

Association for Information Systems

AIS Electronic Library (AISeL)

CONF-IRM 2021 Proceedings

International Conference on Information
Resources Management (CONF-IRM)

Summer 2021

Internal IT Control Systems and Global Regulation of Organizations: The Rise of Control Assemblages

Edward Bernroider

Follow this and additional works at: <https://aisel.aisnet.org/confirm2021>

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2021 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Internal IT Control Systems and Global Regulation of Organizations: The Rise of Control Assemblages

Edward W.N. Bernroider
Vienna University of Economics and Business
edward.bernroider@wu.ac.at

Abstract

The encounter between global regulation and IT offers a challenging environment in organizations to investigate how internal control systems (ICS) emerge and social orders are changed. In this research paper, I used the opportunity to investigate assemblages that have coded and territorialized IT in a large organization. Based on a case study, the paper emphasizes that ICS are composed of loosely structured, ever evolving heterogeneous components and systems, which are involved in constant re-conceptualization. In particular, processes leading to the creation of control assemblages, resulting tensions and conflicts, and the roles of the installed base and exteriorized relations are shortly discussed.

Keywords: Internal Control Systems, Assemblages, Case Study; Information Technology Regulation, Accounting Information Systems.

1. Introduction

The increasing dependence of organizations on Information Technologies (ITs) generates configuration and control phenomena that invite us to reframe our ways of understanding organizational structures and management control (Dechow, Granlund, & Mouritsen, 2006). ITs have not only become critical business enablers, e.g., allowing for enterprise resource planning in both developing and developed economies (Bernroider, Sudzina, & Pucihar, 2011), but also political objects themselves, where their organizational adoption becomes a matter of socio-political controversy (Barry, 2001). Disruptions of business services due to IT related incidents have become common, especially in organizations which are complex, large, growing rapidly, or undergoing restructuring (Doyle, Ge, & McVay, 2007), or among organizations that heavily rely on IT such as banks, which need to explicitly cover associated operational risks (Bauer & Bernroider, 2013; Jobst, 2007).

As response to this problem, international laws and regulations together with supporting standards are constantly emerging, which require constant changes in governance and work routines, and record-keeping control and test procedures to allow for the production of information that can be appraised by management and auditors. For example, the Sarbanes Oxley Act (SOX) requires the design and operation of a broad range of IT controls to protect shareholders from corporate fraud (US-Congress, 2002). It triggered a wave of worldwide adaptations and derivations of SOX with similar compliance requirements, e.g., the European version publicly known as EUROSOX (EU, 2006). Or, more recently, the General Data Protection Regulation (GDPR) was introduced, which has wide implications on how data is governed and controlled across the organization (Tikkinen-Piri, Rohunen, & Markkula, 2018). These laws require organizations to develop and maintain effective internal control over IT services, and constantly strive for achieving regulatory compliance, e.g., in terms of compliant information security behaviors (Bauer & Bernroider, 2015; Bauer & Bernroider, 2017). It is worth noting that these efforts are generally costly and complex. For example, in terms of achieving SOX compliance, organizations reported high control system expenditures and major audit delays (Ettredge, Li, & Sun, 2006).

