DOI: 10.5748/16CONTECSI/AUD-6027

GOVERNING SHADOWS: GOVERNANCE MECHANISMS FOR AUTONOMOUS IT SOLUTIONS

Humberto Caetano Cardoso da Silva - Universidade Federal de Pernambuco - humberto.ccs@gmail.com
Rosamaria Belo Lucena - Universidade Federal de Pernambuco - rosamaria.lucena@gmail.com
Henrique Santos Ferreira - Universidade Federal de Pernambuco - riqueferreira@gmail.com
Jairo Simião Dornelas - Universidade Federal de Pernambuco - jerh57@gmail.com

Abstract: Shadow IT encompasses solutions deployed by users, outside the formal structure of IT management. The dissatisfaction with official systems is often the main motivation for the adoption of Shadow IT. Through it, users expect to streamline business processes and improve the user experience. In terms of IT governance, however, Shadow IT means a challenge. The classic IT governance approach addresses issues of control and compliance. However, in a context where solutions are not endorsed by experts, how can these governance elements can be implemented is a question without a clear answer. In this essay, it is suggested that a possible path to achieved higher levels of IT governance is to bring IT closer to end users, making Shadow IT a source of organizational innovation. To do so, it is necessary to expand the view on IT governance and to extend the use of mechanisms related to the informal dimension of governance, specifically the self-control mechanisms. The self-control mechanisms are implemented, primarily, by the controlled. However, the controller may stablish the formal mechanisms of control, so encouraging or enabling the controlled to exercise self-control.

Keywords: Shadow IT; IT Governance; IT Management; Informal controls; Self-control.

1 INTRODUCTION

In an ideal scenario, all business needs related to Information Technology (IT) would be met and the full potential of IT would be available to users. However, meeting this demand, and sustaining it over time, is a seemingly impossible task (Cleven, 2011).

When IT solutions do not cater to business processes, users tend to create stand-alone solutions outside the formal structure of IT management so they can perform their tasks more efficiently. This type of solution is called Shadow IT or SIT (György et al., 2012).

Kopper and Westner (2016) argue that there are a number of factors that drive users to develop solutions on their own. These include the rigidity of IT systems, the ease of use and the low complexity of development tools, as well as the lack of restrictions on the adoption of solutions. In all cases, the non-fulfillment of users' needs demonstrates a misalignment between IT and business, representing an issue related to IT governance (György et al., 2012; Zimmermann & Rentrop, 2014).

For Peterson (2004), in order to achieve greater return of investments made in the area, effective IT governance is achieved through the mix of structural, procedural and relational mechanisms. Thus, the classic approach to IT governance is related to control and compliance (Weill & Ross, 2004; Damianides, 2005). This idea is aligned with the notion of activity regulation and monitoring, and seeks to elucidate which rules and monitoring mechanisms, through an organizational hierarchy, could be used for the company to achieve its objectives (Ouchi, 1979; Kuhlmann, 2012).

In this line, Kirsch (1996) states that control has two dimensions, formal and informal. The formal dimension has two types, the result and the control of the behavior. The informal dimension, however, deals with clan modes and self-control. Thus, the alignment of the IT governance framework proposed by Peterson (2004), would come from the dimensions of formal control, with structural and procedural mechanisms, and the informal dimension, with the relational mechanism. From that it is possible to verify that the proposed framework does not treat, separately, the relational issues between the members of the organization and the individual's self-control.

However, György et al. (2012) and Zimmermann and Rentrop (2014) suggest that a possible approach to treat SIT-like solutions would be to transfer control of parts of the technology park to the user or to a business unit. Thus, among the informal governance controls, mechanisms of self-control would be added to the relational mechanisms.

Self-control is defined as the establishment of personal goals and monitoring to achieve these goals. It is important to remember that it does not mean lack of control, only the implementation of mechanisms to support self-control (Jaworski, 1988; Choudhury & Sabherwal, 2003; Liu, 2015).

