Shadow IT Management Concept for Public Sector

Lada Šedivcová (nesvedová), Martin Potančok

▶ To cite this version:

Lada Šedivcová (nesvedová), Martin Potančok. Shadow IT Management Concept for Public Sector. 13th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS), Dec 2019, Prague, Czech Republic. pp.65-73, 10.1007/978-3-030-37632-1_6 . hal-03408392

HAL Id: hal-03408392

https://hal.inria.fr/hal-03408392

Submitted on 29 Oct 2021

Shadow IT Management Concept for Public Sector

Lada Šedivcová (Nesvedová)[1[0000-0003-2768-859X]] and Martin Potančok[1[0000-0002-7613-9290]]

[1] University of Economics, Prague 130 67, Czech Republic
lada.sedivcova@gmail.com

Abstract. Shadow IT represents a software, hardware, or any other solution used by employees within organizations that has not received any prior formal approval from the IT department to be used. Currently, the issue of Shadow IT is increasingly under discussion and is beginning to be explored in the private sector. However, this issue is not addressed comprehensively in the public sector. The main aim of this paper is therefore to propose a Shadow IT management concept for the public sector. The proposal of Shadow IT management concept identified problematic areas related to Shadow IT discovered during a case study in connection with the main aim of the paper. There are 7 areas designated as A1 to A7. The recommended approaches and solutions are set for these problem areas. Shadow IT Management Concept was created based on the case study (including interviews with main stakeholders).

Keywords: Enterprise IT management, Management Concept, Shadow IT

1 Introduction

Shadow IT is a software, hardware, or any other solution used by employees within organizations that has not received any prior formal approval from the IT department to be used [1]. The issue of Shadow IT is currently under discussion and is beginning to be explored in the private sector [2]. However, this issue is not addressed comprehensively in the public sector.

According to Gartner [3], up to one third of investments in IT development are managed and funded outside the IT department and its budget. This is very often caused by cloud solutions or mobile applications. These are services that are immediately available and can therefore be relatively easily deployed without IT expertise. On the one hand, Shadow IT can be an innovative element that pushes companies into new technology solutions [4], but on the other hand it can also be a source of trouble if solutions are provided outside the IT department without being informed by IT department managers and not following strategies and official procedures [5].

Nowadays, employees can bring their own devices into the corporate environment. This trend is known as Bring Your Own Device (BYOD). Some of the applications that employees can bring might be a disruption to the entire infrastructure and vulnerability of the agenda system and intrusion into the internal network may occur [6].

Therefore, it is essential that BYOD policy is implemented and it does not cause Shadow IT.

Furstenau also emphasizes the importance of the issue: *“Shadow IT is becoming increasingly important as digital work practices make it easier than ever for business units crafting their own IT solutions.“* [5] For IT departments, it is necessary to determine when users decide to implement the Shadow IT process and start to manage this process [7]. IT as such, including infrastructure (hardware, software, network resources and other services that are interconnected), should be developed, managed and controlled by the IT department [8]. Furstenau [9] states in his study that the most common problems are architectural. More than half of the systems may suffer from inconsistent data, non-scalable technical platforms, unstable servers, or hardware components. The architecture of IS/ICT is, according to Bruckner [10], very important, as it creates a relatively stable IS/ICT solution framework. It constitutes a means of communication, ensures the stability of IS/ICT development, takes into account the requirements for IS/ICT properties and allows to minimize the costs of incorrectly assigned projects. One of the most widely used frameworks in practice are ITIL, TOGAF and Zachman. For example, ITIL is a set of business information management practices through services. It is a library of more than 40 volumes published by the British government agency CCTA in 2013 [11], but currently belongs to AXELOS [12].

Despite its complexity, ITIL does not provide sufficient coverage for Shadow IT. The topic has been addressed by several authors, e.g. Pettey [13], Silic et al. [1], Zimmermann [14], but only with the application to the private sector. In the private sector, companies are able to deal with the issue in different ways, but the public sector seems to be an interesting issue. This is mainly due to the impossibility of immediate intervention. Public administration processes do not allow flexible responses to required changes. [15] In the case of public organizations, this topic has not been comprehensively addressed and is therefore an interesting area for research.

