated by DPM in SC&C and IoT, one can rely on robust methodologies and frameworks. For example, ISO31000 standard, published in 2009 (and reviewed in 2018) to provide principles and generic guidelines on risk management[33]. We can also cite Coso Enterprise Risk Management [34] (Committee of Sponsoring Organizations of the Treadway Commission) or several other methodologies mainly oriented on IT such as OCTAVE, EBIOS, MEHARI or NIST SP 800-82 for example[35]. Each methodology/framework proposes a step-by-step guidance. They can be chosen or used together according the size, the complexity or the culture of the ecosystem to which it is addressed.

To illustrate with an example at an Industry level, the Banking Industry works under the Operational Risk Framework as sponsored by the Basel Committee on Banking Supervision[36]. And as another example, at a Country level, the Swiss Government proposes a Minimum ICT Standard[37] based on the NIST Cybersecurity Framework Core[38].

For our specific focus on Risk Management linked to data processing and management in SC&C and IoT, and with the main objective to open a discussion and help stakeholders implementing Risk Management and adapt it to their specific needs and context, we propose to use the common canvas of Coso (mainly oriented on Governance and Communication) and Basel standard (mainly oriented on calculation accuracy and losses modelling) (Figure 9), which is in line with the ISO31000 Standard.

Figure 9 – Steps to risk management

a) Risk identification

The first step of the risk management process is the risk identification through a bottom-up approach based on proven risks, enriched with a prospective, top-down approach whose goal is to anticipate potential risks.

ISO/IEC FDIS 27005:2010(E)[39] lists typical threats about Information technology/Security techniques/Information security risk management.

b) Risk analysis

Risk analysis is the second step. Several methodologies can be used to analyze the risk. As described in ISO/IEC 27005, “risk analysis may be undertaken in varying degrees of detail depending on the criticality of assets, extent of vulnerabilities known, and prior incidents involving in the organization.”

Whatever the chosen methodology, the objective is to be able, for each risk identified (cf risk identification) to assess its impact in term of consequences and likelihood.

Let us illustrate this, by taking several examples of risk analysis application.

---

[33] Risk Management Basics, ISO31000 standard, Louis Kunimatsu, CRISC, IT Security and Strategy, Ford Motor Company

[34] https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[35] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf Add OCTAVE, EBIOS, MEHARI references

[36] https://www.bis.org/publ/bcbs195.pdf

[37] Minimum standard for improving ICT resilience, Bern 2018, Federal Department of Economic Affairs, Education and Research EAER, Federal Office for National Economic Supply FONES

[38] https://www.nist.gov/cyberframework

[39] ISO/IEC JTC 1/SC 27 Information technology - Security techniques - Information security risk management

First example, Coso proposes to apply a methodology calls Heat Map[40] as shown in the following simple example (Figure 10) where consequences (here called potential impact) and likelihood are classified according the level of risk.

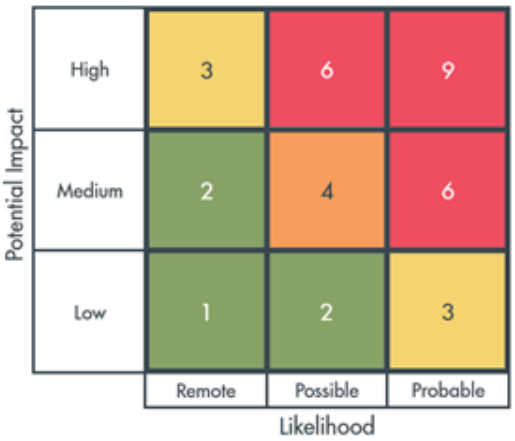

Figure 10 – Enterprise Risk Assessment scale, source : CGMA (Chartered Global Management accountant) January 2012

For a second example, let us illustrate risk analysis at an industry level. In the banking industry, risk related to Data Processing and Management can be categorized in Operational Risks with historical of losses often described as a Loi de Poisson (Figure 8): likelihood (here called loss frequency) and consequences (here called loss severity) show 1/ frequent events with low probability of loss and 2/ low frequency events with high severity loss (extreme events). In Banking, data about frequency and severity of losses are collected and gathered to improve the accuracy of the risk analysis for the whole Industry[41].

