Legal Requirements Process for Compliance and Risk Assessment using Axiomatic Design

Rhythm-Wadhwa[1]

[1] NTNU Gjøvik
Gjøvik 2815, Norway

Abstract

The paper proposes a model integrating regulatory compliance and risk requirements with the top-down axiomatic design/Complexity theory (AD/CT) theory for cloud contracts. The issue of proper division of tasks between man and machine is discussed. The integrated approach is illustrated addressing legal compliance by design and legal contract risk assessment within the realm of cloud computing for manufacturing small to medium sized enterprise (SME).

Keywords: *Product Development, Design Method*

1. Introduction

The communication from the European Union [1], highlights the potential benefits of cloud computing depicting an increase of 2.5 million new European jobs in 2020. The document promotes the need for progress in cloud-contracts for reducing risk for SMEs (Small to medium sized enterprises), legal compliance and supporting actions. Due to the flexibility and rapid growth of computing industry, cloud computing allows manufacturing businesses and governments among other actors to outsource in a cost-effective manner in order to stay competitive. Cloud computing has many advantages, but the one-size-fits-all computing process has accompanying legal implications for organizations. [2]

The sharing of data by either private or public organizations, is subjected to multiple legal constraints. Requirements may be stemming from data privacy rules, copyrights etc. which affects how data is shared. Additionally, specific statutory prohibitions, such as those on government held data may apply. Thus protecting data is crucial for organizations, and sectors using cloud services. The approach taken in this paper is focussed at *compliance by design* with significance on incorporating legal and regulatory requirements into the cloud architecture. Legal guidance, including on core principles of EU data protection law, [11] can thus to some degree be incorporated into the Cloud architecture design.

*1.1. The engineering aspects of requirements process for top-down (**V**), bottom-up (**Λ**) and interdisciplinar (**Ʉ**) design*

At every stage of the top-down Axiomatic design process the design is expressed laterally across fields such as stakeholders, functional, physical, process and vertically within each realm.[5] Bottom-up integrations, object oriented, include those at the systems and sub-system levels. [6] To bridge the gap between law and engineering, CORAS based template, shown in the subsequent sections, may depict un-expected positive results. Viewing this in a larger context of induction with design to define the future of man-machine interactions and decoupling of historical relationships, such mappings could help sensitize us to our advantage. [7] Pulverizing of intellectual streams has been rare, not only while considering predominantly top-down (Axiomatic design) and bottom-up (Design Patterns) approaches [3], requirements processes [4], but also horizontally between interdisciplinar domains of legal research and Axiomatic design. The latter theme is depicted in this paper in context of cloud sourcing with application to a manufacturing SME.

1.2. Compliance by design and risk management in contracts for cloud sourcing- the cloud makes things cloudier

Contractual risk management is legal risk management focused on contracts [8]. The perspective of risk itself is not new since the lawyers in in private practice have always looked to the future in advising their clients. [9] This, Keskitalo's approach to legal contractual risk management suffers from shortcomings of being formulated as a theory and not as a method and putting relatively less emphasis on estimation of risk levels, i.e., risk analysis process of risk management [9], which is described at a level of abstraction higher than, for example, ISO 31000. [10] A contract, which from a purely legal point of view is perfect, can in practice be both a bad contract and a bad tool for business cooperation. [8] The case presented in the work is relating a short-term contract in a single jurisdiction.

2. Integrating the legal requirements process

Major *2.1 Combining Top-down Axiomatic design and structuring the identification of compliance risks using Natural Language Patterns; with bottom-up approach for interdisciplinar design*

The current standards providing compliance guidelines lack in providing a systematic approaches to identifying legal and compliance risks [12][13]. To address this need, one can start with the identification of requirements (binding: such as contracts, legal regulations, court and administrative decisions) (non-binding: industry and organizational standards, ethical standards and principles of good governance), which are relevant to the issue in concern. Legal terminology may be domain specific, applied in a varied manner across multiple laws, may be difficult to interpret or could be related to other laws across multiple jurisdictions. The outsourced nature of the cloud, and the inherent loss of control that accompanies with using cloud computing services, creates challenges for keeping the data confidential.

Figure 1 shows example physical domain (DP) inferred from the functional domain (FR) in AD.[5][27] The cells can be color coded according to identified risk level.

