Towards Secure Data Flow Oriented Multi-Vendor ICT Governance Model

Lars Magnusson
Linnaeus University, lars.mson@gmail.com

Patrik Elm
Linnaeus University, patrik.elm@lnu.se

Anita Mirijamdotter
Linnaeus University, anita.mirijamdotter@lnu.se

Towards Secure Data Flow Oriented Multi-Vendor IT Governance Models

Lars Magnusson[1,2], Patrik Elm[2], Anita Mirijamdotter[2]

[1] Tieto Public, Sweden, [2] Linnaeus University, Kalmar Sweden

Abstract. Since the beginning of this century, we have seen radical changes in the depth and breadth of IT functions. Today's contextualization of IT includes a totally integrated environment, where the norm is everything connected to everything. Such changes have implications both from a management perspective as well as from a security perspective. An additional issue, for those responsible for managing and operating the IT landscape, is the new European Union regulations Network and Information Security (NIS) and General Data Protection Regulation (GDPR) which will be implemented on May 10 and May 25 respectively, 2018. These two regulatory actions will forever change IT governance within the European Union. This paper explores the anticipated paradigm shift in IT management.

Keywords: IT Governance, Data-Flow, GDPR, Agility

1 Introduction

The last two decades have represented a radical transformation of both information technology (IT) in general as well as its management issues and security risks. IT has evolved from pre-90's stand-alone systems to complete integrated systems. Many organizational systems exchange information with other in-house systems as well as with a multitude of external systems, such as government agencies, over cloud services. However, the communication processes have often been created in an ad hoc manner, without consideration of overall strategy or associated security.

Typically today, IT Governance is being regarded as a departmental concern, not an organizational strategy, whether expressed in ITIL, Information Technology Infrastructure Library [1], or COBIT, Control Objectives for Information and related Technology [2] Governance Models. Although IT Governance models are supposed to "describe how those persons entrusted with Governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity" [3], in practice, the first author with more than two decades of practical experience in the area, often has found that the descriptions are not fully translated to corresponding actions and operations.

Still, traditional Governance models, such as ITIL and COBIT, have had some success in handling today's IT landscape; most organizations use one or the other. However, these approaches are primarily systems architecture oriented, developed when data flow was less important in the organizations than today. Therefore, a reviewer often can see limitations in handling data flows. In ITIL, such flows are described as system connectors, i.e., interfaces that interconnect to other systems, defined by their APIs (Application Programming Interfaces), rather than the relation and interaction of the data flows between and among systems.

In addition to this, on May 25, 2018, an upgraded EU Privacy Regulation, the General Data Protection Regulation (GDPR) will be activated [4]. This upgraded privacy regulation includes a substantial strengthening of 1995's data privacy regulations [5], which will profoundly affect any organization operating within the EU. This regulation will, among other things, limit the right to collect and process personal data. It will give the data subject all rights to his/her data sets, independent of where this data has been collected and by whom. Such regulation forces data collecting and processing organizations to have total audit control over any personal data collected and processed. This includes possessing detailed understanding of data flows, who did what and when and under whose authorization, and how data is transported and stored. Maps of data/information flows will be a mandatory part of the system documentation, which must encompass all systems, including outsourced cloud services.

Since mid-2000, there has been a global trend of inter-organizational data integration, independent of type of organizations, public or private. Hence, individual departments in an organization no longer can claim they "own" the data they collect, they need to see that data as part of a bigger picture. If the above integration of some reason ceases to exist or fails, the result can be a direct threat to the survival of the whole organization, due to lack of data where it is needed. Further, interacting at multiple intersections throughout the organization creates a need of a unified base for operative decisions, an IT Governance model is required for handling data flow management. Additionally, if an organization fails to provide transparent documentation of such existing integration; according to the GDPR, substantial economic consequences would result, with penalties up to €20M. Adjusting to the GDPR will likely require costly and time-consuming IT development efforts.

In Section 2, we expand on traditional IT Governance Models, followed by section 3, presenting the new EU legislation, concerning data collection and privacy. In section 4 we will discuss some of the shortcomings of traditional IT Governance Models to handle the consequences of the new legislation and close with some concluding observations.