IT control system configurations, which includes various relationships among diverse actors, artefacts and organizational units, need to continuously adapt and change to meet the requirements of evolving external regulations, standards and frameworks, and dynamic IT risk landscapes (Krumay, Bernroider, & Walser, 2018, 2020). This research study applies assemblages, a conceptual apparatus also inherently unstable and infused with movement (Marcus & Saka, 2006). Assemblages in general terms can be seen as dynamic entities under constant reconfiguration, including changing contexts and territories (Deleuze & Guattari, 1987). Consequently, I apply this dual attention of assemblages to structure and change to the practical problem of how IT is controlled in a large case organization driven by laws and standardization. First, I seek to provide an analysis of processes and components of an IT control assemblage in the given context. I am interested in shedding some light upon the processes through which these heterogeneous, unstable and ephemeral components of such an assemblage are recursively created, and in its movement from a recent past toward a near future, which is the temporal span of emergence I am observing. Second, I seek to discuss the emergence of internal IT control configurations from these processes, the role of tensions and conflicts between material actors, and components in the space of assemblage theory. By doing so, I will explore social construction processes and how these are entwined with IT's material properties, and intentionally move away from isolated techno-centric or human-centered views on control system designs or matters related to control configurations or performance. In methodological terms, I draw on a case study of a large Information and Communication Technology organization on the basis of a cyclic action research design. Next, I will attempt a short overview of what I mean by referring to global forms and assemblages, and IT regulation. However, since there is ambiguity in the referential frames of assemblages in literature and due to the space limitations of this paper, I need to point to other resources for a more informed introduction (e.g. Collier & Ong, 2005; DeLanda, 2006; Harman, 2008; Lanzara, 2009; Marcus & Saka, 2006). Next, an overview of data collection and analysis, and the main results are presented. The following discussion positions these results more clearly in prior literature and selected conceptual elements within the frame of assemblages. The last section concludes the article.

2. Research Background

2.1. Global Forms and Assemblages

The analysis provided in this paper draws on the body of literature using the concept of global forms and assemblage in social and organizational research (Marcus & Saka, 2006; Mennicken & Miller, 2012). Assemblage theory is rooted in the works of Gilles Deleuze and Felix Guattari (1987), but was more fully developed by DeLanda (2006). For the use in this study, we define an assemblage as follows (Collier & Ong, 2005, p.12): *“An assemblage is the product of multiple determinations that are not reducible to a single logic. The temporality of an assemblage is emergent. It does not always involve new forms, but forms that are shifting, in formation, or at stake.”*

Underlying the understanding of such a composite concept is the mapping of exteriorized parts characterized by properties and capacities. When considering exteriorized relations, the properties of single parts cannot explain the relations which constitute the whole. The properties of the whole are dynamic and result from the actual exercise of capacities, which not only make use of a component's properties, but also involve properties of other interacting entities (DeLanda, 2006). Central to mapping these exteriorized relations of assemblages are two axes (Deleuze & Guattari, 1987). The first axis determines the levels of materiality to

expression and the second travels from territorialization to deterritorialization. The latter can be understood as processes in which components are involved that can either stabilize or destabilize the assemblage. Stabilizing usually means to increase internal homogeneity and/or sharpen boundaries (Harman, 2008). A third axis added by DeLanda (2006) invites the investigation of linguistic expressions shifting from codings to decodings, which may either work towards consolidation or flexibilization of the identity of the assemblage.

Still drawing on DeLanda (2006), the resulting components of an assemblage are heterogeneous and can be characterized by either a material or expressive role (or both). While material components are usually resources and reflect the content, expressive components can be seen as the descriptive elements and can include triggers and signals for behavioral responses. Territorialization processes can be connected with components that play a material role and coding processes with components taking expressive roles.

2.2 Global IT Regulation and IT Control Frameworks

Organizations worldwide are affected by laws and regulations (Luthy & Forcht, 2006), which acknowledge the critical role of ITs to ensure the effectiveness and efficiency of business processes, the accuracy of data processing, and security and privacy objectives (e.g. Bauer & Bernroider, 2017; Tikkinen-Piri et al., 2018). Organizations seeking compliance with these laws and regulations need to effectively control risks related to these ITs. It is often suggested to use publicly available standards for such internal control design by public bodies. For example, The Public Company Accounting Oversight Board (PCAOB) was charged with overseeing, regulating, inspecting and disciplining accounting firms in the context of SOX (US-Congress, 2002). As another important actor it releases auditing standards which organizations acknowledge. Their specific standards numbers 2 and 4 consider the importance of IT in the arena of internal control (PCAOB, 2004, 2007).

