Searching for a Governance Model to manage and secure the data flow in organizations, as required by GDPR.

Lars Magnusson, Sarfraz Iqbal, Patrik Elm, Anita Mirijamdotter
Linnaeus University, Växjö / Kalmar Sweden

Abstract. Since the end of the 1980s, there have been several initiatives to control and manage enterprise IT environments. ITIL is one of the more successful models, COBIT another, accompanied by others as British Petroleum's OBASHI model. However, thanks to the IP protocol and Internet, since mid-2000 the world has seen a veritable data explosion, affecting IS governance, singular IS systems now integrated. Some recent predictions expect current data volumes to grow more than 10 times till 2020, with serious implications both on governance as IT security. Additionally, we see some new EU regulations, i.e., primarily the new General Data Protection Regulation (GDPR), implemented in May 2018. Something that directly affect the scope of IS governance within the European Union and for non-European entities handling EU Citizen's personal data; with substantial fines if not complying. The regulation forces anyone handling personal data to consider information strategies that include big data management, IS governance, and information security as a convoluted context, not by themselves, a governance package. This creates a need for a paradigm shift to remediate/mitigate identified limitations in today's traditional governance models. This paper discusses governance from a holistic and agile perspective, based on the overall data flow, as per the requirements of GDPR. Issues which were not envisioned when today's IS governance models were designed or not even in their latest releases.

Keywords: Agility, Data-flow, GDPR, IT Governance, Security

1. Introduction

This paper intends to discuss the consequences of modern IS governance from a practical perspective. IT governance in this paper is about the ability to plan, design and execute the target organization's need of IS/IT services to support its overall operations. Traditionally, IT governance is about managing the individual systems used. However, in todays integrated IS/IT environments, decision regarding one system can have profound effects far outside that system. Simply, IT governance[1] has changed substantially since the 1970s-90s. A transformation of both IT in general as well as associated governance processes and incurred security risks. Evolving from the pre-90s stand-alone systems to mostly organizational-wide multi-dimensional system integrations, with multiple data flows in-between. Today, nearly all systems are

[1] IT management is in this paper referred to as IS governance, since management of IT is more of the day-to-day routines, handling daily operations. Governance, in its turn, includes security.

engaged in exchanging information in various organized degrees with other in-house systems, as well as more often than not, with a range of external systems. Systems such as government agencies' data feed to general cloud services. The organization of such communications was and is often created in an ad hoc manner, without any clear strategy or security concerns, but in response to urgent business needs, not seldom un-documented [1, 2].

Yet, even in 2018, though initiated centrally, IT governance is primarily regarded as a system owner concern, not an overall organizational concern. Often manifested in widespread IT governance model mixtures, such as Information Technology Infrastructure Library (ITIL) [3] and Control Objectives for Information and related Technology (COBIT) [4]. IT governance models are supposed to describe; "how persons entrusted with the governance of an IS entity will consider it and related IT artifacts under their supervision, including monitoring, control, and direction of the entity" [5]. Traditional governance models, such as ITIL and COBIT, have had some success in handling today's IT landscape, though, as any practitioner will testify to, often with modifications [6-7]. They are not one size fit all.

Still, most larger organizations are using ITIL or COBIT as a base for their IT governance. However, being systems architecture oriented, developed at a time when information flow was less important in the organizations; from a practical perspective, the processes appear less helpful in today's agile and integrated environments. This creates some problems when handling integrated data flows. In ITIL, COBIT and most other governance models, these flows are seen as system integrated connectors. It means interfaces interconnect to other systems, defined by their APIs (Application Programming Interfaces), rather than the relation and interaction of the information flowing between the included systems. There is a need for the new ways to review information governance to move focus to the data flow, that neither ITIL nor COBIT or other models currently do. The reason for looking at the problem at this time is that the primary author has been lacking such a governance perspective and supporting management tools in his daily work as Enterprise IT Manager for the last 20 years. Together with effects of new EU regulations, activated in 2018, this situation provides motivation for a study to explore if there exists a fundamental need to adjust to this new scenario.

The key is how information (data) moves in (and out) of the organization, under our control. Today, any organization, public as private, is completely dependent on its information flows [8]. A flow behaving more like the body's blood flow. Restrict the flow and the parts no longer receiving/able to send information will wither and no longer contribute to the total. At the same time, most of the top leadership still regards IT as a pure support function [9], more of a hindrance than an asset. Few to realize that IT or rather, the information, is one of their most critical resources. In addition to this, ComputerWeekly [10] and World Economic Forum [11] estimates a steep increase of the global data volumes to 2020, between 10 to 50 times of today's volumes. Something increasing the load on any IT department. How are these to manage the expected rapid information increase?