2 Traditional IT Governance Models

Since the end of the 80's, British Standard 15000 [6], also known as ITIL [1], has guided organizations on managing their systems environment. Like its competitor COBIT [3], ITIL's primary function is to build a 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. To differentiate between ITIL and COBIT, ITIL provides the "how", while COBIT focuses on the "why". Thus, ITIL focuses on the operational aspects while COBIT focuses on the control objectives needed to fulfill the security and audits requirements.

Both ITIL and COBIT have had some success in sustaining today's IT strategy and processes and most organizations are using one or the other. However, both Governance models are primarily oriented to managing systems, ignoring their data interactions. Further, the systems are managed according to the same processes independent of the characteristics of each system. These models were developed when data flow was less important in the organizations compared to today and we now recognize issues, noticeable when handling the data flows. In ITIL, such flows illustrate connectors that link two or more things together, e.g., interfaces that interconnect different systems as defined by their application programming interfaces (APIs).

COBIT is a bit better in regard to including data flows [7, 8], but still, the model focuses on the "why" issue, not the operational aspects of data flow management. There are, however, indications that new tools are being developed, driven by the Internet of Things (IoT)[9]. These can be characterized as data discovery tools, but, to date, they have not made any significant impact on everyday data management. They have only been influential in specific areas related to IoT. Further, we see a shift in the daily operations of today's organizations. IT, previously looked upon as solely a support tool, easy to outsource, is now increasingly regarded as a critical resource, essential to sustainability of any type of organizations. As a recent example, a Scandinavian IT vendor shut down a Norwegian bank and the Swedish National Train operator (SJ) due to technical issues [10]. Hence, small disturbances have wide effects.

As argued in the above, IT Governance management should redefine IT, from the old support label to being renamed as a critical resource. To give an analog, let's look at the blood circulation of the body. Contemporary IT have similar effects on the organization, as the blood does in the body. The blood transports oxygen to different parts and removes by-products for disposal. This can be similarly attributed to data flows to and from different parts of the system mass. Both flows are vital for the sustainability of the organization and the body, respectively. A difference though; the blood flow has had some 600 million years to develop. Also, the context in which the blood circulation operates does not change. In contrast, an operational IT strategy has a much shorter lifespan, 2-3 years, before leadership or market demands introduction of new operational models. Such operational changes directly affect the data flows. Thus, when new systems are introduced, and new external service vendors (like cloud services), or governmental requirements are put in effect [4, 5], we find that we need to redesign the data flow(s). ITIL and COBIT do not quite support such redesigns; they function (and have their strength) as static control systems that require more strict and stable definitions to satisfy their inherent processes. The inherent limitations in traditional IT Governance models for contemporary data flow management, and thus, contemporary IT Governance models, need to be more agile. Therefore, we propose research on how to add such agility to the management processes of the IT Governance models. The intention is to look further into ITIL, since ITIL is wider spread, has far more certified users, and is also more modified than other Governance methods.

As mentioned in the Introduction, due to the upcoming implementation of the EU GDPR [4] and Network and Information Security (NIS) regulation [11] in May 2018, we need to take an active stance in regard to data flow management, both from an operational or management perspective, and from an information security perspective. The GDPR and its consequences are discussed next.

3 General Data Protection Regulation in short

As seen in recent data breach reports [12], more than 100,000 security incidents have been reported from 82 countries, some very serious – i.e., the breaches in the United States firm Target [13], credit evaluator Equifax [14] and audit firm Deloitte [15]. Federal Bureau of Investigation (FBI) [16] and World Economic Forum (WEF)/McKinsley [17], as well as the EU IT Security organization ENISA [18], claim that this is an increasing trend.

So, in 2012-13, the EU started a discussion to improve the then existing personal data protection, in part because most member states never implemented the 1995 Privacy Data Directive [5] completely. Hence, on April 27, 2016, the European Union passed the new European data protection regulation, GDPR [4], as the successor to the 1995 directive. The old directive was a less useful tool for regulating the security of the EU citizens' personal data in a modern data sharing landscape, because earlier lawmakers not anticipating today's more dynamic and forceful data processing landscape.