One well established control framework is the Control Objectives for IT and related Technology (CobiT) framework (ISACA, 2008) which is extensively used in IT management and control (Bernroider & Ivanov, 2011; Tuttle & Vandervelde, 2007) and seeks to support legal compliance with regulative requirements such as given by the SOX or Basel 2 (Hardy, 2006; Kordel, 2004). CobiT was developed by the Information Technology Governance Institute (ITGI) and its associated Information Systems Audit and Control Association (ISACA). CobiT as well as other systems for management control refer to best practice guidelines with limited empirical and theoretical support. It is used by auditors, IT managers and consultants to evaluate the state of internal control and to manage the IT related risks in the enterprise.

3. Data Collection and Analysis

3.1. Case Description

In considering what kind of practices emerge when facilitating internal IT control in an organization, it is useful to first consider the type of organization and actors involved. The analysis in this paper applies to a large Information and Communication Technology organization with over 5000 employees. The organization needed to develop and certify a SOX compliant internal control system (ICS) especially to account for their heavy reliance on ITs for conducting business. Among the used ITs were hundreds of different artefacts, which potentially had to be considered in the configuration of the ICS. These artefacts were operating on a complex IT infrastructure and connected with numerous extensive data bases and extensive data volumes. IT users and service providers, testers and auditors needed to execute routines and maintain these ITs.

3.2. Data Collection and Analysis

The aim of the two-staged data collection process was to review and support developing the strategy, design and operating effectiveness of the general IT controls used in the organization's internal control system over IT. In both stages I was directly involved in field activities including interviews, presentations, audits, meetings and workshops. Table 1 shows an overview of contact sessions and data collection durations.

The field research strategy followed a cyclic action research design (McKay & Marshall, 2001), where results from the first stage were inputs for the second. The action approach allowed for overcoming the passivity of research found in many traditional case studies. Especially when organisational change is involved, the active role of the action researcher allows achieving a more in depth understanding of the complex multi-dimensional transformations and their socio-technical dynamics. Additionally, informal gatherings provided important sources of information. These multiple data collection sources allowed for a sustained consideration of events with data needing to converge in a triangulating fashion (Wynn & Williams, 2012).

	Research cycle 1	Research cycle 2	Main contact group(s)
Briefings	5	5	Control owners
Operational control tests	28	95	Control owners & executors
De-briefings	0	3	Control owners
Intermediate reporting	1	4	Quality management
General meetings	8	2	Program Managers
Workshops/presentations	1(ex-post)	1 (a priori)	All main stakeholders
Total field sessions	43	110	
Scoping (framework and risks)	1 week	2 day	
Scoping (systems)	2 weeks	2 days	
Design tests	2 weeks	2.5 days	
Operational tests	5 weeks	5 weeks	
Reporting	2 weeks	Concurrent	
Total durations	12 weeks	~6.5 weeks	

Table 1: Overview of field research contact sessions and durations

The early activities during the first three-month research cycle (i) were dedicated to reviewing the legal requirements for IT control in the organizational context, followed by testing the current and desired states of their internal control system, before reflecting upon the findings and suggesting ways to improve the configurations. The second research cycle (ii) followed three months later and took almost 2 months. It placed a stronger emphasis on testing the achieved progress in institutionalizing the ICS and the further collaborative changes needed to remediate identified control problems. The field work was supported by research assistants who helped to coordinate the schedules, prepare documents, and perform repetitive tests with organizational actors such as control executors in relation to specific systems with clear instructions and forms. Almost all exchanges were transcribed into a common format by the testers or interviewers, and used for quantitative and qualitative analysis. Quantitative analysis provided summary statistics on control design and operating effectiveness per area. Ex-post meetings with managers or the auditors allowed for discussing the main themes pertaining to problems, such as conflicts, and make better sense of the rich data collected (Cresswell, 2003).

In addition, the use of further data collection methods at different research stages allowed for data source triangulations to ensure a comprehensive view and increased validity of findings

(Denzin, 1984; Yin, 2003). A large volume of business and technical documentation in particular including prior testing results, control and process definitions, roles and responsibility assignments, and related presentations was analysed. Most importantly, work processes and meetings were not only passively observed but also actively conducted by the researcher in an auditor’s capacity.