Considering the situation mentioned above, we stand before a serious question; how can and will an IT organization handle the above-indicated issues as well as support today's frequently required business changes? Handling the steeply increasing information load, while keeping the information secure and structured? To add to the

complexity, let us go back to the EU regulations; on May 25, 2018, an upgraded EU Privacy Regulation, the General Data Protection Regulation (GDPR) was activated [12]. In order not to make the story too complex, though it has similar effects on IT governance as GDPR, we do leave the EU Network and Information Security Directive (NIS) [13] to the side for this paper. Remediating/mitigating for GDPR is very much doing the same for NIS. In short, GDPR will pose a substantial strengthening of the 1995's Data Privacy Directive [14], seriously affecting any organization operating within EU and in many cases, outside EU as well.

Our ongoing initial research [8] suggests that managing information and mitigating regulations like the GDPR, and at the same time keeping the organization safe from attacks, points to a need for a more logistical approach instead of a technical solution.

The section 2 of this paper will look at some practical aspects of governance models to present the current state of the art. In section 3 we will explain GDPR and its consequences for our context. In section 4 we conduct a smaller analysis, following with a broader discussion in section 5. We conclude the paper with section 6 mentioning further research.

2. General Data Protection Regulation in short

First, let's establish, this paper is not about GDPR [12] per se. But since GDPR will become one of the key drivers for the topic of this paper, it is not possible to continue without a short introduction to GDPR. Even if GDPR is directed towards personal data, it's principles has to be applied in a wider sense. The primary motive in doing so is that the IT organizations never know when personal data could be induced into a data set or an information stream. Applying the regulation's principal requirement on all data simplifies day to day handling. All data treated equally. As seen in recent data breach reports [28] more than 100,000 security incidents have been reported from 82 countries, which includes some very serious incidents. FBI [29], World Economic Forum (WEF)/McKinsley [30] and EU's Information Security Agency, ENISA [31], all claim that this is a rapidly increasing trend.

In 2012-13 EU started a discussion to improve the then existing personal data protection, partly due to that most member states never implemented the complete 1995 Data Privacy Directive [14]. Hence, April 27, 2016, the European Union passed the new European data protection regulation, GDPR [12], as the successor to the 1995 directive, to go active May 25, 2018. The old directive was a less useful tool for regulating the security of the EU citizens' personal data in a modern data sharing landscape, earlier lawmakers not anticipating today's more dynamic, distributed and forceful data processing landscape.

. The regulation will among other things limit the right to collect and process personal information. It also grants the data subject all rights to his/her datasets, independent of where this information has been collected and by whom [12]. The regulation forces all information collecting and processing organizations, handling European residents' personal information, to have total control over any personal information collected and processed. It also includes subcontractors. It also states a need for detailed understanding of the layout of involved information flows including

being able to establish who did what and when and under authorization of whom, and how information is transported and stored [12].

All becoming key aspects of how to manage our information. Yes, GDPR is only about personal data, but such data is everywhere in the flow. Independent of organization type, public or private, this integration is driven by the increased need for business integration. One might say, to paraphrase Avison and Malaurent [15], "Information is the king". To enforce this view, the EU has declared, if the organization fails to provide a transparent documentation according to the GDPR, including the data flows, substantial economic penalties are at stake. With information nowadays interconnected and transformed at all levels, interacting at multiple intersections all over the organization, it has already become a unified base of all operative decisions, whatever the leadership does perceive or understand. The EU has turned the table; from handling one issue at the time we need to look at all together at once. Hence, the conclusion is, we urgently need better IT governance models that are able to primarily handle the growing information flow management, to become more resilient and agiler than with current models.

GDPR aims to both restrict and simplify for the responsible Data Collector (organization collecting personal data). Thus, the data collector should be enabled to arrange and collect data in accordance with both business needs and with the new regulation. The new regulation includes clearer rules to abide by, easier to do in-EU "off-shoring" and with significant clarification of the data owners' rights. The law affects any data collector supporting organization, named Data Processor, handling European residents' personal data for the collector. One of the biggest changes involves the right of data ownership. GDPR has moved all ownership from the Data Collector to the Data Object [12]. This is one of the key element of the new regulation; all EU residents have been asserted a number of rights regarding any data describing the individual resident (data object). Additionally, a large part of personal data is labeled as very sensitive. Including medical data, data about underage residents, political and sexual preferences.