GDPR aims to both restrict and simplify the responsible Data Collector (organization collecting personal data). Thus, such organizations would be enabled to arrange and collect data needed in accordance with both business needs and with the new regulation [5]. The new regulation includes clearer compliance rules, easier to observe in EU "off-shoring", including clarification of the data owners' rights. The law also affects any Data Collector supporting organization, as well as any Data Processor.

One of the biggest changes involves the right of data ownership. GDPR has moved the ownership from the Data Collector to the Data Object. This is the key element of the new regulation; all EU residents have been assigned a number of rights regarding any data describing the individual data object, including:

a. The described individual is the sole owner of any data describing him or her.
b. Where in the world such data collections are performed is insignificant.
c. The data owner has the right to request his/her data to be audited, destroyed or moved entirely to any competing IT services in some defined areas like military, law enforcement and/or healthcare information. (National exemptions may exist.)
d. Data regarding residents younger than 16 years of age are viewed as extra sensitive.
e. Data regarding legal or healthcare information, sexual orientation and ethnicity are equally sensitive.
f. The data collector needs to have an undeniably free, unbiased and clear consent – in some cases a non-reputable approval from the data owner – to process his/her data.
g. A Data Processor involved in helping a Data Collector is equally responsible for following GDPR.
h. Data Collector must have exact knowledge of what data collected, where it is stored and how it is moved. To include a data-flow map, also including any Data Processors.
i. Both the Data Collector and Processor need to have data securing controls in place, so that data stored and/or processed will not be lost.

j. Lost data have to be reported within 72 hours to the national overseer in the member state where the loss occurred. The regulation also includes the requirement to notify the data owners.
k. If data loss take place, and responsible people fail to notify the overseer within the allotted time, both these conditions can induce EU fines up to €20M.

Thus, the new EU regulation that will come into effect on May, 25, 2018 includes a substantial strengthening of the individual privacy and rights concerning data collection. We anticipate that this new regulation will profoundly affect organizations operating within the EU.

4 Discussion

The traditional IT Governance model should support business changes, updating of existing systems, system replacements, support of users and access control, authorizations, and regular information/IT security actions. Simultaneously, IT departments invest more in urgent repairs than to plan for adopting to the future situations. According to a 2016 survey [20], 70-80% of all IT costs can be referred to the organization's legacy systems, to keep things running. Every new API or function that is added to an existing system increases the management effort. Hence, with time the IT organization creates a management mess.

To this, as mentioned in the previous section, the organization have a far more aggressive security landscape, where most measures are not sufficient enough from a protection point of view. The well-known security researcher Gene Spafford [21] has issued serious warnings on our cyber security vulnerability. Thus, they need to improve their security thinking. In this aspect, it is hard to see that current Governance models will help, due to their static nature. Therefore, in our research, we propose a need for more agile data flow management.

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 result in data loss have severe consequences. Therefore, the IT organization need to be proactive in improving its data management to fulfill GDPR's data mapping requirements and monitor where data is, who has access and how it is protected.

Requirements already exist in both ITIL and COBIT, but these lack explicit focus on information security as well as monitoring the data flow that is to be mapped and protected. Issues that can be resolved with support by PCI-DSS [22] and Sarbanes-Oxley Act (SOX) [23]. Both include lots of examples on how to follow processes and practices to secure data, such as protective control objectives. However, neither of them are about personal data management, which is the focus of GDPR. Still, several US advisors has 2016-17 recommended any US organizations working in Europe to take out their SOX playbooks, to support any remediation of their GDPR issues.

Implementing GDPR requires a substantial change in processing personal data. The organization collecting the data is no longer the owner of such data. In regards of individuals with residence in Europe and being the "data object", these individuals owns any data describing him or her, even if collected by Chinese, US or Russian intelligence communities. In such cases, because these are foreign states, EU residents have no control. But the EU legislation gives individual residents an unambiguous ownership to any data describing him or her and thus the right to give any approval of pending processing. Therefore, this regulation will affect foreign states and companies collecting private and personal data about EU residents outside the EU.