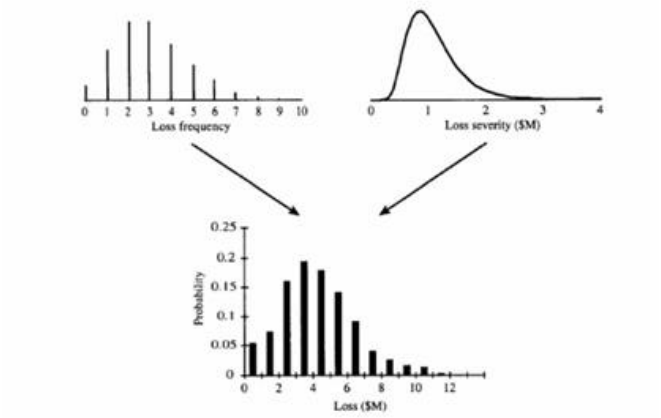

Figure 11 – Operational risk[42]

As a third example, the aeronautical industry also collects data about incidents to improve accident prevention and risk management for the whole Industry[43]. Such collections should be organized at a high level in the Smart Cities and IoT ecosystem to help the whole ecosystem in improving risk assessments.

---

40 Coso risk assessement in practice, By Deloitte & Touche LLP Dr. Patchin Curtis | Mark Carey. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

41 Loss collection https://www.bis.org/bcbs/publ/d355.pdf or Loss Data Collection Exercise https://www.ffiec.gov/ldce/

42 John Hull : Risk management and financial institutions

43 See Aviation accidents and incidents statistics such as The Bureau of Aircraft Accidents Archives (B3A) established in Geneva in 1990 for the purpose to deal with all information related to aviation accidentology: http://www.baaa-acro.com/

c) Risk evaluation

"The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk" [44]

Risk evaluation and decisions should take into account the organizations tolerance, also called risk appetite: "Risk appetite can be defined as 'the amount and type of risk that an organization is willing to take in order to meet their strategic objectives. […] Organizations have to take some risks and avoid others. To do so, they need to be clear about what successful performance looks like. This question may be easier to answer for a commercial organization than for a government department, but can usefully be asked by boards in all sectors."[45]. This quote, from Institute of risk management, invites all kind of organization to discuss their risk appetite, whatever the difficulty to do so. The maximum risk an organization, an ecosystem is willing to take is something that should be clearly articulate and communicate. The risk appetite of any organization should be defined. This means that the amount of loss that the organization accepts (is able) to bear should be assessed to adapt the risk treatment accordingly.

In other words, SC&C and IoT stakeholders should be able to assess their risk appetite and manage the consequences and the costs of uncertainty generated by their operations.

d) Risk treatment

Risk treatment can be defined as "preventive measures designed to minimize the probability that the negative events described can occur [and] containment measures designed to detect and limit the effects on the business of events which bypass preventive controls and threaten operations." [46]

Four risks responses are commonly described and used by the risk managers community to treat the risk:

- Modification,
- Retention,
- Avoidance,
- Sharing.

So, various actions, such as the improvement of tools and processes, monitoring and control, training, data literacy, insurance, subcontracting etc. all contribute in addressing risks. An efficient risk management process consists in taking risk treatment decisions based on a multidimensional analytics approach including the environment, the culture, the severity of the potential losses and the risk appetite.

6.3.3 Guidance for organisations and ecosystems

Each and every project under construction should be challenged in the light of identified risks and threats to ensure their success in term of economics, social and societal growth. Whatever the chosen methodology, based on the 4-steps canvas described in 6.2, the following best practices are proposed:

a- Risk identification:

A list of typical threats is a foundation that must be completed by a list of specific threats related to the studied project/environment/perimeter. In the context of our focus group, we identified four families of specific risks related to data processing and management in SC&C and IoT (Figure 16 in

---

[44] Risk Management Basics, ISO31000 standard, Louis Kunimatsu, CRISC, IT Security and Strategy, Ford Motor Company

[45] https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/

[46] Risks in computer and telecommunication systems (July 1989), https://www.bis.org/publ/bcbsc136.pdf

4.3). But data-related threats evolve as smart cities and IoT develop, prompting the evolution of the risk management fundamentals of threat lists. Hence, it is advisable to continually enrich and update the lists of typical and specific threats on a regular basis.[47]

b- Risk analysis

Based on the experience of other industries, such as banking or aeronautics, it could be benefic to start building, without delay, a loss collection related to Data Processing and Management in IoT and SC&C, fed and shared by all the stakeholders, to help the Ecosystem managing its risks and improving the risk assessment's accuracy by facilitating likelihood calculation. Such collections should be organized at a high level to benefit the whole ecosystem.