The result is that any collecting/processing entity has to have detailed data lists of the type of data and information/data flow descriptions. Data mapping has become a mandatory part of the system documentation [12]. This encompasses all systems, including any outsourced services, such as cloud services. A vital consequence is that individual departments no longer can claim they "own" the information they process, isolating them from the rest both from a GDPR, as well as an organizational perspective. A situation that will create conflicts.

So, how do "we" support an increasing adaptation to business needs, at the same time secure the data flow as well as satisfying the information security controls, now mandatory with GDPR?

We anticipate that this new regulation will profoundly affect all organizations operating within the EU, forcing how they handle this type of data. It also imposes a more rigorous operative management, enforcing the knowledge to where a set of data is, why and when, including authorized by whom. In effect, suddenly we have a legal obligation, discussing information and data flow management. No longer on a whim nor for fun. It includes penalties at 4% of the global turnover or if this being less than €20M, up to €20M, the need of finding a way to better information governance has a deadline, May 25, 2018 [12]. An academic discussion about better governance models

becoming a critical process to remediate/mitigate today's critical legal demands. A discussion this team has started.

3. Practical aspects of IT Governance Models

The basic intention has been to look at expanding traditional IT governance models, like ITIL. Trying to integrate the security need and the new EU legislation concerning information collection and privacy, all focused on the information flow. The basic theory is to simplify the governance by treating all systems as logistic black boxes, only noting the information flow, not the infrastructure. Enhancing IT governance to deal with the challenges of increasing data volumes, while complying with the new information handling regulations, such as GDPR. Operating an information flow perspective, as well as to look at more seamlessly integrating information and IT security into the fundament of the governance process.

Let's look at some of the shortcomings of traditional IT Governance Models in handling issues related to big data, data management. Since the end of the 80ies, British Standard 15000 [16] also known as ITIL [3], has guided organizations on managing their systems environment. Likewise, its competitor COBIT [4], ITIL's primary function is to build an operative management process to ease the daily operations of an IT organization. Both COBIT and ITIL are aimed at guiding management to anticipate issues that can disrupt the operations and mitigate when they occur. To differentiate between ITIL and COBIT, ITIL provides the "how", while COBIT focuses on the "why". Thus, ITIL focuses on the operational aspects where COBIT focuses on the control objectives, needed to fulfill the security and audit requirements. Both ITIL and COBIT have had a reasonable success in penetrating the organizations, giving support, sustaining today's IT strategy and processes. Most organizations are today using one of these models, though more often in modified form. The reason can be found in the ITIL "bible" [3], business changes are completely out of scope. Any change would result in a defined system change, nothing else. Reviewing the organizational environment from an information as well as a business process perspective is thus excluded. Thus, today's governance models are focused at primarily managing systems, not information. They ignore today's often dynamic data interactions, which we can see in the operational space [1, 2]. It is due to the fact that these models were developed when information flow was less important in the organizations compared to today's requirements. Their limitations are more recognized and noticeable when handling the more volatile and increased data flows we have today. Table-1 below presents a comparison of three major IT governance models.

	ITIL	**COBIT**	**OBASHI**
Description	Best practice for IT Management	Business Framework for Enterprise Governance	A framework to evaluate IT from a business perspective
Topic Focus	Main focus on internal IT processes	Main focus on IT governance and compliance	Main focus is how IT resources add to the overall results

Target Audience	Internal IT operation staff	IT audit and compliance personnel	Business personnel, to understand IT's tribute to their business area
Function	Defining internal IT service processes	Defining audit and compliance requirement for IT	To manage the data-flow between business assets

Table 1. Comparison of three IT governance models

In ITIL such flows are illustrated by connectors that link two or more entities together, e.g., interfaces that interconnect different systems and defined by their application programming interfaces (APIs). Which is not enough with keeping the flows organized and under control, which GDPR's Article 35 exclusively requires if personal data is transported. COBIT is a bit better with respect to including data flows [17, 18], but still, the model focuses on the "why" issue, not the operational/governance aspects of data flow management. There are, however, market indications pointing at new self-analyzing tools being developed [19], mainly driven by Internet of Things (IoT). These can be characterized as data discovery tools, but, by now, they have not made any significant impact on everyday data management. These tools have so far only been influential in specific areas related to IoT, something expected to change. Besides, IoT is singled out as one of the key drivers of the expected data explosion during the coming 4-5 years [10, 20]. OBASHI [21] is one governance model that may have benefits in handling the issues at hand. Early in the 2000s, British Petroleum commissioned a business data flow oriented governance model (OBASHI) to support business changes as well as to visualize and explain how IT did support business [21]. But, currently, while being a business process oriented solution, OBASHI still seems to end up in complex technology-like solutions, not the logistical view we are seeking.