In view of the aforementioned framework, it is necessary to develop approaches that measure and manage IT, seeking mechanisms that promote effective IT governance. Thus, the present theoretical essay discusses such approaches, and suggests the addition of a dimension of self-control to the IT governance framework proposed by Peterson (2004).

The present theoretical essay is organized from this introduction, which outlined the initial topics of the subject. Then, in order to construct the theoretical body of research, the

concepts of Shadow IT (SIT), control in organizations and IT governance will be discussed. In the third section, the theoretical construct proposed in this essay will be presented. Finally, the conclusions of the study are presented.

2 THEORETICAL FOUNDATION

2.1 Shadow IT (SIT)

Shadow IT is a recurring phenomenon in organizations, but its definition remains the object of divergence in the literature. In a recent systematic review, Magunduni and Chigona (2018) present different terms related to SIT*:* “Shadow Systems”, “Feral Practices”, “Workarounds”, “Un-enacted projects” and “Shadow Sourcing”. The same authors also report that there are studies that refer to SIT as an information system, while others define it as an unofficial project. However, one element in common is the understanding that SIT is implemented directly by the business units, without the involvement or approval of the IT department.

Shadow IT can be considered an "internal threat" in which a non-malicious agent (employee) installs unapproved software, in disagreement with information security policies (Warketin & Willison, 2009). Not all authors, however, classify Shadow IT directly as a threat. György et al. (2012), for example, treat noncompliant user innovations as security threats, but distinguishes situations in which SIT is intentionally made to support a business process and not to cause malicious economic damage.

The dissatisfaction with systems approved by the organization is pointed out as the main cause for the implementation of SIT, as well as lack of confidence (Carlos & Apacada, 2016). This dissatisfaction stems from the misalignment between IT department objectives and functional department goals (GYÖRY et al., 2012). ERP systems are an example of this. Much of the literature on the subject advocates that a "vanilla" implementation, that is, without customizations, is one of the factors that contributes to ERP success (Shaul & Tauber, 2013; Bertram, 2016). Success, in this perspective, is related to the fulfillment of the schedule and budget defined for the project (Dwivedi et al., 2014). From the point of view of end users, however, the lack of customizations may mean that features essential to the business process will not be available (Magunduni & Chigona, 2018). And even when features are available, they are often difficult to use (Behrens, 2009). Thus, a favorable scenario for the implementation of SIT is created. In addition, increased end-user technical knowledge coupled with ease of access to cloud-based solutions (Zimmermann & Rentrop, 2014; Gozman & Willcocks, 2015) contribute to the dissemination of the practice.

Research on the implications of SIT presents contradictory evidence. Although it is generally associated with risk, it is also argued that it can be beneficial to organizations (Behrens, 2009; Silic, 2015). Among the benefits, we can mention: increasing the creativity and innovation of the end users and improving the performance of the business. On the other hand, there are multiple risks, such as compromising the privacy and confidentiality of the organization's data and the difficulty of maintaining and supporting the SIT solutions, caused by the absence of documentation (Behrens, 2009).

Because of the risks presented, some researchers have suggested ways to manage and control SIT. Shumarova and Swatman (2008), for example, suggest three ways to deal with the phenomenon: companies can allow end users to implement SIT; can devise a strategy to restrict SIT implementation; or can regulate SIT through IT policies. Gory and others (György et al., 2012) advocate a strict IT security policy, considering that their noncompliance can be catastrophic for the company. Silic and Back (2014) suggest identifying SIT as an alternative path for IT managers, since an already identified solution would offer less risk than an unknown solution.

Thus, reflecting on possible ways to deal with the SIT phenomenon in organizations requires exploring the concepts of IT governance and governance. Thus, these topics are addressed in the following sections.

2.2 Control in organizations

The control in organizations has different nuances. However, the concepts of domination of an individual or group of individuals through the exercise of power or the regulation and monitoring of activities are the most present ideas (Otley & Berry, 1980; Kuhmanman, 2012).