A way forward, is to define a mapping process that addresses and solves the agility issues related to dynamic data flows. One that also include information security as an integral aspect of the process. The suggestions we propose is to develop IT Governance models that allow for such refocusing on data needs and flows, not on system needs and their interaction interfaces, integrating security in the governance. Such an IT Governance model would be based on a new paradigm that frees us from the individual systems architecture perspective, leading to no or very little control of data flowing in-between systems or its security.

5 Conclusion

Though GDPR goes active first at May 25, 2018, and some of its effects still is up for debate and interpretation, GDPR has given enterprise architects a financially strong motive to re-implement the overall system architecture and to move toward the data-driven design criteria that the GDPR mapping requirement encourages, which includes securing both systems and data. Simultaneously, IT organizations do need new tools, preferably working in consistency with existing IT Governance models like ITIL or COBIT in order to not to do too abrupt breaks with existing systems management approaches.

In conclusion, we argue that in a long term perspective a new IT Governance Model is required, characterized by being data centric and by managing the data flows independent of the involved systems. This is a needed approach to meet the GDPR demands on managing any data collection and Collectors, and any data processing and Processors. With GDPR's data mapping requirement, we also see an additional driver for finding an approach that allows for a more agile data oriented Governance model. Such a model, we argue, is requested in most organizations if they are to meet modern digitalization requirements.

This research is in its initial phase, with the first task to define and discuss the problem area. Next, empirical investigations will be reported to analyze and discuss the awareness of practice and how organizations will deal with the changes we anticipate will emerge by the GDPR implementation.

References

1. Axelos, "What is ITIL", Axelos Inc, London, UK, as viewed, Oct 9, 2017: https://www.axelos.com/best-practice-solutions/itil/what-is-itil
2. ISACA, "What is COBIT 5?", ISACA, IL, US, as viewed Oct 9, 2017: http://www.isaca.org/cobit/pages/default.aspx

3. 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
4. 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.
5. 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.
6. British Standard, "BS 15000", bs15000 org, as viewed Oct 12, 2017: http://www.bs15000.org.uk/bs15000.htm
7. Suer, M., Nolan, R., "Using COBIT 5 to Deliver Information and Data Governance", Jan 12, 2015, COBIT Focus, ISACA, IL, US
8. Suer, M., McMonagle, L., "Extending COBIT 5 Data Security and Governance Guidance", Jan 30, 2015, COBIT Focus, ISACA, IL, US
9. 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/
10. IDG.se, "IT-haveri hos Every", Computer Sweden, IDG, Stockholm, Sw, as viewed Oct 9, 2017: https://computersweden.idg.se/2.2683/1.690181/every-haveri-sj-nere
11. 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:

a. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

12. 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
13. 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/
14. 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
15. Reuters staff, “Deloitte cyber-attack affected up to 350 clients”, Reuters, London, UK, as viewed Oct 11, 2017, https://www.reuters.com/article/us-deloitte-cyber/deloitte-cyber-attack-affected-up-to-350-clients-guardian-idUSKBN1CF29M
16. Federal Bureau of Investigation, “Internet Crime Complaint Center (FBI)”, 2014 Internet Crime Report, 2015, FBI, Washington, US
17. World Economic Forum/McKinsey & Company (WEF), Jan 2014, “Risk and Responsibility in a Hyperconnected World”, Geneva, CH
18. Marinos, L., Sfakianakis, A., ”ENISA Threat Landscape”, Sept 28, 2012, ENISA, Crete, Greece
19. Swedish Parliament, Svensk författningssamling 2014:821, Patientlag (2014:821), 2014
20. 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/
21. 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.
22. PCI-DSS Standard, 2005, PCI Security Standards Council, Wakefield, MA, US, https://www.pcisecuritystandards.org

23. 107th United States Congress, Pub.L. 107–204, 116 Stat. 745, The Sarbanes Oxley Act, Washington, 2002