4. Main Results

In this section, I firstly give the identified main assemblage components before describing the specific processes producing assemblages, which were enacted based on the capacities of the given components. The following discussion in more detail explains how these findings relate to assemblages and the roles of regulation and standards in their dynamic creation.

1.1. Main Assemblage Components

The main components identified in the assemblages are summarized in Table 3. They are heterogeneous, can be material (e.g. software applications) or take on an expressive role (e.g. control owners). Material components are resources and can be interpreted as the content of the assemblage. While expressive components are actively engaged in coding processes, the material components can be connected with territorialization.

	Research cycle 1	Research cycle 2
Professional auditors	4	3
IT processes	14	13
Control owners	21	17
Control executors	>50	>50
Process owners	>100	>100
Systems (applications only)	16 (out of >50)	10 (out of >50)
Core networks	10	(not considered)
User developed applications	11	8
IT general controls (incl. system instances of abstract controls)	>100	>100

Table 3: Selection of assemblage components

1.2. Main Processes

The first set of processes includes scoping and designing activities sought to harmonize the global standards and adapt a configuration suiting the context of the organization. Linking into the assemblage theory, these processes exhibit territorialization and codification characteristics which were guided by global standards (see Figure 1). These were prescribed by the SOX act and their regulative bodies (such as the PCAOB) as external legislation, and framework recommendations, which in our case relates to the CobiT framework. The product of territorialization and codification at one point of time included 14 IT processes with cross-referenced control objectives, links with 16 application systems, 10 core networks, 11 user-developed applications and large sets of testable controls designs, which were all linked to internal and external people with associated responsibilities. In addition to scoping these components, common measurement systems including sampling procedures were established. The second set of processes is related to operational tests and reporting, which can be conceptually related to aims of qualification, where the qualities of business processes are assessed by means of past control executions and operational tests in order to show if they meet the criteria laid out in effective design documents.

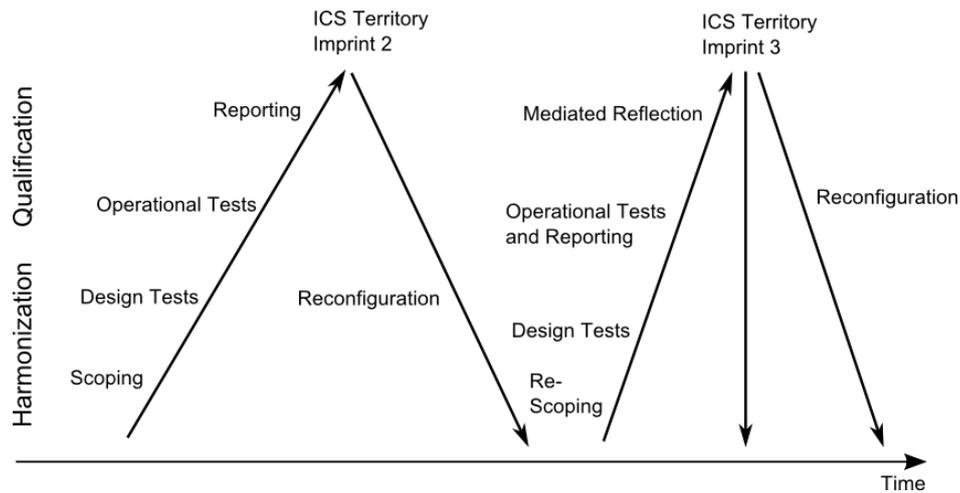


Figure 1: Harmonization and qualification processes in constant ICS re-creation

2. Discussion

2.1. The Emergence of Control Assemblages

The identity of an assemblage as noted by DeLanda (2006, p.28), “*at any level of scale is always the product of a process and it is always precarious, since other processes can destabilize it.*”. The identified processes were also recursive, emergent and contingent, while the created identities of assemblages can become almost stable. Aiming at accountability is inherently territorializing (Mennicken & Miller, 2012). The continuous and shifting assemblage always has a territory while the borders, which define “zones of control” (Lemos, 2010), change over time as they are challenged by regulative and social forces outside of and within the organization. Drawing on the case, different types of (de-)territorialization processes struggled with these often opposing forces in what was called scoping the IT process and ITs landscapes, and control objectives which guided the further design of effective IT general controls to be used for calculative practices.