For Ouchi (1979), control is a matter of information flow. The central point is to define what rules and mechanisms of monitoring, through an organizational hierarchy, could be used for the company to achieve its objectives.

Thus, organizational control can be defined as the attempt to regulate the behavior of individuals or groups, through mechanisms, to ensure that they contribute to organizational goals (KUHLMANN, 2012).

Control mechanisms can be classified as formal and informal. Formal controls include rules, standards and targets visible and implementable from centralized management. On the other hand, informal controls are not explicitly designed and are usually derived from the cultural aspects of the organization (Langfield-Smith, 1997; Kuhmanman, 2012; Di Tullio & Staples, 2013).

Concurrently, Kirsch (1996) states that control has two dimensions, formal and informal. The formal dimension has two types: the result, which involves aspects of performance and completeness of tasks; and behavior control, which deals with desired behaviors from defined and controllable processes. The informal dimension deals with the clan mode, involving mechanisms for creating common goals, and the self-control mode, addressing personal aspects of self-monitoring, empowerment and autonomy (Di Tullio & Staples, 2013).

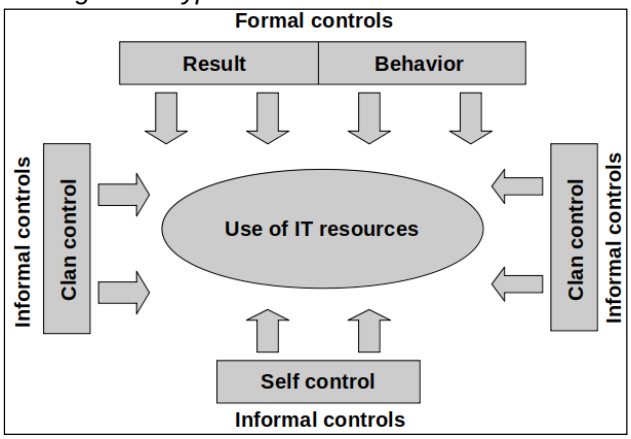
As opposed to the formal dimension, in which the outcome of a task must be known and measurable or rules and procedures to be followed and observable, the informal dimension has no specified behavior or results. The clan defines acceptable behaviors through a set of beliefs, values, and social norms. Thus, in situations where it is not possible to measure outcome or compliance with process standards, clan control has the ability to maintain integrity and adherence to norms shared by group members (Srivastava & Teo, 2012).

In addition, the self-control mechanism has a personal aspect, of self-imposed norms and personal motivation, being, therefore, of difficult implementation or imposition from a deliberate context of control tools. However, it is possible to establish work environments that facilitate this type of control by valuing the intrinsic motivation and the reward for the ability to self-manage (Srivastava & Teo, 2012; Di Tullio & Staples, 2013).

Managing organizational control in situations where users develop their own solutions is an important issue for achieving effective IT governance (Zimmermann, Rentrop, & Felden, 2014). György et al. (2012) propose the alternative in which the organization retains much of the control, but part of this control is passed to the user.

Thus, there would be a scenario in which all mechanisms would be involved, with defined roles. Formal mechanisms would act to control core resources from a top-down perspective in the organization, while clan mechanisms would act to control users so that unenforceable or unsafe solutions would be discarded. Finally, the self-control mechanisms would act to create solutions that are really necessary and to diffuse them when used successfully. The relationships between control types and the use of IT resources can be seen in figure 1.

Figure 1: Types of controls and IT resources



Source: based on György et al. (2012) and Kuhlmann (2012).

2.3 IT Governance

IT governance has origins in corporate governance. Over the years its definition has undergone a series of adjustments and additions. Currently, IT governance is defined as the specification of decision-making rights and accountability on information technology, so that desirable behaviors by the IT manager are encouraged (Weill & Ross, 2004; Lunardi et al., 2014, Bergeron et al., 2017).