No.	Functional Domain	Physical Domain
1.	High level Compliance requirements (FR 1)	Contract risk assessment (DP1)
2.	Confidentiality (FR 2)	Automated contract data sharing agreement (DP2)

Color coding risks						
High	Liability gap (Warranty)	Fit for purpose gurantee (Warranty)	Product Recall (Safety-related liability)	Accidents (Safety-related liability)	IPR Infringement (Intellectual Property Rights)	Copyright (Intellectual Property Rights)
Medium	Delivery Schedule Change	Quality requirements change	Liability	Disputed IPR claim	End of Breach	Non-performance
Low	Incoming goods inspection	Part Non-conformance	Ingredient disclosure			

Figure 1. Example FRs and DPs

The bottom-up approach puts together the structuring of the obligation and prohibition requirements, using CORAS. [6]

The obligation and prohibition is a clear identification on whose behalf the risk assessment is conducted. Following the identification of the subject and object of compliance, the modality pattern assists in identifying relevant obligations (Os) and prohibitions (Ps) and the output of such an activity provides the list of relevant Os & Ps with references to the articles containing these requirements. Hohfeld's legal taxonomy [14] remains a dominant contribution to the modern understanding of the nature of obligations, for understanding legal rights. Although natural language patterns primarily involve a manual process for identifying elements in compliance norms and respective modalities, there are also tools available, such as, TXL [15] acting as adapters (Figure 2), helping bridge the interdisciplinar gap. A number of related publications based on ISO/IEC 270001 [16], natural language patterens [17], using control techniques to extract legal requirements [18] and others have been mentioned in literature, but somehow axiomatic design as a top-down approach has been overlooked.

Header	From data sharing agreement
Source of requirement	Article 17
Actor	Controller: Read shared data inside. Default:deny
Action	Obligation: <actor> should/must/<verb> Prohibition: <actor> should not/may not <verb>
Object	Personal data
Resources	Technical measures
Threat Scenario	Contravene obligation: not do activity (what) <failure to><verb><object> Contravene prohibition: do activity (what) Section no.
Expiration Date	04/07/2016
Geography	Inside EEA. Default: allow
SIGNED HASH	

Figure 2. Example Cloud Object Adapter

In order to transfer the relevant elements of the requirements for compliance risk model generation the elements of the table are then graphically modelled in CORAS to enable re-usability and enable creation of generic risk database. [6] A knowledge source that can support this step in the method is the ENISA cloud vulnerability list supports the risk model instantiation when the client is an SME. [19] Identification of threat triggers ,i.e. the negation of the main security properties, to the general compliance threat is what makes the risk assessment specific to a target under analysis. One disadvantage of this approach is the deficit of reusable information, which can be a challenge. Nevertheless, in some realms reusable knowledge base can be used a triggers, for example ENISA. In the long term, creating compliance databases with vulnerabilities and threats could be a way forward. The following step would be to instantiate undesirable incidences in terms of consequences, i.e., valued endangered by requirement non-compliance. From a manufacturing SME perspective, this can be relevant for communication of the results of the assessment to the stakeholders, since a general non-compliance with *Article* may be insufficient to understand the implications, so intantiating this in terms of regulatory penalty or customer loss can prove useful. With risk levels decided, lower level compliance measures (FR 11) can be assessed. The above integrated process could prove challenging if one is trying to structure and model all relevant legal obligations/ prohibitions and this can be surmounted by relying on the concerns specified by regulatory authorities. The above approach should be guarded against occurences when the SME conducts compliance risk assessment as a part of their technical assessments. Without a complete compliance approach including legal, technical and managerial teams can prove limited due to subjectivity in risk levels varying between individuals who might be limited in identifying contractual or legal consequences.