For these reasons, the main aim of the paper is to propose a Shadow IT management concept for the public sector.

2 Methodology

Shadow IT Management Concept was created based on a case study, partial results for one type of public organization [16], the Multidimensional Management and Development of Information Systems (MMDIS) [10] and Management of Business Informatics (MBI) [17] models. Different organizations from the public sector were selected for the case study. For the purposes of the case study, higher local government units - regional authorities were addressed. The Vysocina Regional Authority showed the greatest interest in the outputs of the case study and also provided documents that are not publicly available. Close cooperation took place especially with the head of the department of informatics.

As part of the case study, interviews with stakeholders (employees, managers, IT employees and IT managers) were conducted. Respondent groups were distinguished by job position - managerial level in the IT field, positions on managerial level in another field and positions that are not on any of the previous ones (these are positions of common end users, e.g. clerk, accountant, lawyer, etc. The total number of respondents was 35, of which 9 were men and 26 were women. The average length of one interview was 60 minutes. The beginning of each interview was unstructured to get as much information and as many opinions and information on organizations from the public sector as possible, followed by a semi-structured part with questions about Shadow IT. Other sources of information included strategies of organizations and their structures. The research is fully consistent with the definition of a case study as a qualitative research method within the exploratory and theory-building phase presented by [18] and [19]. The structure of this paper corresponds to the above.

3 Shadow IT criteria and reasons for existence

3.1 Shadow IT criteria

Since employees (users) can ignore the central IT system, the performance of the specific organizational units of the public sector may be influenced.

According to Rentropa and Zimmermann [14], the so-called evaluation model is used for systematic quality assessment and Shadow IT evaluation criteria. It is therefore appropriate to clarify this model in the case of Shadow IT to find ways to map and respond to the occurrence of Shadow IT. The evaluation model will be used to formulate questions for the interview, which is one of the selected collection methods in our case study.

To define Shadow IT criteria, it is necessary to identify specific Shadow IT cases and associated organizational processes in the first step. These instances are then analysed and evaluated. This evaluation makes it possible to establish basic control over the Shadow IT and to draw up effective strategies to control the Shadow IT. Because this model is developed for the Shadow IT mapping in the private sector, it has been adapted for the public sector to cover specifics and influencing this sector [20]. Evaluation criteria based on [14] are presented in Table 1 and are further described below.

Table 1. Shadow IT criteria, based on [14]

Criterion	Sub-criterion	Sub-criterion
Relevancy	Strategic relevance	
	Criticality	Business processes
		IT security
		Compliance
		IT services management
Quality	System quality	Software
		Technical processes
	Quality of services	
	Quality of information	
	Quality of processes	
Size	Utilization of resources	
	Number of users	
	Shadow IT components	
Innovative potential		
Parallel		

C1 Relevancy

This criterion described Shadow IT along with its relevance to the organization's processes. It carries value and risks. This criterion is therefore subdivided into sub-criteria. 1) Strategic importance is necessary to assess how strong the impact on the region's strategy and strategic decisions regarding IT infrastructure is. 2) Criticality: the use of Shadow IT can influence several things, such as IT security risk, compliance, and inefficiencies in business and business processes. Significance in erratic behaviour brings a degree of risk in many areas. This sub-criterion relates specifically to business processes, IT security, IT service management at different levels of criticality.

C2 Quality

This is an important criterion for assessing the quality of Shadow IT. It refers to the technical quality of the system itself, the quality of IT services and the information generated. These main dimensions of quality represent the success of information system research. On the other hand, it is also necessary to look at the quality of processes where there is a potential occurrence of Shadow IT.

In the case of Shadow IT, it is the quality of hardware and software and the quality of process creation and design. Quality can be defined by models such as Capability Maturity Model Integration (CMMI) [21] or other standards.

Quality of service is a criterion that occurs in the context of Shadow IT, especially for IT department services. The quality of services can be evaluated e.g. on the basis of ITIL [22]. Thanks to best practices in IT service management, existing processes can be better managed, monitored, measured, evaluated and continually improved.