Additionally, we see a shift in the evaluation of the daily IT operations of today's organizations. IT, previously mostly looked upon as solely a support tool, easy to outsource, now seem to increasingly be regarded as a critical organizational resource. Maybe because today's extensive integration gives the effect that even small, local IT disturbances could have companywide effects, far outside the failing system's management borders. If proper risk analysis had been performed, revealing the total involvement/data interaction, the failing organization might have been able to take more pro-active, pre-mitigating actions. But, as most information security postmortems show, such analysis is seldom done. Based on public failings like Equifax [22], Deloitte [23] and Target [24], IT governance need to be redefined, moving IT from being a simple support function, to be the vehicle to manage the organizational information.

One key problem might be the lack of the IT organization's ability to (in a pedagogical way) visualize how IT or rather information, has become that critical resource. To show the leadership, how much they depend on the information flow, a very simple analog could be the previously mentioned blood circulation of the body. Both flows are vital for the sustainability of their respective "entity". However, from an operational perspective, an information flow has much shorter lifespan than the bloodstream. Often for only 2-3 years before leadership or market demands or introduce new operational models. Operational changes that directly affect the information flows. Thus, when new systems are introduced and/or new external service vendors (like cloud

services) added [25,26], or new governmental requirements are put into effect, we find that we often need to redesign the existing data flow(s).

ITIL and COBIT do not quite support such redesigns of data flows; they function (and have their strength) as system controls, requiring more strict and stable definitions to satisfy their inherent processes. The authors have recognized these limitations within traditional IT governance models and claim that contemporary data flow management, and thus, contemporary IT governance models, need to become agiler. Therefore, we propose to explore how to add agility to the management processes of the IT governance model. The intention is to look further into ITIL, since ITIL is more spread, has far more certified users, and is also more modified than other governance models. As mentioned in the Introduction, due to the implementation of GDPR [12] and NIS [13] in May 2018, there is a need to take an active stance in regard of data flow governance/management. Not only from an operational or management perspective but to a higher degree due to regulatory and information security perspectives. As mentioned earlier, these new regulations tie everything together in ways not seen before in modern IT. Therefore, we cannot ignore the regulation's influence on how to govern information. The regulations represent the primary motive to search for new governance models/solutions. However, in this paper, we concentrate on GDPR. Note that its expected effects are not something new, the effects of the US Sarbanes Oxley Financial Act of 2002 [27] were very similar, driving understanding of governance, data, and security.

4. Review of the situation – from an Automotive case

Following, we will review the implications, primarily of GDPR on state-of-the-art governance models (see section 2) to later find better management solutions. To deal with the future intertwined challenges of regulations and managing increasing volumes of data and information flows. A situation posing a major challenge to global IT, not only for Europe. The issues are not new, they are well-known and thus the driver for EU to strengthen the older directive [12]. As IT professionals we need to think differently. Today's operational processes and models do not give us the tools to fulfill future demands nor GDPR's requirements. Neither do our security processes. As we tried to point out in this paper, we urgently need to drive the development towards new solutions, like British Standards did with BS15000 [16] in the late 1980s. The IT organizations need to know their data flows far better than what they do today. The US government Sarbanes Oxley Financial Act of 2001 (SOX) [27] created a similar precedence when it came, forcing companies to do far-reaching adjustments. SOX handles financial data similar to how GDPR handles personal data.

In 2007, the primary author was the responsible security architect, mitigating a SOX deficiency at his then employer (Saab Automobile/GM), to block all ftp communications [1,2]. The night when the ftp ability was closed, thousands of connections were registered. This, though the team had worked with system owners all over GM for six months to move away from ftp.

Many of the connections were undocumented but valid data connections, yet, some 1300 were found to be orphans. Connections easy for a scanning hacker to use since

login information for ftp go as clear texts. They only need to scan for a couple of hours to get a trove of critical passwords. Now it is 2018 and the same author have recently, in his final position as Enterprise Security Architect, early 2018, been discussing GDPR consequences with customers, still depending on ftp. When asking the customer managers, these admitted a lot of connections to be undocumented. In 10 years, nothing has changed. However, ftp is not the only risk, we have a lot of unsecured http. From both a GDPR as Information Security perspective, we all are sitting on a live bomb, waiting to go off. As seen by the examples of Target, Equifax, and Deloitte [22-24] there are other risks threatening the organization, like the steep penalties under GDPR. Earlier noted, we also see large increases in the data flow volumes, IoT working its way in.