The control objectives should account for risks, which, however, were mainly derived from the standards through mediation processes including external consultants, internal quality management and revision. This again demonstrates the strong impact of global forms. Drawing on the concept of an “global variable” (Collier & Ong, 2005), the used CobiT framework was available to all components in particular the actors of the assemblage, and offered universally accepted best-practice content, which, however, was modified or overwritten if conflicts emerged with other local variables or views. We can extend the concept of the “global variable” to reflect the situational multiple outcomes of standards (Timmermans & Epstein, 2010), by interpreting these as “abstract global variables”, which may be overwritten in specific sociomaterial contexts.

The established measurement systems in the first set of identified processes can be conceptually linked with an assemblage as a metrological zone (Barry, 2001). According to this concept, differences in measurement approaches are minimized to allow for performance comparisons across components of the assemblage. Once the process reaches testing and reporting activities, the assemblage moves to a zone of qualification (Barry, 2001). Once the reports were officially delivered to upper management, a new “official” ICS imprint with clearly outlined borders denoting zones of control was established, which, however, gets instantly outdated through its constant re-creation by continuous process and control executions or failures.

2.2. The Tension of Creation

The notion of global forms in the context of control assemblage suggests an inherent tension in (re-)creation. The term global implies the existence and institutional relevance of broadly encompassing, seamless and mobile norms or structures which need to be imposed on assemblages, which imply heterogeneous, fluid, partial, contingent and situated components (Collier & Ong, 2005). This inherent conflict was clearly observable in the case.

The above sketched (re-)creation processes iterated in short or long cycles, and each iteration synthesized a new population of assemblages. The capacities of internal and external experts as material components worked together to identify and codify the IT processes and activities, the central systems and self-developed applications. New expressive components, e.g., design documents and control instructions, and material components, e.g., workflow systems and internalized consultants, were created and existing ones changed. However, the interaction with standards (e.g. CobiT) was always partial and uneasy as attempts were made to align the broadly encompassing norms with existing heterogeneous and contingent elements. The tension of creation derives from the ongoing struggle between these processes, the unstable interrelationships with global forms, and the direction of territorialization or codification (re-)creation processes generate. However, the processes were framework-mediated, and framework-supported institutional arrangements emerged as a result.

Multiple conflicting logics emerged in the organization as control-based imperatives derived from global forms entered established institutional domains, which caused low perceptions of legitimacy through individual cognitions. For example, formal control requirements for certain tasks were partly at odds with existing routines and legitimacy principles of autonomy and fairness. Low perceptions of both aspects of legitimacy have been linked with low control compliance intentions in the context of IS development (Walser, Cram, Bernroider, & Wiener, 2020). Middle management's attempts of coercive methods of influence partly failed to mobilize human agents expected to provide essential control capacities. It is suggested that resulting partial or situated circumventions of control requirements and their effects are as much part of the assemblage as the global form is itself (Dunn, 2005). In this context the study of global control assemblages offers how actors reflect upon global forms and call them into question. Failure to account for control requirements may require actors to accept these as unavoidable conditions for which, however, new or alternative modes of rational action can be used as an intervention (Holmes & Marcus, 2005). In this case for example, failure to automatically produce testable information on user accounts for certain systems may result in providing alternative ways of book-keeping users profiles and accounts, or alternatively, deterritorialization processes changing boundaries.

Moreover, legal and cultural forms of accountability interact with each other. It is therefore difficult to obtain fully functional, formalized and well-integrated configurations. What is achieved instead are incomplete, semi-automated and incompatible components such as "abstract" controls, which need to be instantiated and changed according to contextual requirements. Moreover, other institutional components, which were created in the past and are now partially or fully incomplete, cannot not be easily discarded or replaced. They have distinct identities and remain part of constantly changing assemblages.