C3 Size
The size criterion can be used to estimate the extent of the Shadow IT in an organization. The size of Shadow IT refers to the use of Shadow IT resources and expertise, distribution and penetration with components and service services. Partial criteria are: 1) Use of resources and professionalism. 2) Number of users. 3) Shadow IT components. 4) Service processes.

C4 Innovative potential
It is necessary to assess the innovative potential of the Shadow IT. On the one hand, Shadow IT offers the opportunity to introduce new technologies or improve processes in the research environment. On the other hand, Shadow IT may not be technologically suitable.

C5 Parallel
The parallel is an important criterion that assesses how Shadow IT runs in parallel to an existing, official IT system. This means how the identified Shadow IT replaces the official IT solution in the departments where it is used. It may also be the case that Shadow IT complements the IT system.

3.2 Reasons for existence

The authors define various reasons for the existence of Shadow IT and therefore this chapter analyses reasons from multiple source regardless of the industry.

According to Bayan [23], the reasons are as follows: 1) Shadow IT is enforced due to a pressure to significantly reduce IT spending and an increasing demand for IT solutions for infrastructure problems. These pressures lead to a growing IT volume of unfinished projects. It is necessary to respond to the needs of other departments, many of which depend on IT projects to achieve the goals of the organization. 2) Shadow IT is a solution for specific needs. In some cases, these needs must be met quickly. Also, the return on initial investment pushes the department to realize shadow projects. This is partially because initial investments do not address the project lifecycle, support or infrastructure costs. 3) Shadow IT is stimulated by the fact that Shadow IT solutions seem faster. Some departments are pushing the IT department because they believe that another employee would do the job faster and without some of the IT department's demands.

Author Hulsebosch [24] sees the reasons for the emergence of Shadow IT as follows: 1) Business and IT weaknesses due to a lack of communication between them. Lack of communication leads to a mismatch between users and IT providers in the environment, leading to a decision as to whether the cost of resolving this issue is lower than the cost of circumventing it. 2) The absence of an official solution due to various binding documents or laws, some IT solutions are not possible, which may lead to recourse to the Shadow.

A combination of different facts leads to the emergence of specific Shadow IT. Individual causes of Shadow IT are closely related to the management of the whole organization or IT department. Due to inefficient processes associated with the required solution, mismatch between IT and business departments, or new policies in the organization, the potential incidence of Shadow IT increases. An example of a typical Shadow IT product is cloud-based SaaS (Software as a Service). [6]

In his study, Hulsebosch [24] lists categories that identify the reasons for Shadow IT. Particularly speaking about 1) No official IT solution. 2) The official solution is not extensive enough. 3) Official IT solution is not easily accessible. 4) The official solution is perceived as more expensive. 5) Employees are too strict. 6) Employees underestimate the risks. 7) It is very easy to use Shadow IT and opportunities are created for employees to use it.

4 Shadow IT management concept

The proposal of Shadow IT management concept contains problematic areas related to Shadow IT, which were discovered during the case study in connection with the main aim of the paper. There are 7 areas designated as A1 to A7. The recommended approaches and solutions are set for these problem areas.

The model is inspired by MMDIS [10] and MBI [17] models and methodologies. Both concepts define the process from global goals to the design of individual informat projects. Based on the content analysis of the documents, it is a simplified model similar to those of the regions mentioned in their strategic plans. The model is complemented by Shadow IT problem areas, which are coloured in red. These areas are marked A1 to A7, which are further detailed.