For Silva, Araújo and Dornelas (2018) IT governance is the responsibility of the company's management, and cannot be left only to the IT team, since it deals with the definition of processes that can guarantee support to organizational objectives and strategies.

The theoretical framework traditionally used to analyze the phenomenon of IT governance is agency theory (Lunardi, 2008). The focus of this theory is the problems of

agency, which arise when managers aim to maximize personal utility rather than maximizing the return on the principal's investments (Jensen & Meckling, 1976).

However, Van Puyvelde et al. (2012) propose that Stewardship theory be used as a complement to agency theory, since even when the interests of the principal and agent are not aligned, the agent could act maximizing the interests of the principal since, in doing so, it would be seeking personal goals as personal achievements, improvement in relation to the main and self-realization.

Both theories, Stewardship theory and agency theory, would complement the understanding of governance (Van Puyvelde et al., 2012). In particular, dealing with IT governance and autonomous IT solutions, it is necessary to provide elements that allow these informal structures to be controlled and redesigned within the organization's governance (Zimmermann, Rentrop, & Felden, 2014).

For Peterson (2004), effective IT governance could be achieved through the use of structural, procedural and relational governance mechanisms, shown in table 1. Each of these mechanisms used in a formal or informal way can help the organization to obtain of the best results in the use of information technology resources (Lunardi et al., 2010).

Table 1: IT Governance Mechanisms

Structures	Process	Relational Mechanisms
• Roles and responsibilities • IT Strategy Committee • IT Steering Committee • IT organizational structure • CIO on the board of directors • IT Projects Committee • Project Office	• IT Performance Indicators • Strategic planning of information systems • COBIT; ITIL • Service Level Agreements • Methods of evaluating return on investment • Levels of alignment	• Active participation of key stakeholders • Collaboration among key stakeholders • Formal communication practices • Shared understanding of IT and business objectives • Inter-functional training between IT and business • Rotating IT and Business Tasks

Source: adapted from Peterson (2004)

3. THEORETICAL CONSTRUCT

György et al. (2012) propose three approaches to address the Shadow IT phenomenon within IT governance. The first would be to control IT, more traditional and aligned with the framework proposed by Peterson (2004), which is based on central control and compliance, not allowing the user to innovate, making the IT department always organizational needs. The second, user-driven approach alters the responsibility of IT innovations to the user while being extremely open to risk. Finally, the third, user-oriented approach aims to use the best of each of the above, controlling IT and absorbing the best solutions to business problems that have not yet been perceived by IT managers, and that is the approach that is proposed in the present work.

Although it is widely recommended in the IT Governance literature (Weill & Ross, 2004; Bradley et al., 2012; Lunardi et al., 2014), the relational dimension present in the framework proposed by Peterson (2004) seems to be insufficient to aggregate the autonomous IT solutions in the organization's body of governance, so that these become part of the organizational IT portfolio.

This relational dimension of IT governance includes elements such as the IT sector manager's leadership capacity, mutual learning that takes place between IT and business, and communication between the parties (Bradley et al., 2012; Wilkin, 2012; Wu, Straub, & Liang, 2015). Thus, these are elements that are present at the organizational relational level, and can thus be included in forms of clan control, as proposed by Langfield-Smith (1997) and Kuhlman (2012).

As for self-control, it acts on a different level of clan control. Self-control in the present work can be understood as the establishment of personal goals, monitoring the achievement of these goals and behavioral adjustments so that it is possible to fulfill what was established. It is important, however, to be clarified that self-control does not mean no control (Jaworski, 1988; Choudhury & Sabherwal, 2003; Liu, 2015).

Thus, mechanisms that support self-control are implemented, primarily, by the controlled. These mechanisms include behavior patterns, goal setting, and deadlines to be met. Nonetheless, the part of the relationship that establishes the formal mechanisms of control may also encourage or enable the controlled to exercise self-control (Choudhury & Sabherwal, 2003).