c- Risk evaluation

The question of risk appetite and, more pragmatically, who bears the risks and will have to bear the costs of uncertainty (companies, governments, cities or citizens?) is a critical issue. The maximum risk an organization or an ecosystem is willing to take is something that should be clearly articulated and communicated. The risk appetite of any organization should be defined. This means that the amount of loss that the organization accepts (or is able) to bear should be assessed to adapt the risk treatment accordingly. Stakeholders should be able to assess their risk appetite and manage the consequences and the costs of uncertainty generated by their operations. In a UN perspective, for each potential risk/breach, the Ecosystem should propose an appropriate response that preserves the poorest and most vulnerable people.

d- Risk treatment

The following is a selection of efficient actions that can be taken in the specific context of DPM in IoT and SC&C:

d.1 - Data minimization[48]:

As of today, data are considered as an asset, and often compared to oil or gold. So then it is tempting to collect and store a maximum of data, even sometime "just in case" or for "legacy" purposes. This behavior is reinforced by the ease of storage at lower cost made possible by more and more efficient technologies.

But data is not an asset like the others: ubiquity, obsolescence, heterogeneity (quality, format, historical depth…) make their management complicated and their value is related to a multiplicity of factors.

Hence, minimize data collection and storage has often no impact on efficiency or business and reduces significantly the related risks.

To support this, we can recall that, according Veritas Databerg report[49], only 14% of data are business critical. The other 86% or either dark, or ROT (redundant, obsolete or trivial).

Two other examples:

- the French CNIL. From EBIOS methodology, guide to manage the risks. Frame Maintenance and Data destruction.[50].

---

[47] For example, in the banking industry, the Basel Committee proposed a first list of risks that the actors are continually expanding. The Coso also recommend improving the risk assessment process to be align with the evolution of the technologies and markets (as of today, Coso recommend taking into account the data issues, but hasn't yet include the data in the model itself.)

[48] Internet of things, privacy & security in a Connected World, FTC Staff report. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[49] Veritas, the Databerg Report, Identify the value, risk and cost of your data, http://info.veritas.com/databerg_report

[50] Les guides de la cnil - Edition 2017. La sécurité des données personnelles. https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

- Effective contingency plans, provisions for off-site backup of critical data files, of software and of hardware, as well as alternative means of processing information[51].

d.2- Foster data aggregation capabilities and end-to-end visibility of treatments

- Global risk monitoring relies on the ability to analyze data and capture the big picture of an activity through a capacity of reporting and data aggregation. It also relies on the end-to-end visibility of treatments. Indeed, operational data governance is a condition to control, monitor and protect the ecosystem as it allows the cartographic understanding of the data owned, used and stored by the system: what data, who produces the data and why, where do the data come from and where are they stored and secured.
- Main obstacles to reporting, data aggregation capabilities and end-to-end visibility are: shadow systems, existence of silos, system or language heterogeneity, problems of interoperability or technical issues. Hence, organisations and ecosystems should also coordonate efforts at a high level to foster data aggregation capabilities and end-to-end visibility of treatments[52].

d.3- Communication

Risk management is a process, ongoing and flowing[53] through each entity of a system. It relies on guidelines, machines and people, at each stage of the organization. Thus, risk can be mitigated thanks to a fluent communication between heterogeneous systems and players, and the dissemination of clear guidelines established and based on a common language, the availability of a readable documentation, including definitions and calculation methodologies if any, clear labels and metadata encouraging data lineage and end-to-end visibility of data processing.

d.4- Dissemination of a risk and data culture

Risk can be mitigated thanks to the dissemination of data literacy and the development of a data culture. Awarness about data and risks is key to mitigate the risks. This postulate was one of the major themes of the Internet Governance Forum (Dec. 2017, Geneva) whose title was "Shape your digital future!"[54]. Through these works and discussions, a consensus emerges about the three following points:

- The need to evaluate people available skills and compare them to the one that are needed to apprehend our digital world. See for example, DigComp[55] framework, or the proposition of personalized management of training and self-evaluation courses[56];

---

[51] Basel Committee on Banking Supervision (BCBS), 1989.

[52] Such a recommendation is adressed by BIS to the Banking industry : "Principles for effective risk data aggregation and risk reporting" https://www.bis.org/publ/bcbs239.pdf

[53] See COSO – *Enterprise Risk Management – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, September 2004

[54] Conferences accessible on https://igf2017.sched.com/info

[55] More info on https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

[56] « Fonction Finance : 140 innovations au service de la croissance ». Collection les Livres Blancs, Pôle de compétitivité mondial FINANCE INNOVATION, 2018 (PI 21 et PI 22)

- The need to bridge gaps and train individuals through continuous and flexible training plans. As remind us the council of Europe[57], digital training is a process, not a state that individuals reach after validating a training;
- The need to become aware of the importance of soft skills, to encourage curiosity and creativity to understand and understand the digital world and the changes it generates.

d.5 Coordination

Smart city management is needed on the risk management process. For instance if the data collected by a IoT system operator and provided as a dataset to a service provider is compromised, then the operations of the service provider will be compromised.