Managing large data repositories has earlier been proven both costly and with the risk of storing the wrong data [32]. Alongside expected data volumes, the GDPR included provisions for collectors to expediently correcting erroneous data. Once again, with costly penalties, if not doing so. As seen from the example of Saab and the responses from the IT manager discussions, organizations that have working governance processes still have wide holes. Holes that poses grave risks and must be mitigated in the coming 2-4 years. Some organizations might have an unpleasant wake-up call after May 25, 2018, if EU sends GDPR auditors visiting them. The authors have identified a need to go forward, improving experienced limitations in the current operative IT environment; limitations visible in any security audit review.

5. Discussion and further research

The traditional IT governance models have tried to support business changes, updating of existing systems, system replacements, support of users and access control, authorizations', and regular information/IT security actions. But as seen in most, if not all audits [33, 34], we see critical shortcomings in our IT environments. Simultaneously, IT departments invest more in urgent repairs of old systems than planning for adapting to the future situation. According to a 2016 survey [35], 70-80% of all IT costs can be referred to the organization's legacy systems; to keep broken systems running. Every new API or function that is added to an existing system, increases the management effort. Hence, "we" have created a management nightmare. To this end, as mentioned in the previous section, we now have a far more aggressive security landscape, where most of the current measures are not sufficient enough from a protection point of view. The well-known security researcher Gene Spafford [36] and former British Telecom's Security Evangelist, Bruce Schneier, has many times issued serious warnings on our current cybersecurity vulnerability. Schneier [37] is particularly vocal about cyber-attacks being attacks on our everyday existence. We need to improve our security strategies. From this aspect, it is hard to see that current governance models will help [38, 39], due to their static nature. Therefore, we propose the need for more agile data flow management. To primarily manage data, not the systems. And how will that look like?

Currently, we do not know all the answers, it is a work in progress. But one option is to make a simple model, taking ideas from ITIL, and maybe COBIT and OBASHI.

Describing data, we get in through existing processing or created “first line” internally. An order for a product, manufacturing/design data and similar, any starting point where data first appear in our particular “data sphere”. We need to isolate the starting points from any re-processing done in our data sphere, first being primary data sources. The rest is secondary data sources or the end result, being what’s leaving the data sphere. One problem is that outsourcing, or cloud services make data go out, looking like end results, but here we need to be cautious, since that data can enter again as processed data, i.e., as secondary data. By isolating data this way, we can handle business changes, because these normally create a clean change in the flow patterns. Like a new subway line affecting the existing traffic flow in other existing lines.

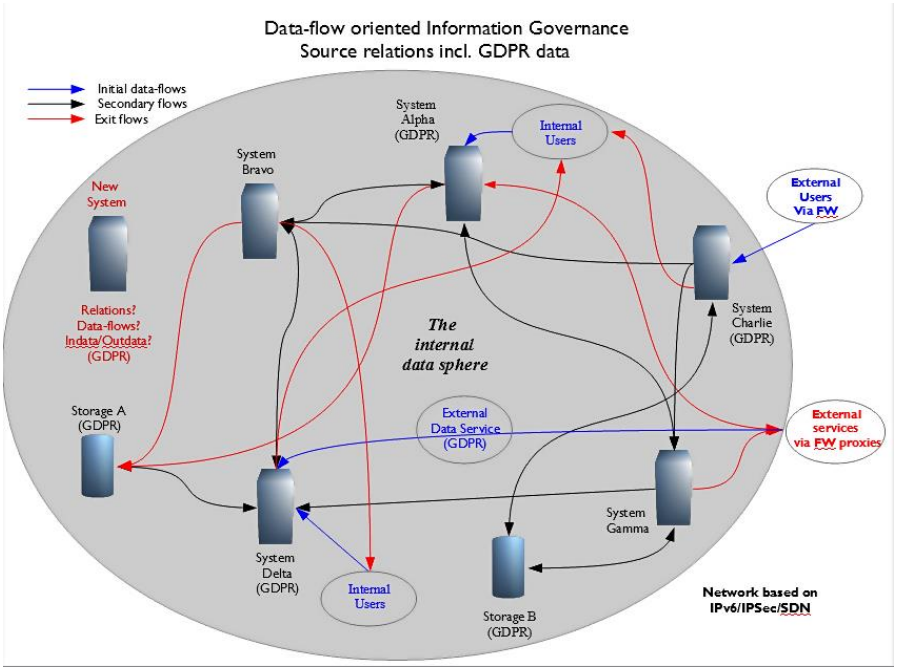

Fig 1. Complexity of the data flow

Figure-1 represents the complexity of the data-flow – where to connect the new system. GDPR forces an understanding and exact view of how data relates and is managed, both internally and externally. We need a clear view of the involved data sphere. The issue of ITIL, the change mechanisms exist and are mostly correctly documented but lacks documentation structures to describe the intended data flows. Earlier, redesigning existing systems was often the only economically viable way. However, today we have the possibility of using business process analytics and messaging systems to better control the flow patterns. Tools capable of running small purpose-built applets, altering the information content within the flow. A design, anyone being a Unix/Linux system administrator (sysadmin) is familiar with; the Unix software tools, awk, sed, grep, sort, uniq, perl and hundreds of other commands,