2.2 High Level Compliance requirements in cloud outsourcing

The identification of general compliance requirements to be considered during cloud outsourcing depends on the type of cloud service sought and the jurisdiction of the cloud user and this regulatory requirement category may not be exhaustive, but only certain select rules are discussed. But certain requirements may fall into more than one category, there may be newly enacted rules, and the focus on public vs. private users could raise additional issues. The category of **data privacy rules** (Table 1) relates to personal data [21], which include data security, location of data and data transfer rules (European Data Protection Directive 95/46/EC) and data subject rights. This suffers from limitation, namely, no guidance is provided as to whether the cloud provider is considered as a data processor or a controller. The cloud customer would need to pay attention to which jurisdiction stores the data and evaluate the resulting risks. Under the EU reform which was recently approved in December'15, the data subjects are given the right to delete their data. The **e-discovery rules** addresses data access as a means of law enforcement by government agencies. The category **notification of breach** (Table 1) is a generic category of rules related to network, service or data. It is important to note here that many cloud providers offer non-negotiable terms in the contract for controllers such as small-to-medium sized enterprises.

2.2.1 ***Contract***

Some of the contractual issues in purchasing cloud services that might affect compliance, among others, are:

-***liability and warranties*** :it is not straightforward to identify the part responsible in case of breach;

-***change of terms*** :it is commonly noticed that cloud service providers allow the unilateral right to for modification while the customer is unaware;

-***subcontracting*** affects when the cloud customer is not aware of the chain of actors such as software and storage providers or network providers located in different countries.

-***multiple jurisdictions*** :occurs when the customer is not aware how the cloud service provider is trying to limit their risk by operating in multiple jurisdictions.

-***data conveyability*** :denotes that the customer has limited ability to migrate data to a new provider, due to reliance on the current or lack of standardized data formats or service interfaces.

The cloud security alliance (CSA) provides the cloud controls matrix (CCM) when organizations are securing cloud services, and the mapping of the above discussed compliance issues to the control measures, which could assist in re-usability of potential remedies is shown in Table 1.

Table 1 Mapping to CCM

Category	Sub Categories	Mapping to CCM
Privacy of Data	-Technical measures - Organizational measures - Data location and transfer - Subjects rights - Secondary usage	Application interface security (AIS); AIS 2; AIS 4; Business continuity planning (BCR); BCR 3; BCR 5; BCR 6; BCR 7; BCR 10; BCR 11; Change control (CCC); CCC 3, CCC 4; CCC 5; Data security and information lifecycle (DSI); DSI 1; DSI 2; DSI 5; DSI 7; datacentre security asset management (DCS); DCS 2; DCS 3; DCS 4; encryption and key management (EKM); EKM 2; EKM 3; EKM 4; Human resources asset returns (HRS); governance and

		risk management (GRM); identity and access management audit tools (IAM); Infrastructure and virtualization security(IVS)
E-discovery	Compliance to the e-discovery requests by the cloud user	IVS 1; Security Incident Management, E-Discovery and Cloud Forensics (SEF); SEF 1; SEF 5
Contractual issues	-Liability -Subcontracting -Portability -Change of terms at the providers conditions	CCC 1; CCC 2 ; CCC 3; CCC 5; STA 03; STA 7 ; STA 9; HRS 1; HRS 2; HRS 7; Interoperability and portabiltiy APIs (IPY); IPY 1; IPY 2; IPY 3; IPY 4; IPY 5.

CCM: Cloud Control Matrix [26]

The mapping of the control measures doesn’t qualify its effectiveness in addressing the issues, but only indicates the potential remedy that one should consider while adopting cloud services.

2.2.1 User risks in cloud contract structure

Most risks involving cloud computing relate to security, availability and integrity of data. [22] In public clouds, data moves across multiple servers, with unspecified security levels. User information may be disclosed to third party advertising, government agencies, helpdesk operators etc. [23] Much information uploaded to cloud is in hands of private parties and larger the cloud structure, greater the attack surface. Unclear terms for may cause risk to users. For example, a recent case of well established cloud service provider *Nirvanix¸* an apparent competitor to Google, gave its users only two weeks to obtain their data, before closing [24], which may not be sufficient time for an unsophisticated SME. Cloud providers mentioning short or vague time schedules is not uncommon. Some cloud consumers may have special risk considerations regarding document preservation which may cause loss of constitutional protection in case of permissive contract terms.