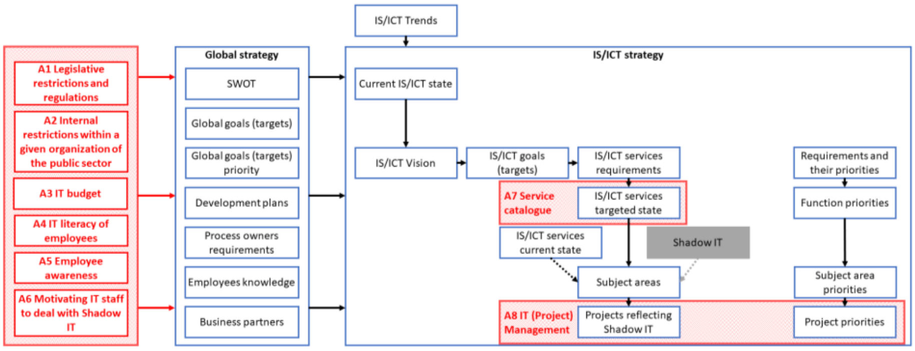
IS/ICT Trends
A1 Legislative restrictions and regulations
A2 Internal restrictions within a given organization of the public sector
A3 IT budget
A4 IT literacy of employees
A5 Employee awareness
A6 Motivating IT staff to deal with Shadow IT
Global strategy
SWOT
Global goals (targets)
Global goals (targets) priority
Development plans
Process owners requirements
Employees knowledge
Business partners
IS/ICT strategy
Current IS/ICT state
IS/ICT Vision
IS/ICT goals (targets)
IS/ICT services requirements
A7 Service catalogue
IS/ICT services targeted state
IS/ICT services current state
Shadow IT
Subject areas
A8 IT (Project) Management
Projects reflecting Shadow IT
Requirements and their priorities
Function priorities
Subject area priorities
Project priorities

Fig. 1. Shadow IT management concept

A1 Legislative restrictions and regulations

The IT department has to take into account legislative restrictions and regulations when developing its own internal procedures. All internal employees must then follow these internal procedures. Since it contains various orders and prohibitions, it is necessary to take into account the needs of its employees in its creation, thus eliminating the risk of Shadow IT occurrence. The recommendation is to actively make comment in the legislative process.

A2 Internal restrictions within a given organization of the public sector

Protection of the internal network and official architecture is a priority for the public sector. Especially due to cloud storage, data leakage or loss may be imminent and therefore these tools (SaaS) are prohibited in public administration. If the IT department is able to respond to employees' requests in time, potential use of Shadow IT can be avoided. The IT department should meet the demands of employees or entire departments. It should be the initiator of the change and achieve it by working with employees outside its department.

A3 IT budget

With a sufficient IT budget, Shadow IT detection tools, security assurance and tools that eliminate the occurrence of Shadow IT can be acquired or developed. These may be, for example, licenses of programs that are often used by employees but not authorized by the IT department.

A4 IT literacy of employees

IT employees might be trained by organizing or attending trainings and seminars on different topics. Furthermore, it is also necessary to motivate employees to attend this training. Training areas can vary according to the identified threats, such as security training from the SW and HW point of view (related BYOD issues) and strong instruction on internal regulations. Internal regulations should be available to all employees and it should never happen that the CIO does not inform their employees about these regulations.

A5 Employee awareness

It is important that CIO or IT department should always inform employees about how the IT requirements management is addressed and where to find all the supporting documents, internal regulations, etc. Within this staff policy, training and development policies can be set, both in managerial positions and in other subordinate positions. Various sources are used to determine the level of employee awareness. Examples include questionnaires, observations, task analyzes, etc. [25]

A6 Motivating IT staff to deal with Shadow IT

The motivation of existing workers can be addressed based on various techniques that fall within the psychological theme. An example of the neglected component of motivation of human behavior may be based on the well-known Maslow's pyramid of needs [26]. Typical incentives for work motivation according to Růžička [27] include: work evaluation, group evaluation (appreciation of performance of a given employee by appreciation, respect, etc.), working conditions, financial reward, possibility of independent work.

A7 Service catalogue
There should be a catalogue of ICT services. There are clear rules for managing operations and developing services. [28] The most important rules are: 1) Each service must have its own administrator, technical administrator and operator. 2) Clear rules must be in place, based on a binding and approved service architecture. 3) It is necessary to monitor investment and operating costs of individual services. It is also necessary to monitor the scope and quality of these services. In connection with the Shadow IT, it is also appropriate to measure employee satisfaction with the services - whether they adequately cover their needs.

A8 IT (project) management
If an analysis of needs and setting new goals in the field of IT (in response to the elimination of the occurrence of Shadow IT) is to be created, it is essential to define whether the project management of the given region is functionally or process-oriented. The demands on IT management arise mainly from the economic, business and operational needs of the region, along with the new possibilities of ICT. Pressure on the performance of IT has lead to the emergence of various methodologies and models. The previously mentioned ITIL library is one of the procedures for informatics management that can be used.