possible to join as shell-scripts [40] solving new information processing needs. But today uses tools as Java, Python etc. As a matter of fact, most of today's messaging platforms can run Java, Javascript, Python, php, Erlang and other applets, taking a data flow or three, re-modeling data to what the receiver wants, without changing any of the large legacy systems. Although we need to keep track on what "we" are doing, with what, where and why, because if that flow includes personal data, GDPR demands "us" to document both the flow and the "applications".

The organization becomes more agile and resilient while working with smaller changes and smaller applications which makes it easier to analyze the effect of a change. Particularly, if using a central messaging hub. Servers and containers, not having user interfaces are locked to talk only to the hub, which has its interfaces hardened against anything listed in OWASP Top 10 [41] and SANS top 25 Vulnerabilities [42] as well as following the old network security maxim, "Deny all, Allow needed". Even if a messaging hub is not used, drawing that network map will identify multiple, parallel communications [2], sometimes possible to integrate as a single data flow. Limiting the attack profile, making the environment more resilient. This way we also have up-to-date documentation, seeing when services are no longer needed and can be removed, another often overlooked risk mitigation. As illustrated in section 3, data security controls need to be in place and data flows need to be documented. Failure to meet these demands and eventually resulting data losses have severe consequences (mentioned earlier regarding GDPR penalties). Therefore, we need to be proactive in improving our data management to fulfill GDPR's requirements and to monitor where data is located, who has access and how it is protected. Using the above-described data sphere analog could be a possible solution, but we still lack a working nomenclature.

A lot of requirements mentioned here already exist in both ITIL and COBIT, but lacking explicit focus on both data flow as well as information security. Issues that can be resolved with support by PCI-DSS [43] and Sarbanes-Oxley Act (SOX) [27] regulatory frameworks. Both frameworks include lots of examples of how to implement processes and practices to secure data, including needed protective control objectives. Though neither of them is about personal data management as per GDPR [12], their practical remediation is still directly applicable on GDPR objects. Several US advisories have in 2016-17 recommended US organizations working in Europe to take out their SOX playbooks, as a support to remediate their GDPR issues [44-46]. A substantial change that the implementation of GDPR includes is the basics of processing personal data.

Beside the key condition that the organization collecting the data no longer is the owner of that data with regards to European residents, it is these data objects that own all data describing him or her. The condition is valid even if collected by US, Chinese or Russian authorities. Albeit, in such cases, being foreign states, EU has no control, but EU legislation still gives EU residents an unambiguous ownership and the right to give/revoke any approval of data processing. Therefore, this regulation also affects non-EU states and companies collecting European private and personal data. However, when looking at the full GDPR picture, as previously stated we see a convenient motive in having a holistic approach to both governance, data management, and information security.

We propose a way forward, by defining a process that addresses and solves the agility issues related to dynamic data flow changes including tools to manage these better. The suggestion we propose is in its infancy, but allow for defining the IT systems out of their data needs and flows, not based on system needs and their interaction interfaces. Anyone active in data analytics will recognize this from the discussion of Big Data architecture [32]. However, our intention is not to plainly do data management and architecture, but securely manage systems' relations based on the included data flows. Such an IT governance model would be based on a new paradigm, that frees us from the current individual systems architecture perspectives, leading to no or very little control of the data flowing in-between systems. Through GDPR's data mapping requirement and penalty structure, we experience an additional driver for finding such new approach, allowing for a more agile data-oriented governance model. We are not yet there, we are still in the interim, defining the questions needed to be defined, reviewing the underlying science theories, in order to see if there is a possible solution in managing information systems this way. Additionally, it is included to see if this approach can improve system governance or if it is to be of similar effectiveness as our current governance models.

6 Conclusion

This paper focuses partly on the effect of the GDPR and partly on IT Governance Models, to reorient information governance to align to data flows rather to systems' interfaces interaction. Our argument for this standpoint throughout the paper is that GDPR has created a game changer, how we govern our IS environment. We are convinced that a new, more agile enterprise IT Governance model is needed. For, with the current rapidly changing information landscape, something needs to be done. The issues pointed out through GDPR includes increasing data volumes, the need to move towards a data-centric approach to handle this increase, as well as making the data flow independent of the involved systems, being secure. Thus, to find ways, how the GDPR's demands on data integrity and security can be fulfilled. Additionally, it also includes that how involved data collectors and data processors must align with GDPR's unique demand of "*Security by demand and default*".

