

Association for Information Systems

**AIS Electronic Library (AISeL)**

---

MENACIS2021

MENA

---

11-14-2021

## **Shadow-IT System as a Workaround: A Theoretical Review**

Asif Shaikh

Follow this and additional works at: <https://aisel.aisnet.org/menacis2021>

---

This material is brought to you by the MENA at AIS Electronic Library (AISeL). It has been accepted for inclusion in MENACIS2021 by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# Shadow-IT System as a Workaround: A Theoretical Review

*Short Paper*

## Introduction

Since the turn of the century, as technology advanced, convergence among all kinds of information and communication forms tied the related knowledge together into one common underlying infrastructure based on digital techniques, i.e. Information Technology (IT). A phenomenal use of emergent consumer technologies at workplace is rapidly shaping today's organizational environment (Györy et al., 2012). The employees (IT users) who derive their own technological solutions, called Shadow-IT, are changing the central IT department's role in its support of providing technological tools to employees to perform work tasks. Shadow technologies are often collaborative systems used by employees to communicate and share content with co-workers, clients, or external partners. Shadow-IT is the adoption of a business process supporting IT solutions and tools in either replacement or as an extension of the IT functionalities officially provided by the IT department (Walterbusch et al., 2017). The Shadow-IT system, solutions, and components exist in parallel to other formal IT systems (Zimmerman et al., 2017). Shadow-IT termed as a form of a workaround when employees adopt it as a reaction to a perceived situational constraint with the intent to enhance work performance (Haag and Eckhardt, 2017).

Workarounds are defined as irregular use of IS where actual practices are not coherent with the intended use and official rules (Azad and Kings, 2008). However, workarounds are becoming an important part of most organizations. Workaround behavior is studied frequently in information system research upon the assumption that it influences organizational performance (Guo et al., 2011). Workarounds are used to solve problems in different situations (Niazkhani et al., 2011). The specific interest of this review is on the employee use of Shadow-IT tools and resources as inconsistent practices that may lead to harmful consequences (Behrens, 2009).

The theory of workaround is based on the presumptions of an information system (IS) discipline that systematically defines the Shadow-IT system as a form of workarounds. A theoretical review of the conceptual understanding of a Shadow-IT system both as a collaborative tool and a possible hazard to information assets bring possible insights in dealing with contemporary challenges employee usage of such informal systems.

The remainder of this paper is organized as follows. In the next section, we present the concept of Shadow-IT System as a workaround. This is followed by propositions of a workaround theory, alignment, and application of theory in Shadow-IT system research. We then present the critique in the next section. The conclusion forms our final section of the paper.

## Shadow-IT System as a Workaround

In 2014 Steven Alter, defined workarounds routines in business processes as:

*"...a goal-driven adaptation, improvisation, or other change to one or more aspects of an existing work system in order to overcome, bypass, or minimize the impact of obstacles, exceptions, anomalies, mishaps, established practices, management expectations, or structural constraints that are perceived as preventing that work system or its participants from achieving a desired level of efficiency, effectiveness, or other organizational or personal goals" (Alters, 2014, p.1043).*

The theory describes how and why workarounds are created. The theory of workarounds is an extension of his conceptual framework of work system (Alters, 2013). The work system framework is a system in which human participants and/or machines perform work using information, technology, and other resources to produce products/services identifying three elements that are part of a basic understanding of a work system: the surrounding environment that affects the work system (e.g., organizational culture, politics, and history; organizational policies and procedures; relevant standards and regulations; competitive issues technological trends), the external infrastructure that the work system relies on, and strategies at several levels (Alters, 2013).

**Propositions of a Workaround Theory**

The theory of workarounds is integrated by extant research on the consequences of workarounds (Ansari et al., 2010; Azad and King, 2008; Boudreau and Robey, 2005; Ferneley and Sobreperez, 2006; Martin et al., 2013). Five ‘voices’ of workarounds (Figure 1) are developed to structure a) phenomenon associated with workarounds, b) types of workarounds, c) direct effects of workarounds, d) different perspectives on workarounds and e) subsequent organizational challenges and dilemmas related to workarounds (Alter, 2014).