- each organization or project should carry out its own management of risk;
- an overall coordination of risk management ensures a common understanding of the risks at ecosystem level.

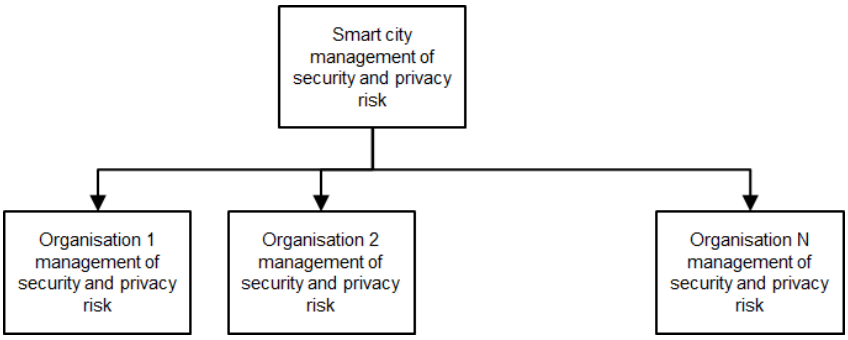

Figure 12 – Smart city management of security and privacy risk

7. Governance framework for data processing and management

7.1 Pillars of data governance

The 3 pillars of data governance are:

- Rules and policies that would allow a smart city governing body or national authority to supervise the activities related to DPM, i.e. to capture a *big picture* of its activity and by extension, of the related data.
  - A smart city should be able to capture the big picture of its activity, and by extension should also be able to capture the big picture of the data owned, used and stored within the ecosystem.
  - The big picture should accurately capture the activity. Organizations of the ecosystem involved in data processing should facilitate data aggregation capabilities and reporting practices to enhance activity and risk monitoring, supervision, and to be able to identify and track problems quickly.
  - Data lineage and end-to-end visibility of data processing may be hampered by the existence of silos, the lack of a common language or the existence of shadow system. This is the reason why an interoperability viewpoint must also be taken (covered below)
  - The manipulation of data requires agility provided by flexible tools that need to be sharply designed for clear purposes. But it happens that the end model is unknown because it is a new activity or a new sector, as IoT and smart cities businesses. As long as the end model

[57] Digital Citizenship Education Volume 1 : Overview and new perspectives, Octobre 2017 (p.23)

is not known, ad-hoc tools can't be designed and granular data should be collected to keep the maximum flexibility.

- Rules and policies on *data quality*.
  - Each organization should be able to classify data and recognize whether data are critical for the organization or not.
  - Critical data should always be secured, updated, and everything should be done to keep their highest level of quality through time.
  - The quality of high value data needs to be monitored on a regular basis and should be everyone's business in the Ecosystem.
  - Data quality is always the result of an ongoing effort.
  - Each type of data should be characterized by a life cycle, allowing the application of appropriated rules (i.e. delete obsolete data).
  - Redundant, trivial or obsolete (ROT)[58] data shouldn't be stored and should be deleted to limit the resources wastage linked to storage, security, IT processing and data mining.
  - There is a « butterfly effect » of data quality[59]: poor data quality is contagious. Errors spread along the process because there is porosity between databases.
  - Poor data quality is recurring: same anomalies come back over and over if the problem is not addressed.
- Rules and policies on *data users, providers and lineage*. The identification of data users and providers and the enhancement of data usability and lineage through *lineage management tools* are needed:
  - "Fit for use data" requires communication between users and providers.
  - The main obstacles to communication between users and providers are:
    - users and/or providers are not clearly identified;
    - silos: sometimes people do not communicate because they do not work together, organizations are segmented;
    - there is time lag between production and use of data: data are used several months or years after production.
  - To improve communication, tools are used to improve « usability » and lineage of data. Those tools are:
    - The use of a common language;
    - The availability of a readable documentation, including definitions and calculation methodologies if any;
    - Labels;
    - Metadata.
  - The importance of lineage and usability of data should be known and understood by each and every provider and user.
  - Governance must foster the "Data Quality Culture".

7.2 Relationship between security, privacy and governance

The relationship between security and privacy is showed in Figure 10.