References

1. Magnusson, L., "FTPshell issues", Internal problem analysis, Saab Automobile IS&S, March 19, 2010, Saab Automobile AB, Trollhättan Sweden.
2. Anulf, B., "Orphan connections discovered at activation of Saab FTPshell router fence", Personal Interview, Feb 24, 2018.
3. Axelos, "What is ITIL", Axelos Inc, London, UK, as viewed, Oct 9, 2017: https://www.axelos.com/best-practice-solutions/itil/what-is-itil
4. ISACA, "What is COBIT 5?", ISACA, IL, US, as viewed Oct 9, 2017: http://www.isaca.org/COBIT/pages/default.aspx

5. IT Governance Institute, 2003. Board Briefing on IT Governance, 2nd Edition, as viewed Oct 5, 2017: https://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf
6. Johnson, B., 2012, "How Many ITIL Experts Do You Need to Change a Light Bulb?", HDI institute, US, as viewed May 29, 2018: https://www.thinkhdi.com/library/supportworld/2012/itil-experts.aspx
7. Florentine, S., 2016, "7 questions to ask before implementing ITIL", CIO magazine, IDG.com, US, as viewed May 29, 2018: https://www.cio.com/paper/3040629/libraries-frameworks/7-questions-to-ask-before-implementing-itil.html
8. Magnusson, L, Elm, P, Mirijamsdotter, A, Towards Secure Data Flow Oriented Multi-Vendor IT Governance Model, UBT/Springer, (In Print).
9. Durbin, S., (2015), "The CFO's Role in Cyber Security", CFO.com, March 31, 2015, as viewed March 15, 2018; http://ww2.cfo.com/accounting-tax/2015/03/cfos-role-cyber-security
10. Adshead, A, Data set to grow 10-fold by 2020 as internet of things takes off, Computer Weekly, Apr 9, 2014, as viewed Nov 28, 2017: http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off
11. Breene, K, What is the future of the internet?, World Economic Forum, Jan 17, 2018, as viewed Nov 28, 2017: https://www.weforum.org/agenda/2016/01/what-is-the-future-of-the-internet/
12. 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, Bruxelles, May 10, 2016.
13. Directive (EU) of the European Parliament and Council, regarding security of networks and information systems (the NIS Directive) adopted by the European Parliament on 6 July 2016, Bruxelles as viewed Oct 9, 2017: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
14. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**,** Bruxelles, Oct 24, 1995.
15. Avison, D., Malaurent, J., "Is theory king", Journal of Information Technology (2014) 29: 327
16. British Standard, "BS 15000", bs15000 org, as viewed Oct 12, 2017: http://www.bs15000.org.uk/bs15000.htm
17. Suer, M., Nolan, R., "Using COBIT 5 to Deliver Information and Data Governance", Jan 12, 2015, COBIT Focus, ISACA, IL, US
18. Suer, M., McMonagle, L., "Extending COBIT 5 Data Security and Governance Guidance", Jan 30, 2015, COBIT Focus, ISACA, IL, US
19. Kavanagh, E., "What is Data Flow and Why Should You Care", Feb 24, 2014, InsideAnalysis.com, Bloor Group, TX, US, as viewed Oct 9, 2017: https://insideanalysis.com/2014/02/what-is-data-flow-and-why-should-you-care/
20. Pharris, C., "The IoT Data Explosion, IPv6, And The Need To Process At The Edge", Digitalist Magazine, SAP, Sept 20, 2017, as viewed Feb 23, 2018:

http://www.digitalistmag.com/cio-knowledge/2017/09/20/iot-data-explosion-ipv6-need-to-process-at-edge-05350752