However, despite the possible success of using self-control in the governance of autonomous information technology solutions (Liu, 2015), external incentives to people, which are composed of other forms of formal control, must be present so that the desired behavior is achieved (Jaworski, 1988). Thus, IT governance, which allows the inclusion of solutions developed by users or groups of users, should be composed of formal elements, structures and processes, and informal elements, relational mechanisms and self-control.

Thus, based on the proposition of user-oriented governance mechanisms proposed by György et al. (2012) and the portfolio of organizational control mechanisms presented by Kuhlman (2012), it is possible to suggest an additional dimension to the framework of governance mechanisms proposed by Peterson (2004), referred to here as self-control. This dimension would encompass practices related to how users can aggregate new tools to the IT portfolio, valuing the intrinsic motivation of the user and rewarding for the ability to self-manage. The proposed framework is shown in table 2.

Table 2: Proposed IT Governance Mechanisms

Structures	Process	Relational Mechanisms	Self control
• Roles and responsibilities • IT Strategy Committee • IT Steering Committee • IT organizational structure • CIO on the board of directors • IT Projects Committee • Project Office	• IT Performance Indicators • Strategic planning of information systems • COBIT; ITIL • Service Level Agreements • Methods of evaluating return on investment • Levels of alignment	• Active participation of key stakeholders • Collaboration among key stakeholders • Formal communication practices • Shared understanding of IT and business objectives • Inter-functional training between IT and business • Rotating IT and Business Tasks	• Incentives and rewards • Recognition • Sense of autonomy • Empowerment

Source: based on Peterson (2004), Kuhlman (2012) and György *et al*. (2012)

4. CONCLUSION

The SIT phenomenon has attracted the interest of several researchers in recent decades and represents a challenge for the classic approach to governance, based on constraints and compliance requirements. In this article, we tried to relate the concept of Shadow IT to the issues of organizational control and IT governance. Far from facing SIT as a threat simply, the idea presented here contemplates the possibility of transforming it into a source of organizational innovation. However, it is understood that this operation is not free of risks, which implies the need to implement governance mechanisms that can protect the organization from losses.

In this sense, the present work suggests the expansion of the theoretical body of IT governance already established in the area, based on the framework proposed by Peterson (2004), to contemplate the dimension of self-control. Thus, the control mechanisms to be used in the organization would cover formal and informal elements.

As proposed by György et al. (2012), the impossibility of total control of the solutions developed by users requires that a certain level of control be passed on, thus allowing innovation that is not glimpsed by the information technology team. However, in order to achieve the appropriate level of control, formal governance mechanisms, structures, and procedures need to work together with informal mechanisms, such as self-control.

In this way, stimuli would be established for the innovation, while at the same time it would reach the organizational consciousness in relation to the autonomous IT solutions in use, stimulating the return of solutions that can contribute to a better organizational performance and cooperation between the organization and the employee.

Controlling what is being performed on users' devices, or through Internet sites, or personal electronic spreadsheets, has been an arduous task and the contribution of the user can be the alternative for the aggregation of innovative solutions and great potential.

REFERENCES

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. Communications of the ACM, 52(2), 124-129.

Bertram, M. (2016). Introduction: The neglected role of customization for software product management. In: The Strategic Role of Software Customization (pp. 1-39). Springer Gabler, Wiesbaden.

Bradley, R. V., Byrd, T. A., Pridmore, J. L., Thrasher, E., Pratt, R. M., & Mbarika, V. W. (2012). An empirical examination of antecedents and consequences of IT governance in US hospitals. Journal of Information Technology, 27(2), 156-177.

Choudhury, V., & Sabherwal, R. (2003). Portfolios of control in outsourced software development projects. Information systems research, 14(3), 291-314.

Cleven, A. (2011, June). Exploring patterns of business-IT alignment for the purpose of process performance measurement. In ECIS (p. 19).

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. Information Systems Management, 22(1), 77-85.