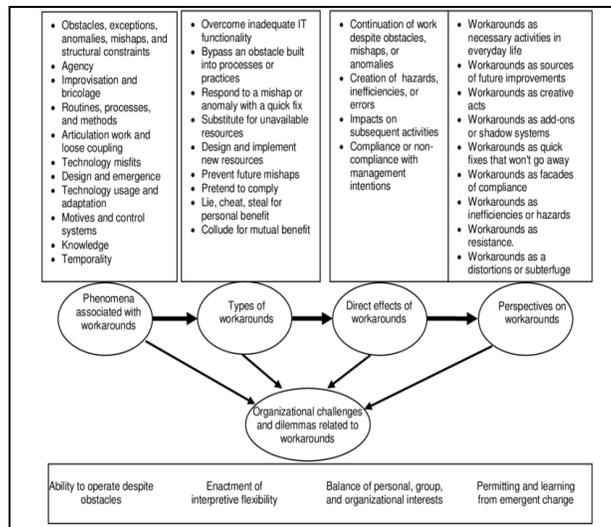
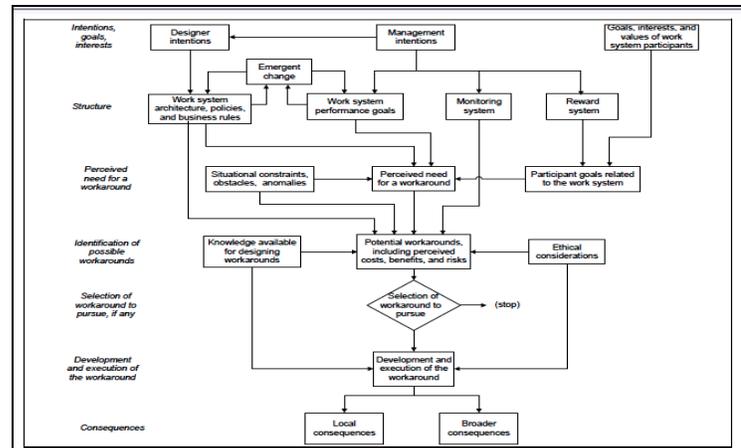


Figure 1 - Five voices of Workarounds (Alter, 2014, p.1048)

The theory suggest seven steps (Figure 2) are suggested based on which workarounds can be analyzed and understood: (1) intentions, goals, interests of each work participant; (2) structure, architecture and characteristics of the work system; (3) perceived need for workaround; (4) identification of workaround by consideration of all knowledge available; (5) selection of workaround; (6) development and execution of the workaround; (7) local and broader consequences including advantages and disadvantages of workarounds (Alter, 2014).



**Figure 2 - Theory of Workarounds (Alter, 2014, p.1056)**

The above figure identifies generic steps in perceiving the need for a workaround and then creating it. This sequence reflects a basically rationalist view in which work system participants create workarounds by identifying obstacles and deciding what to do about them (Alter, 2014).

### ***Alignment of Theoretical concept of Workaround vis a vis Shadow-IT System***

Shadow-IT is relatively a new phenomenon, and only a few scientists have concentrated on this concept as a distinct phenomenon (Gyory et al., 2012; Silic et al., 2017; Walterbusch et al., Fietz, and Teuteberg, 2017; Zimmerman et al., 2017; Haag and Eckhardt, 2017; Oliveira et al., 2016). The study of the Shadow-IT phenomenon from user's perspective reveals that employees use Shadow-IT that leverages their flexibility, enhances productivity and agility, boosts performance, and improves collaboration and communication (Furstenau and Rothe, 2014). Shadow-IT usage is often, therefore, termed a *form of a workaround* as sometimes shadow users build and maintain Shadow-IT system to work around the limitations of established processes (Alter, 2014). The work system places Shadow-IT system as a workaround that suggests change with possible sources of problems in a working system (e.g., use information from an unofficial shadow system), possibly because of problems with the quality, timeliness, completeness, or cost of the officially prescribed information. It will then bypass expected uses of infrastructure (technical, informational, and human resources shared with other work systems), e.g., by accessing information by using infrastructural resources, such as human infrastructure (see figure -1) to help in creating workarounds such as shadow systems or add-ons (Alter, 2014). The theory of workarounds sees Shadow-IT system as facades of compliance, and as inefficiencies or hazards (Alter, 2014). It takes the shadow-IT system outside the purview of an organizational system that frequently brings information security problems hence should not be trusted (Alter, 2014).

With this perspective of Shadow-IT system, the theory of workarounds can help in questioning pejorative terms such as shadow system and feral system that implies workarounds are illegitimate despite its stated benefits in the previous literature. Another expected contribution of the theory is the idea that workarounds may entail resistance and intentional non-compliance with the authority (Alter, 2014). It, therefore, helps address concerns on what should be done in a scenario wherein employees build and maintain private records, spreadsheets, or databases in order to work around the limitations of established processes and bypass organizational information policy controls. The next section will briefly attempt to apply the variables of theory in the context of Shadow-IT.

### ***Application of Theory in Shadow-IT System Research-Proposed Framework***

The author of theory suggests that the contributing features of workaround theory is its treatment to such actions that occur in a working system in the form of short-term adaptations as *add-ons or shadow systems* (Alter, 2014, p. 1052). In combination, five voices: the phenomena, types, effects, and perspectives generate a range of organizational challenges and dilemmas related to workarounds" (Alter,

2014, p.1047). Earlier research used a replication logic used on the theory of workarounds by substantiating the five voices identifying the relevant dimensions for analyzing workarounds (Röder et al., 2014). Similarly, substantiating the five voices can help analyze whether a particular phenomenon can bring specific effect in using Shadow-IT system.