[58] See the Veritas Databerg report. http://info.veritas.com/databerg_report

[59] See "The Butterfly Effect of Data Quality", MIT conference, Steve Sarsfield

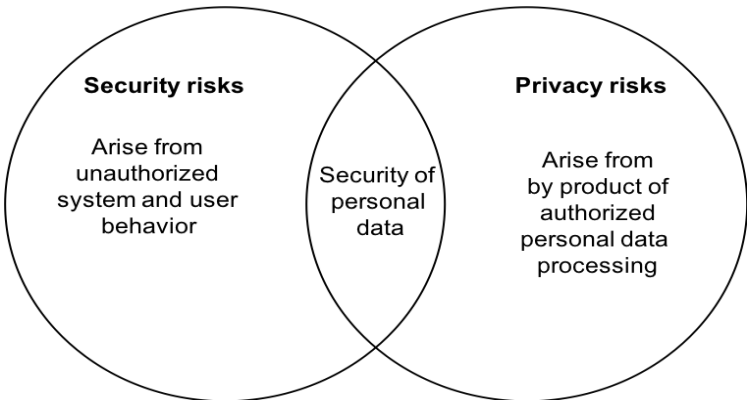

Figure 13 - Relationship between security and privacy (Source: ISO/IEC 27550 privacy engineering for system life cycle processes)

The relationship between security, privacy and governance is shown in Figure 11:

- a governing stakeholder applies a governance process in an ecosystem
  - to establish policies,
  - to monitor a data processing management (DPM) stakeholder who provides services on data assets, and
  - to monitor services in operation.
  - an entity can be a person, a system, an organisation;
- a data processing management stakeholder provides a service on data assets, following policies;
- a data processing management stakeholder applies the following processes:
  - a collaboration process in order to manage data sharing agreements between DPM stakeholders in the ecosystem,
  - a lifecycle process to manage data assets used and updated by the service, according to policies established by the governing body, and
  - a risk management process to manage security and privacy risks on the data assets.

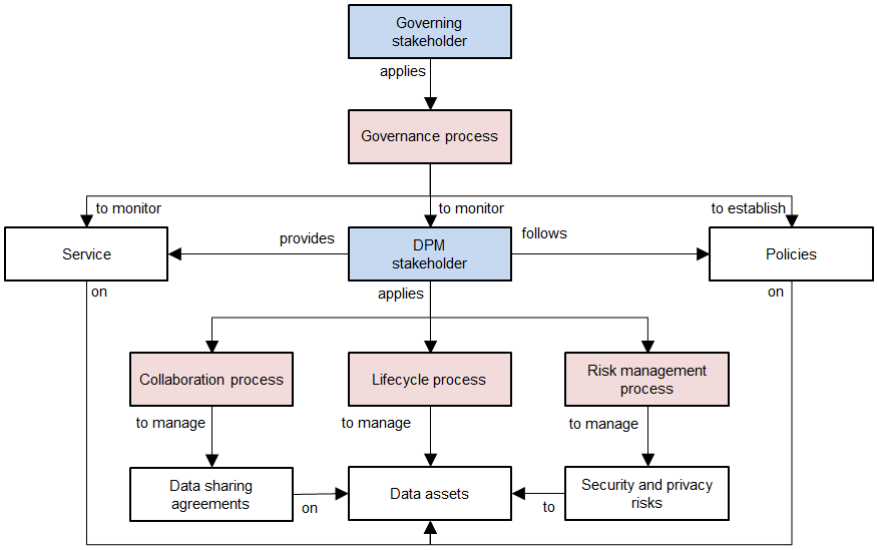

Figure 14 – Relationship security, privacy and governance in DPM

Figure 15 describes the elements for a data governance framework for IoT and SC&C based on three key dimensions:

- the governing subject dimension which provides a participant plan,
- the governing object dimension which provides a data plan, and
- the governing process dimension which provides a data process and management plan.