Di Tullio, D., & Staples, D. S. (2013). The governance and control of open source software projects. Journal of Management Information Systems, 30(3), 49-80.

Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., ... & Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. Information Systems Frontiers, 17(1), 143-157.

Gozman, D., & Willcocks, L. (2015). Crocodiles in the regulatory swamp: navigating the dangers of outsourcing, SaaS and shadow IT.

Györy, A. A. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012, June). Exploring the shadows: IT governance approaches to user-driven innovation. Association for Information Systems.

Jaworski, B. J. (1988). Toward a theory of marketing control: environmental context, control types, and consequences. Journal of Marketing, 52(3), 23-39.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of financial economics, 3(4), 305-360.

Kirsch, L. J. (1996). The management of complex tasks in organizations: Controlling the systems development process. Organization science, 7(1), 1-21.

Kopper, A., & Westner, M. (2016). Deriving a framework for causes, consequences, and governance of shadow it from literature. MKWI 2016 Proceedings, 1687-1698.

Kuhlmann, D. (2012). Governing IT Outsourcing Relationships: The Roles of Contract, Control, and Relational Norms. Diplomica Verlag.

Langfield-Smith, K. (1997). Management control systems and strategy: a critical review. Accounting, organizations and society, 22(2), 207-232.

Liu, S. (2015). How team risk and planning and control risk moderate the effects of clan and self control on the process performance of IT projects: the perspective of user liaisons. Information Development, 31(1), 27-39.

Lunardi, G. L. (2008). Um estudo empírico e analítico do impacto da governança de TI no desempenho organizacional. Tese. Porto Alegre, UFRGS. 2008.

Magunduni, J., & Chigona, W. (2018, March). Revisiting shadow IT research: What we already know, what we still need to know, and how do we get there?. In 2018 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-6). IEEE.

Myers, N., Starliper, M. W., Summers, S. L., & Wood, D. A. (2017). The impact of shadow IT systems on perceived information credibility and managerial decision making. Accounting Horizons, 31(3), 105-123.

Otley, D. (2016). The contingency theory of management accounting and control: 1980–2014. Management accounting research, 31, 45-62.

Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. Management science, 25(9), 833-848.

Peterson, R. (2004). Crafting information technology governance. Information systems management, 21(4), 7-22.

Shaul, L., & Tauber, D. (2013). Critical success factors in enterprise resource planning systems: Review of the last decade. ACM Computing Surveys (CSUR), 45(4), 55.

Shumarova, E., & Swatman, P. A. (2008). Informal eCollaboration Channels: Shedding Light on" Shadow CIT". BLED 2008 Proceedings, 18.

Silic, M. (2015). Shadow it–Steroids for Innovation. Available at SSRN 2633004.

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. Computers & Security, 45, 274-283.

Silva, H. C. C., Araújo, M. A. V., & Dornelas, J. S. (2018). Determinantes da não utilização de frameworks de gestão e/ou governança de TI. Revista Gestão & Tecnologia, 18(2), 271-296.

Srivastava, S. C., & Teo, T. S. (2012). Contract performance in offshore systems development: Role of control mechanisms. Journal of Management Information Systems, 29(1), 115-158.

Van Puyvelde, S., Caers, R., Du Bois, C., & Jegers, M. (2012). The governance of nonprofit organizations: Integrating agency theory with stakeholder and stewardship theories. Nonprofit and voluntary sector quarterly, 41(3), 431-451.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2), 101-105.

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Wilkin, C. (2012). The role of IT governance practices in creating business value in SMEs. Journal of Organizational and End User Computing (JOEUC), 24(2), 1-17.

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. Mis Quarterly, 39(2), 497-518.

Zimmermann, S., & Rentrop, C. (2014). On the emergence of shadow IT-a transaction cost-based approach. Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0.

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing shadow IT instances–a method to control autonomous IT solutions in the business departments. Twentieth Americas Conference on Information Systems, Savannah.