2.3. The Role of the Installed Base

As institutions can become wired into IT-topologies and infra-structures, the installed base is critical for organizational change and control requirements (Chae and Lanzara, 2006; Ciborra

2000). In the sense of the sum of history, the installed base summarizes the current technologies and systems the organization dominantly uses. In the case study, the installed base included over 50 centrally registered systems and even more de-central and self-developed applications supporting various business processes (see Table 3). Systems reside on heterogeneous IT infrastructure and are operating with extensive data volumes. The classic views on the technical dimensions of the installed base, however, do not account for the concept of assemblages, where one equally needs to consider interrelated heterogeneous components and exteriorized relations. Moreover, within assemblages technical objects and systems can become institutional and constitutive (Lanzara, 2009). These material components thus become equally critical for their capacities for execution as well as for the roles they play in the configuration of relationships among heterogeneous components, such as risks, control objectives, controls and human actors. This can lead to a better understanding of a competitive situation, where, e.g., ITs and regulation, or IT owners and (human or artificial) actors with control responsibilities strive to “harmonize” one another, each trying to impose views, principles or norms.

In the case, this phenomenon was clearly observed through conflicts between systems and rules, e.g., when unintentional changes of legacy systems could not be automatically identified due to a lack of logging capacities which opposed the standard requirement of being able to back-track any system changes. One central implication arising from this situation is about the question of design. If the installed base is dynamic and dominates business routines, and is an independently given ex ante context, can the requirements of global norms be applied to freely design system-related controls? The more general question is whether the underlying assemblage can be designed (Lanzara, 2009). With regard to the case study, the answer seems to be no. Actors had to cope with the properties of the installed base and design feasible and innovative workarounds termed compensatory controls especially related to legacy systems and self-developed applications.

2.4. The Importance of Exteriorized Relations

Components through exteriorized relations affect each other, in particular the historic components of the organization. The idea of exposure to the exteriority of relations within control assemblages is largely neglected in IS accounting literature. Conventional literature views components of control systems as largely internalized, self-presented subjects, which can be independently used as inputs for control activities, assessments or audits. Either technocentric or human-centered perspectives dominate, while constitutively entangled social and material views are largely missing (Orlikowski, 2007; Orlikowski & Scott, 2008).

In assemblage theory, however, the properties of the whole are not “the result of an aggregation of the components’ own properties but of the actual exercise of their capacities” (DeLanda, 2006, p. 11). While these capacities depend on the components’ properties, they cannot be reduced to them since they involve reference to the properties of other interacting components. To illustrate this situation, the effectiveness of the control assemblage cannot be determined through aggregating control effectiveness for each material component, e.g., a particular software application, or expressive component, e.g., a IT general control description, in isolation. Only through understanding the actual exercise of capacities involving a number of heterogeneous components in a sociomaterial process, insightful estimates of control effectiveness levels can be attempted. In sum, it is essential to consider externalizing the component as opposed to thinking of self-containing individual elements in an attempt to simplify the analysis. This in particular applies to IT risks which have complex externalized exposures effectively guiding the territorialization of IT control assemblages.

Deterritorialization through exteriorized relations can disrupt spatial boundaries or increase heterogeneity. For example, in the case study the introduction of new global standard or framework revisions (CobiT version 3 to 4 by ISACA) or new guidelines from the oversight body (audit guidelines issued by PCAOB) have potential deterritorialization effects and may lead to shift of boundaries and the exclusion or inclusion of new components within the assemblage.

3. Conclusions

This paper refers to the idea of control assemblages with which to address the problem of introducing broadly encompassing and seamless global forms for internal control, while accounting for the history and dynamics of the organization, and heterogeneity within the ephemeral (Marcus & Saka, 2006). While the global prescription derived from norms and standards are reasonably well covered in prior literature, their constant socio-material reconceptualization with effects, contradictions, and changing relationships is not. The mix of both, the global and structural with the unpredictable and contingent, is usually not considered within the classical traditions of social or computer science based IS research. A number of interesting observations were made in the case study deemed to offer interesting options for further analysis in future research.