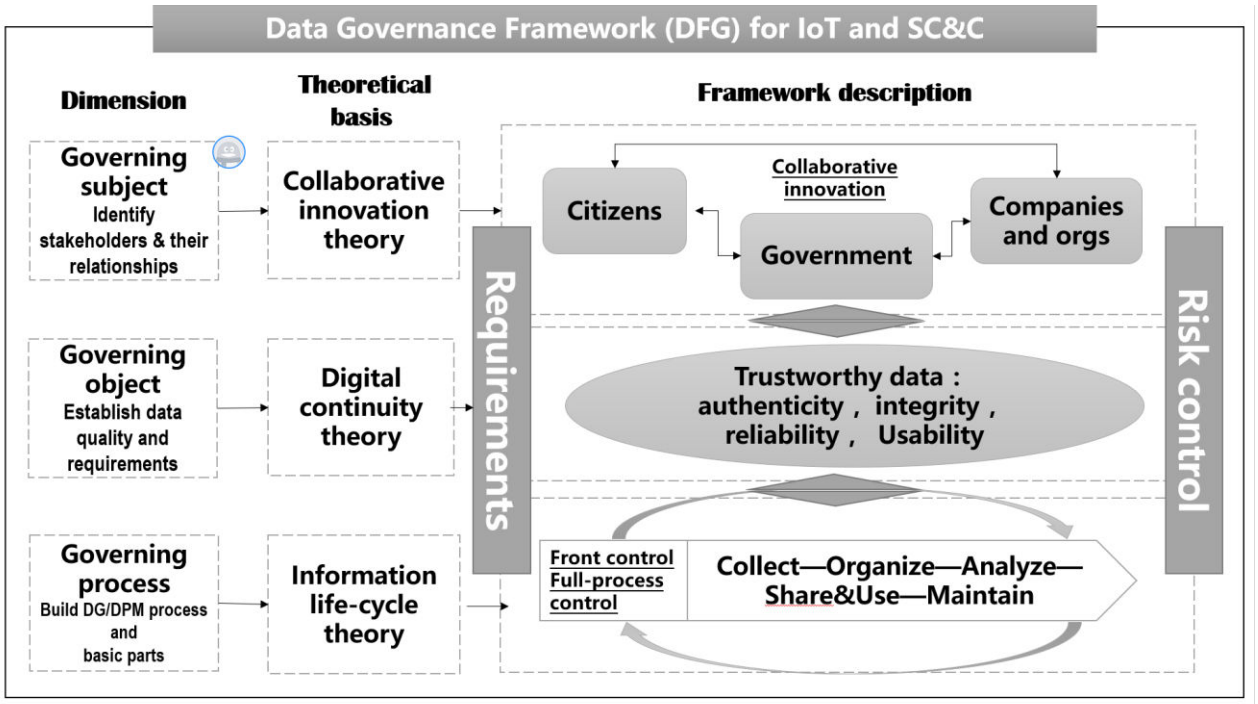

Figure 15 – Key components of a data governance framework

7.3 Impact of ecosystems on governance

A data governance framework should include an ecosystem viewpoint. Data processing will not be associated with a single organisation, but with a number of interconnected stakeholders. Figure 16 lists examples of such stakeholders:

- Suppliers provide the components making up the ICT infrastructure: a sensor, a (smart device), a cloud system, electronic components, security components, operating systems, middleware, tools, methods and so forth.
- Integrators build an ICT system, integrating the various components provided by suppliers.
- Operators deploy, operate and maintain the IoT system.
- Application managers are the interface with end-users.
- Policy makers provide rules concerning the application.
- End users are the beneficiary of the IoT system.

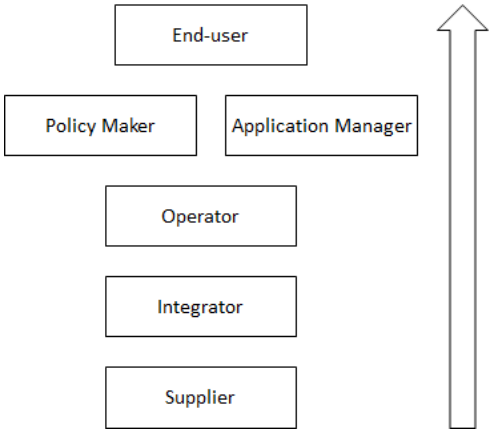

Figure 16 – Ecosystems Stakeholders

The following is an example for a smart transport application providing real-time traffic advice to citizens. End users are the inhabitants of a city. The application manager and the policy maker is the city. The operator can be a local SME associated with a major international cloud operator. The integrator can be a very large company with experience in building complex systems. The suppliers can be local producers of devices (e.g. a display system), an external start-up providing features for real-time advice, and a big operating system provider.
The resulting complexity of an ICT ecosystem also has an impact on the way security and privacy can be integrated. Figure 17 shows the specific roles and stakeholders that need to be taken into account when focusing on security and privacy.
From the security viewpoint:

- suppliers provide components that may contain security capabilities (e.g. dedicated security hardware, or security mechanisms integrated in a larger component);
- integrators have to provide the overall security capabilities integrating those provided by suppliers;
- security operators have to carry out the specific security operation duties (e.g. security supervision, security incident management);
- security authorities provide operation rules to the security operators (e.g. guidelines upon security incident):
- auditors verify that operation rules are well followed (e.g. security management conformance);
- application managers get the operation rules from the security authority;
- end users or the beneficiary of the IoT system are protected at the security level.