2.2.2 Conflicts between European Union Data Protection Law and contracting structure

The European Commission has highlighted the uncertainty in contract terms on issues such as liability for service failure, loss compensation and user rights concern in cloud computing. [24] The asymmetrical and non-standardized operations between cloud service providers includes their operational and logistical decisions such as data storage, deletion policy, data location and transfer of data to third parties. Although, it is the cloud consumer deciding on the service, the service provider currently has a greater ability to mitigate risks and balancing this risk will be bought about by the reform. For instance, building on the article 17 (Cloud Object, Figure 2) of the of the Data Protection Directive [25] , article 26 of the proposed data protection regulation will initiate additional requirements to the processor in certain situations. Also, due to change in article 58 of Digital Administration Code, **manually signed data service agreements** (Figure 3.a) **are not required anymore** (Figure 3.b). The scenario 3.b is th**e point of implementation of automation of objects** (Figure 3.b) into the cloud layer, as shown in Figure 3.

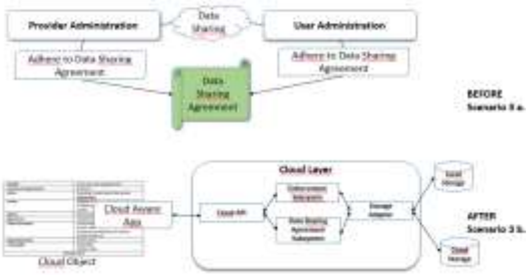


Figure 3. Example cloud data sharing agreement *automation* application built to be accessible by external users

1. 3. Case

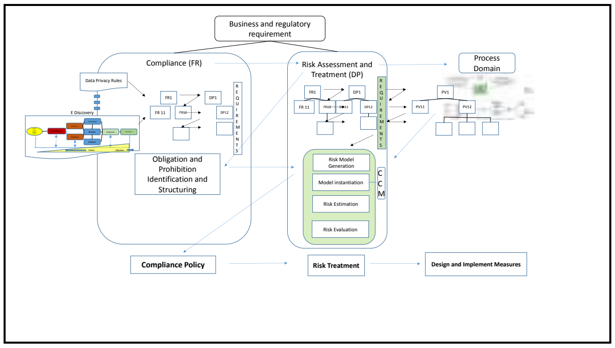
The case company, a supplier of hydraulic connectors with software to an OEM (Original Equipment Manufacturer) wished to analyse the General Terms and Conditions issued by the OEM. Their details of contractual relationship, general terms and conditions (GTCs) is confidential. The *qualitative* risk assessment was conducted on suppliers request, with a team of managers engineers and lawyers, to recommend law related risks and controls to prepare the drafting of corporate contracting policy, to be reproducible for future assessments and negotiations. The manufacturing contract worth 200 million Euros was assessed during 22 meetings with the stakeholders over a period of four months. The supplier operates and handles confidential information such as financial, technical and personal data. The case study evaluated the use and challenges of using the model (Figure 4) and to observe where the methodology with respect to current practices.

The risk identification resulted in 90 risks, which was documented in a risk register. It was later reduced to 22 consisting of 12 high risks, 6 medium and 4 low risks. In a contractual context, the legal risk management methodology will need to manage the non-legal aspects as well which are typically implied in the nature of the manufacturing industry, which needs to be governed by the contract. [29] The risk treatment focused on three types of risk controls. The first category was a letter sent to the OEM requiring special terms and conditions with respect to certain clauses in the suppliers GTCs which were considered particularly risky. These legal controls were accompanied with technical measures in manufacturing processes which intended to modify the respective risks. The third control had a long term focus on contracting policy that identified the risks to be managed in future contract assessments. On comparing the identified risks and risk controls, the correlation between risk level and the control utilized becomes apparent. First, the diversity of treatment strategies correlated to the level of risk , i.e., high risks required treatment with an integrated approach, which included all three types –contract negotiation, contracting policy and other controls. Second, higher the risk level, the likely it is to be considered with law related controls of contract negotiation and contracting policy. The low risks were considered to be treated with non-legal controls. It is important to note that the risk management processes should have a positive cost-benefit ratio for large-scale or high-risk contracts. A tool such as the stakeholder spreadsheet was found to be cumbersome, and limited in facilitating interdisciplinary communication.[4] Nevertheless, the CORAS tool [6] proved beneficial while communication legal risk within the non-legal team members. Such a graphical modelling tool does suffer from the limitation that it is limited in capturing complex legal issues and when interpreting laws that are drafted on an abstract level, which requires legal expert judgement. This can prove challenging taking into consideration the fact that Axiomatic design relies on establishing clear definitions. The tool also tends to oversimply extremely complex legal issues.