5 Conclusion

The main aim of the paper was to propose a Shadow IT management concept for the public sector. The proposal of Shadow IT management concept contains problematic areas related to Shadow IT, which were discovered during the case study in connection with the main aim of the paper.

There are 7 areas designated as A1 to A7 (legislative restrictions and regulations, IT budget, IT literacy of employees, employee awareness, motivating IT staff to deal with Shadow IT, service catalogue, IT management). The recommended approaches and solutions are set for these problem areas.

The proposed Shadow IT Management concept should be used by public sector organizations to work effectively with Shadow IT and above all to eliminate risks.

6 Acknowledgements

This paper was written thanks to the long-term institutional support of research activities by the Faculty of Informatics and Statistics, University of Economics, Prague.

7 References

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

2. Raden N (2005) Shedding light on shadow IT: Is Excel running your business. DSSResources com 26:
3. Grásgruber L (2015) Role IT oddělení a jeho manažera se mění | IT Visions. In: ITVisions.cz. http://www.itvisions.cz/2015/10/role-it-oddeleni-a-jeho-manazera-se-meni/. Accessed 20 Sep 2019
4. Silic M, Back A (2014) Shadow IT–A view from behind the curtain. Comput Secur 45:274–283
5. Fürstenau D, Rothe H (2014) Shadow IT systems: discerning the good and the evil
6. Zatřepálek T (2016) Analýza problematiky stínového IT. České vysoké učení technické v Praze. Vypočetní a informační centrum.
7. Chua C, Storey V, Chen L (2014) Central IT or shadow IT? Factors shaping users' decision to go rogue with IT
8. Voříšek J, Basl J, Buchalcevová A, et al (2008) Principy a modely řízení podnikové informatiky. Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, Praha
9. Fürstenau D, Sandner M, Anapliotis D (2016) Why do shadow systems fail? An expert study on determinants of discontinuation
10. Bruckner T, Voříšek J, Buchalcevová A (2012) Tvorba informačních systémů; Principy, metodiky, architektury. Grada Publishing, a.s., Praha
11. Gála L, Pour J, Toman P (2006) Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. Grada, Praha
12. Axelos (2019) About AXELOS. https://www.axelos.com/about-axelos. Accessed 20 Sep 2019
13. Pettey C (2016) Don't Let Shadow IT Put Your Business at Risk - Smarter With Gartner. https://www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/. Accessed 3 Nov 2019
14. Rentrop C, Zimmermann S (2012) Shadow IT evaluation model. In: 2012 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, pp 1023–1027
15. Zákon (2000) Zákon č. 129/2000 Sb. o krajích (krajské zřízení)
16. Šedivcová (Nesvedová) L (2017) Návrh metodického postupu pro práci s Shadow IT ve veřejné správě na úrovni krajů České republiky. Vysoká škola ekonomická v Praze
17. MBI (2015) MBI - Management of Business Informatics. In: Manag. Bus. Informatics. http://mbi.vse.cz/. Accessed 29 Nov 2015
18. Myers MD (2013) Qualitative Research in Business & Management, 2nd ed. Sage, London
19. Yin RK (2009) Case study research: Design and methods, 4th ed. Sage publications, Thousand Oaks
20. Stemberger MI, Jaklic J (2007) Towards E-government by business process change—A methodology for public sector. Int J Inf Manage 27:221–232
21. Clerc V, Niessink F (2004) IT Service CMM: A Pocket Guide. Van Haren Publishing
22. ITIL (2007) spri. The Stationery Office (TSO), London

23. Bayan R (2004) Shed light on shadow IT groups. techrepublic.com 9:
24. Hulsebosch MAC (2016) Cloud Strife: an analysis of cloud-based shadow IT and a framework for managing its risks and opportunities
25. Kocianová R (2010) Personální činnosti a metody personální práce. Grada Publishing a.s., Praha
26. Simons JA, Irwin DB, Drinnien BA (1987) Maslow’s hierarchy of needs. Retrieved Oct 9:2009
27. Růžička J, Nový I, Provazník V (1993) Řízení profesní kariéry zaměstnanců. Vysoká škola ekonomická
28. Vláda ČR (2015) Usnesení vlády České republiky č. 889. Usn vlády České republiky