Likewise, from the privacy viewpoint:

- suppliers provide components that may contain data protection capabilities (e.g. de-identification mechanisms);
- integrators have to provide the overall data protection capabilities integrating those provided by suppliers;
- data controllers and data processors carry out data protection related operations (e.g. consent management, privacy breach management);
- data protection authorities provide operation rules to the data controllers and data processors (e.g. privacy impact analysis guidelines);
- auditors verify that operation rules concerning privacy management are well followed;

- application managers get the operation rules from the data protection authorities;
- end-users or citizens using the IoT system are protected at the privacy level.

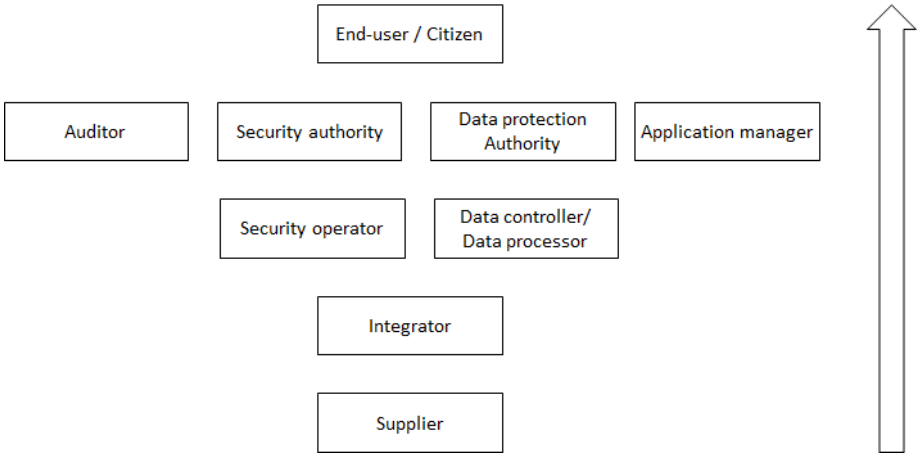

Figure 17 – Ecosystems Stakeholders from a Security and Privacy Viewpoint

A security and privacy framework for data processing management should take into account an interoperability viewpoint. This is motivated by two interoperability scenarios: a supplier scenario and a data sharing agreement scenario.
Figure 18 illustrates a supplier scenario:

- suppliers provide data processing security and privacy capabilities;
- these capabilities are integrated in the subsystems that the suppliers are providing to an integrator;
- the integrator must ensure that the overall data processing security and privacy capability integrates properly the suppliers' capabilities;
- these capabilities are used by data processing stakeholders, e.g. a market place operator, or a service provider.

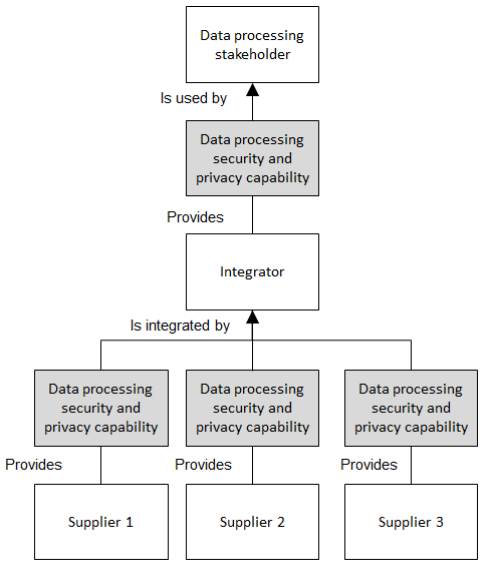

Figure 18 – Interoperability in a Supplier Scenario

Figure 19 illustrates a data sharing agreement scenario:

- two data processing stakeholders A and B negotiates a data sharing agreement;
- data processing stakeholder A provides data to data processing stakeholder B;
- the data sharing agreement set outs obligations on data processing security and privacy capabilities provided by each stakeholder.