Conclusions

The paper describes the integration of top-down and bottom-up approaches, when seen in light of single jurisdiction contract based compliance risk assessment. The limitations of the method and case study have been discussed. Often cloud services deliver what they promise, however if delays are encountered consumers including SMEs may struggle in assigning liability, and be able to meet compliance requirements on standard contract terms. There is a potential for mutual advantage to manufacturing businesses while integrating the such approaches for legal compliance, but as Aristotle once said, ‘*one swallow doesn’t make summer*’, further applications to multijurisdiction and high regulatory environments, are on-going.

Figure 4. Model



References

[1] Communication on ‘Unleasing the potential of cloud computing in Europe’. COM (2012), 529.
[2] Araiza AG, (2011), Electronic discovery in the cloud, *Duke Law and Technology Review*, No.8.
[3] Thomas J, Mantri P, (2015), Axiomatic Design/Design Pattern Mashup: Part 1 (Theory)*, CIRP 9th ICAD, Florence, Italy,* 268-274.
[4] Thompson MK, (2013), Improving the requirements process in Axiomatic Design Theory, *CIRP Annals-Manufacturing Technology* 62/1: 115-118.
[5] Suh NP, (1990), The Principles of Design, 1st edition, NY, Oxford Press.
[6] Lund MS, Solhaug B, Stølen K, (2011), *Model driven risk analysis, The CORAS approach*, Springer-Verlag Berlin Heidelberg.
[7] McAfee A, Brynjolfsson (2012), *Race against the machine,* Digital Frontier Press, MA.
[8] Nysten-Haarala (2006), Contract law and everyday contracting, *Scandinavian studies in law*, (49), 264.
[9] Keskitalo P (2006), Contracts+Risk+Management=Contractual Riskmanagement? *Nordic Journal of Commercial Law,* no.2.
[10] ISO 31000 (2009), Risk Management- Principles and guidelines.
[11] Council Directive 95/46/EC, article 2 (d).
[12] Australian Standard AS 3806 (2006), Compliance programs.
[13] COSO (2004), Enterprise Risk Management: An integrated framework. Committee of sponsoring organizations of the Treadway commission.
[14] Hohfeld WN (1913), Fundamental legal conceptions as applied in judicial reasoning, *Yale Law Journal*, 23 (1), 710-770.
[15] CORDY JR (2006), The TXL source transformation language. *Science of Computer Programming*, 61(3): 190-210.
[16] Mellado D, Medina E, Piattini M (2007), A common criterion base d security requirements engineering process for the development of secure information system, *Computer standards and interfaces*, 29:244-253.
[17] Breaux TD, Anton AI (2008), Analyzing regulator rules for privacy and security requirements, *IEEE transactions on software engineering*, Vol. 34., No. 1.
[18] May MJ, Gunter CA, Lee I (2006), Privacy APIs: Access control techniques to analyse and verify legal privacy policies, *19th Computer Security Foundations Workshop*.
[19] ENISA (2009), Cloud computing: benefits, risks and recommendations for information security. *European Network and Information Security Agency.*
[20] Deng M, Kim W, Riccardo S, Bart P, Woute J (2011) A privacy threat analysis framework: supporting the elicitation and
[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (2012) *Unleashing the potential of cloud computing in Europe,* COM, Commission communication.
[22] Jansen W, Grance T (2011), Guidelines on security and privacy in public cloud computing, *National Institute of Standards and Technology.*
[23] Gervais DJ, Hyndman DJ (2011), Cloud control: copyright, global memes and privacy, *Journal On Telecomm. And High Tech L.*
[24] European Commission (2012) Unleashing the potential of cloud computing in Europe, *EUR-LEX 5.*
[25] European Commission Justice, Protection of personal data. http://ec.europa.eu/justice/data-protection/index_en.htm.’
[26] https://cloudsecurityalliance.org/
[27] Suh NP(2005), Complexity: theory and applications, *Oxford University Press*,NY.
[28] Kim SG, Nordlund M, Oh H, Lee T (2015), Axiomatic design: 30 years after, *IMEC 2015-52893,* ASME.
[29] Iversen (2007), *Legal risk management I private virksomheder*, Forlaget Thomson.