21. Seow, S, OBASHI White Paper, APMG-International, High Wycombe, UK, 2011
22. Riley, C., Pagliery, J., March 19, 2015, “Target will pay hack victims $10 million”, CNN Money, as viewed Feb 4, 2016; http://money.cnn.com/2015/03/19/technology/security/target-data-hacksettlement/
23. Gressin, S., “The Equifax Data Breach: What to Do”, US Federal Trade Commission, as viewed Oct 1, 2017; https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
24. Reuters staff, “Deloitte cyber-attack affected up to 350 clients”, Reuters, London, UK, as viewed Oct 11, 2017, https://www.reuters.com/paper/us-deloitte-cyber/deloitte-cyber-attack-affected-up-to-350-clients-guardian-idUSKBN1CF29M
25. De Jong, M, van Dijk, M, Disrupting beliefs: A new approach to business-model innovation, McKinsey Quarterly, July 2015, as viewed Nov 28, 2017: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/disrupting-beliefs-a-new-approach-to-business-model-innovation
26. White, R, Business models: a little more fluid than Newton’s laws of physics, Medium, as viewed Nov 28, 2017: https://medium.com/@RachelCFO/business-models-a-little-more-fluid-than-newtons-laws-of-physics-e8f023fb1538
27. 107th United States Congress, Pub.L. 107–204, 116 Stat. 745, The Sarbanes Oxley Financial Act.
28. Report, “Verizon 2016 Data Breach Investigations Report”, Verizon LLC, NY,US, as viewed Sept 10, 2017: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
29. Federal Bureau of Investigation, “Internet Crime Complaint Center (FBI)”, 2014 Internet Crime Report, 2015, FBI, Washington, US
30. World Economic Forum/McKinsey & Company (WEF), Jan 2014, “Risk and Responsibility in a Hyperconnected World”, Geneva, CH
31. Marinos, L., Sfakianakis, A., ”ENISA Threat Landscape”, Sept 28, 2012, ENISA, Crete, Greece
32. Goetz, M., Leganza, G., Peyret, H., Hoberman, E., "Customer Ecosystems Demand Outcome-Oriented Data Governance Processes: The Data Management Playbook", Forrester, Dec 28, 2017
33. Robinson, K., 2017, "The six most common audit failures", Blog, F5.com, US as viewed May 29, 2018; https://www.f5.com/labs/papers/cisotociso/the-six-most-common-audit-failures
34. Deloitte, 2018, “Leading Lights, 2018 Hot topics for IT internal Audit in Financial Services, London, UK.
35. McLelland, C., “IT budgets 2016: Surveys, software and services”, Oct 2015, ZDNet.com, as viewed Oct 12, 2017: http://www.zdnet.com/topic/it-budgets-2016-a-cios-guide/
36. Spafford, E.H., 111th Congress, "Cyber Security: Assessing Our Vulnerability and Developing an Effective Defence", 111th Congress, US Senate Committee on Commerce, Science and Transportation, Mar 19, 2009.

37. Schneier, B., “Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection", Subcommittee on Digital Commerce and Consumer Protection, Committee on Energy and Commerce, United States House of Representatives, Nov 1, 2017,
38. Bloomberg, J., 2015, "DevOps And ITIL: Friends Or Enemies?", Forbes, US, as viewed June 4, 2018; https://www.forbes.com/sites/jasonbloomberg/2015/11/13/devops-and-itil-friends-or-enemies
39. Daine, G., 2018, "ITIL® Vs. DevOps! 25 Influential Experts Share Their Insights (Is ITIL® Agile Enough?)", Purplegriffon.com, as viewed June 4, 2018; https://purplegriffon.com/blog/is-itil-agile-enough
40. Robbins, A., Beebe, N., “Classic Shell Scripting”, O’Reilly Media, Dec 2008.
41. OWASP.org, “OWASP Top 10 Vulnerabilities”, OWASP.org, Dec 29, 2017, as viewed Jan 9, 2018; https://www.owasp.org/index.php/Top_10-2017_Top_10
42. SANS Institute, “CWE/SANS TOP 25 Most Dangerous Software Errors”, SANS.org, June 27, 2011, as viewed Jan 9, 2011; https://www.sans.org/top25-software-errors
43. PCI-DSS Standard, 2005, PCI Security Standards Council, Wakefield, MA, US, https://www.pcisecuritystandards.org
44. Pugnet, J., "Is GDPR the new SOX?", Digitalist Magazine, SAP, Aug 21, 2017, as viewed Feb 23, 2018: http://www.digitalistmag.com/finance/2017/08/21/is-gdpr-new-sox-05283449
45. Yuwono, E., "Next Generation of Privacy in Europe and the Impact on Information Security: Complying with the GDPR", SANS Institute InfoSec Reading Room, The SANS Institute, December 2nd, 2016, as viewed Feb 23, 2018: https://www.sans.org/reading-room/whitepapers/legal/generation-privacy-europe-impact-information-security-complying-gdpr-37457
46. Zanni, J., "Understanding GDPR Through the Lens of Sarbannes-Oxley (SOX)", Acronis Blog, Dec 21, 2017, as viewed Feb 23, 2018: https://www.acronis.com/en-us/blog/posts/understanding-gdpr-through-lens-sarbannes-oxley-sox