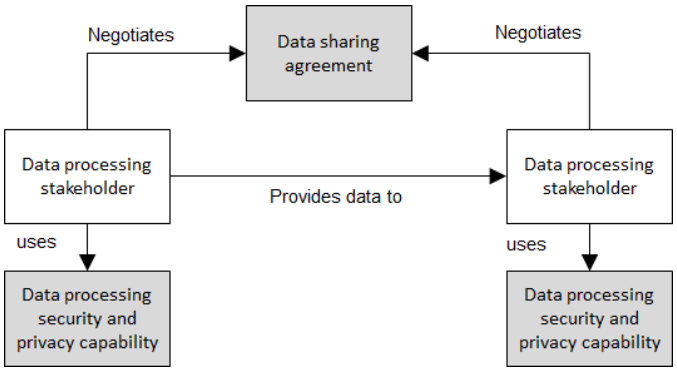

Figure 19 – Interoperability in a data sharing agreement scenario

The fact that different stakeholders must combine security and privacy capabilities means that a common security and privacy description is needed (for instance a common information model integrating security and privacy descriptions), as shown by Figure 20.

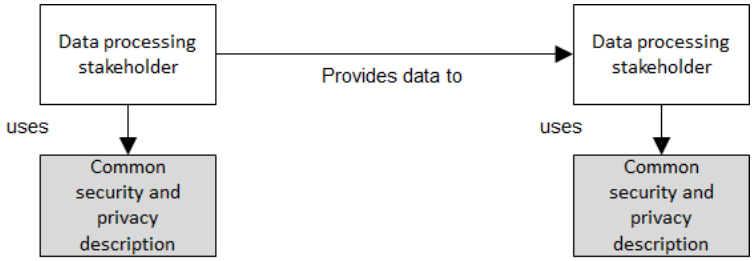

Figure 20 – Common Security and Privacy Capability Descriptions

7.4 Governance enablers

Table 6 provides a list of elements that are useful for describing and structuring governance.

Enablers		Key components	Requirements and roles
Governing subject (Arrangement of governance)		Government	Responsibilities, commitment
		enterprise	Obligations, engagement
		individual	Right and benefit, involvement
	Front-control	Requirements	Functional requirements ▪ (with respect to the different DPM capabilities indicated above) Non-functional requirements, incl. ▪ Availability ▪ Data continuity ▪ Flexibility ▪ Interoperability ▪ Reliability ▪ Safety ▪ Security and privacy Trust (incl. traceability) Other requirements Available International Standards supporting the requirements (if any References (related to above standards or other useful information (e.g. on regulatory aspects))
Governing process		Data quality	Data input characteristics ▪ Data granularity ▪ Characteristics of meta data

(Activity of data governance)			Data output characteristics ▪ Data accessibility ▪ Data availability ▪ Data traceability ▪ Data quality considerations ▪ Data authenticity ▪ Data reliability ▪ Data integrity ▪ Data usability
	Process-control	Data management capabilities	▪ Access and use ▪ Administration ▪ Acquisition and collection ▪ Creation ▪ Preservation incl. protection ▪ Sharing ▪ Storage ▪ Update
		Data processing capabilities	▪ Aggregation and grouping ▪ Cleaning and filtering ▪ Classification and indexing ▪ De-identification, anonymization and pseudonymization ▪ Transfer ▪ Pre-processing and processing ▪ Analysis and analytics ▪ Reading and query ▪ Visualization
		system capabilities	▪ Functions and operations ▪ Service Level Agreements (SLAs) ▪ Performance (incl. 5Vs of Big Data) ▪ Data models and modelling ▪ Data backup, archiving and recovery ▪ Event management ▪ System resilience ▪ System sustainability
	Entire process control	Data continuity and lifecycle control	Data accountability Data isolation SLAs enforcement Risk management, incl. different concerns and dimensions and of risks (cybersecurity, privacy, safety, risks assessment, change management) Data value chain maintenance, incl. data asset management (data asset value appraisal, identification, registration and disposition) Incident management process Continuous improvement process, incl. data minimization Data distribution ▪ Technical management considerations on data distribution ▪ Data access rights and data authorization considerations according to the different stakeholders (e.g. in a smart city scenario, (1) main groups of internal employees, (2) external business partners, (3) general public)
		Data privacy and protection	Data sensitivity Data classification Data security IPR and Licensing ▪ Open data vs private data ▪ Licenses of data use and reuse
Governing object (Artifacts of data governance)		data	▪ Volume ▪ Variety ▪ Value ▪ Velocity ▪ Variation

	Architecture	▪ Communication infrastructure (incl. connectivity) ▪ Data consistency across systems involved in the use case ▪ Deployment considerations ▪ Interface requirements, incl. user interfaces and APIs ▪ Performance criteria

Table 6: Enablers for governance

_____