I can reasonably speak of control-mediated institutional arrangements which emerged from sociomaterial practices within an assemblage involving global rules and the regulatory regime exemplified by the case analysis. The organizational setting provided a rich field of problems and resistances in control assemblages driven by IT related risks and the attempt to impose control-imperatives on social practices and material elements. The identified standardization and harmonization processes enacted by the capacities provided by material and expressive components aimed at achieving accepted commonalities and establish assemblages as zones of control, measurement and qualification. However, a number of tensions, conflicts and conflicting logics emerged in ongoing struggles between components, in particular based on the uneasy relationship with global forms. Observed partial or temporary circumventions of controls are suggested to be part of the assemblage as much as the global form itself. Furthermore, exteriorized relations in particular linked with the global form can disrupt spatial boundaries and trigger new de-territorialization processes.

The formation, development and sub-sequent evolution of control assemblages were clearly path-dependent. The complexity of current conditions and previously made decisions including non-human components (such as the installed base), and human components and capacities (such as their tacit knowledge) imposed given constraints limiting free-designs derived from global forms. In relation to research cycle one, the organizational stakeholders and external auditors alike accepted with sufficient reasoning and compensating processes that certain elements of global forms had to be “overwritten”. Thus, the global form was accepted as “abstract global variable”, which instances are context-specific temporally territorialized assemblages.

In the context of global assemblages for internal control over IT, further research is warranted to extend upon these issues or develop other potentially rewarding avenues in space of assemblage theory. One empirically overlooked issue is that organizational actors are offered capacities from emerging assemblages through relations of exteriority with new potentials for quality control, which may go beyond compliance and its view of “only” satisfying legal control requirements.

References

- Barry, A. (2001). *Political machines: Governing a technological society*. New York: The Athlone Press.
- Bauer, S., & Bernroider, E. W. N. (2013). *IT Operational Risk Awareness Building in Banking Companies: A Preliminary Research Design Highlighting the Importance of Risk Cultures and Control Systems*. Paper presented at the International Conference on Information Resource Management (CONF-IRM), Natal, Brazil.
- Bauer, S., & Bernroider, E. W. N. (2015). *The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring*. Paper presented at the Human-Computer Interaction International Conference (HCII) - Human Aspects of Information Security, Privacy, and Trust, Switzerland.
- Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *ACM SIGMIS Database: The Data Base for Advances in Information Systems*, 48(3), 44-68. doi:10.1145/3130515.3130519
- Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, 29(3), 325-336. doi:10.1016/j.ijproman.2010.03.002
- Bernroider, E. W. N., Sudzina, F., & Pucihar, A. (2011). Contrasting ERP absorption between transition and developed economies from Central and Eastern Europe (CEE). *Information Systems Management*, 28(3), 240-257. doi:10.1080/10580530.2011.585581
- Collier, S. J., & Ong, A. (2005). Global assemblages, anthropological problems. In A. Ong & S. J. Collier (Eds.), *Global assemblages: Technology, politics, and ethics as anthropological problems* (pp. 3-21).
- Cresswell, J. (2003). *Research design: qualitative, quantitative, and mixed methods approaches*. California, USA: Sage Publications.
- Dechow, N., Granlund, M., & Mouritsen, J. (2006). Management control of the complex organization: relationships between management accounting and information technology. *Handbooks of Management Accounting Research*, 2, 625-640.
- DeLanda, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. New York: Continuum.
- Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.
- Denzin, N. (1984). *The research act*. Englewood Cliffs, NJ: Prentice Hall.
- Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1-2), 193-223. doi:DOI: 10.1016/j.jacceco.2006.10.003
- Dunn, E. C. (2005). Standards and Person-Making in East Central Europe. In A. Ong & S. J. Collier (Eds.), *Global assemblages: Technology, politics, and ethics as anthropological problems* (pp. 173-193).
- Ettredge, M., Li, C., & Sun, L. (2006). The impact of SOX Section 404 Internal Control Quality Assessment on Audit Delay in the SOX Era. *Auditing: A Journal of Practice & Theory*, 25(2), 1-23.
- EU. (2006). Directive 2006/43/EC. *Official Journal of the European Union*, L 147(87), 1-21.
- Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11(1), 55-61.
- Harman, G. (2008). DeLanda's ontology: assemblage and realism. *Continental Philosophy Review*, 41(3), 367-383.

- Holmes, D. R., & Marcus, G. E. (2005). Cultures of expertise and the management of globalization: toward the re-functioning of ethnography. In A. Ong & S. J. Collier (Eds.), *Global assemblages: Technology, politics, and ethics as anthropological problems* (pp. 235-252).
- ISACA. (2008). *COBIT - 4th Edition (Version 4.1)* (3 ed.). Rolling Meadows, USA: Information Systems Audit and Control Foundation, IT Governance Institute.
- Jobst, A. A. (2007). It's all in the data – consistent operational risk measurement and regulation. *Journal of Financial Regulation and Compliance*, 15(4), 423-449.
- Kordel, L. (2004). IT Governance Hands-on: Using COBIT to Implement IT Governance. *The Information Systems Control Journal*(2), 39-46.
- Krumay, B., Bernroider, E. W. N., & Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. In N. Gruschka (Ed.), *Lecture Notes on Computer Science (LNCS) - Proceedings of the 23rd Nordic Conference (NordSec 2018)* (Vol. 11252). Oslo, Norway: Springer.
- Krumay, B., Bernroider, E. W. N., & Walser, R. (2020). *A Framework to Achieve Cybersecurity Accountability of Critical Infrastructure Providers – a Design Science Research Approach*. Paper presented at the 17th Conference of the Italian Chapter of AIS (Association for Information Systems), Pescara, Italy.
- Lanzara, G. F. (2009). Building digital institutions: ICT and the rise of assemblages in government. In F. Contini & G. F. Lanzara (Eds.), *ICT and innovation in the public sector: European studies in the making of e-government* (pp. 9-48). London: Palgrave Macmillan.
- Lemos, A. (2010). Post—mass media functions, locative media, and informational territories: New ways of thinking about territory, place, and mobility in contemporary society. *Space and Culture*, 13(4), 403-420.
- Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*.
- Marcus, G. E., & Saka, E. (2006). Assemblage. *Theory, Culture & Society*, 23(2-3), 101-106.
- McKay, J., & Marshall, P. (2001). The dual imperatives of action research. *Information Technology and People*, 14 (1), 46–59.
- Mennicken, A., & Miller, P. (2012). Accounting, territorialization and power. *Foucault Studies*(13), 4-24.
- Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization studies*, 28(9), 1435-1448.
- Orlikowski, W. J., & Scott, S. V. (2008). 10 Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The academy of management annals*, 2(1), 433-474.
- PCAOB. (2004). *Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*. Retrieved from
- PCAOB. (2007). *Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements*. Retrieved from
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153.
- Timmermans, S., & Epstein, S. (2010). A world of standards but not a standard world: toward a sociology of standards and standardization*. *Annual review of Sociology*, 36, 69-89.

- Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, 8, 240–263.
- US-Congress. (2002). *Sarbanes-Oxley Act of 2002* (H. R. 3763). Retrieved from Washington:
- Walser, R. J., Cram, W. A., Bernroider, E. W. N., & Wiener, M. (2020). *How Control Configurations and Enactments Shape Legitimacy Perceptions and Compliance Intentions in IS Development Projects*. Paper presented at the 28th European Conference on Information Systems (ECIS), Online AIS Conference.
- Wynn, J., Donald, & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS Quarterly*, 36(3), 787-810.
- Yin, R. K. (2003). *Case Study Research - Design and Methods* (3 ed.). London: SAGE Publications.