RQ1: What are the direct effects of Shadow-IT as a workaround on organizational information security?

RQ2: What organizational challenges related to Shadow-IT as workaround on management control?

To answer these two research questions, we develop a theoretical model that focuses on the variables of “motives and control systems” as one of the “phenomenon associated with workarounds” (Alter, 2014, p.1050) as a first voice. This phenomenon assumes that quality and characteristic of control systems might affect the likelihood that inappropriate or personally opportunistic workarounds will be noticed. Secondly, variable of “design and implement new source” (Alter, 2014, p.1051) that explains a situation when Shadow systems can be analyzed as a type of unsanctioned workaround to address the shortcomings of a sanctioned system. Third voice maintains that one of the effects of workarounds is the creation of hazards, inefficiencies, or errors. While explaining the perspective on workarounds as the fourth voice, the Shadow-IT system is defined as a feral system that frequently brings information security problem (Alter, 2014). Lastly, the fifth voice anticipates organizational challenges and dilemmas related to the workarounds which balance interpretive flexibility versus management control as a key organizational challenge (Alter, 2014).

<b>Foundational concept: Theory of Workaround (Five Voices)</b>				
1. Phenomenon associated with workaround	2. Types of Workarounds	3. Direct effect of workaround	4. Perspective on workaround	5. Organizational challenges related to workaround
Motives and control systems	Design & implement new source	Creation of hazards, inefficiencies, or errors	add-ons or feral system that create information security threat.	Balancing interpretive flexibility versus management control

**Table-I: Application of the concepts in theory of workarounds in understanding Shadow-IT system**

A qualitative analysis of the propositions for Shadow-IT systems in the five voices of the theory of workaround will be conducted to help illustrate tensions between inefficient and sometimes unsafe variability, on the one hand, and cumbersome and counterproductive controls, on the other. I would like to take the perspective of IT managers in organizations through interview method.

An inductive thematic analysis of empirical material will be done using grounded theory technique (struass & corbin?) to enable the assessment of a phenomenon with a fresh lens. This technique will also help refine the elements of workaround theory further and aid in advancing the theoretical domain of shadow-It systems as *add on risks* in information security research.

## Limitations of Theory of Workaround

While all of the factors in the theory are significant, in some workarounds at least some of the factors are latent and have little impact (Alter, 2014). The theory of workaround is a fresh theoretical lens and so far, been applied in limited contexts such as digital construction design (Merchbrock and Munoz, 2015); health care (Roder et al., 2014). Scholars are of the view that while this theory provides a structure for analyzing workarounds, we still lack a deep understanding of how and why workarounds occur and how employees enact workarounds in organizations (Roder et al., 2014). There is still a lack of conceptual consensus on workaround theory as a profound applicable framework. In order to address this limitation,

future research might need to integrate additional constructs that may contribute to control problems for IT professionals, risk managers, and auditors.

## Next Step

For many, workarounds are seen as ‘messy practices’ that are frequently observed behavior among employees (Merschbrock et al., 2015). For proposed research, the theory of workarounds can serve as a foundational concept that could lead to insights related to organizational challenges to the management, work practices, standards, security controls, data breaches, insider threat, and technology adoption because workarounds are entwined with organizational research topics, practical management issues, and the implementation and realistic use of technology. A comprehensive review of a theory of workarounds is systematically presented to inform about the theory and its contributors; its origin and development over time; the intellectual traditions and research milieu in which the theory can be applied. An attempt is made here to gain understanding of the conceptual framework that can explain the Shadow-IT systems as a form of a workaround representing deviations from existing work systems. A possible framework is provided for future research to understand organizational challenges in management control and information security as an effect of a Shadow-IT usage utilizing the concepts of workaround theory. In this context comparative study of the results of a workaround-centric approach with other possible approaches might also provide insights on integrating relevant phenomena related to adaptations, appropriation of technology, and organizational change.

## References

- Alter, S. 2014. “Theory of Workarounds,” *Communications of the Association for Information Systems* (34), pp. 1041-1066.
- Alter, S. 2013. “Work System Theory: Overview of Core Concepts, Extensions, and Challenges for the Future,” *Journal of the Association for Information Systems* (14: 2), pp. 72-121.
- Ansari, S. M., Fiss, P.C; and Zajac, E.J. 2010. “Made to Fit: How Practices Vary as they Diffuse,” *Academy of Management Review* (35: 1), pp. 67-92.
- Azad, B., and King, N. 2008. “Enacting Computer Workaround Practices within a Medication Dispensing System,” *European Journal of Information Systems* (17:3), pp. 264-278.
- Behrens, S. 2009. “Shadow systems: The good, the bad and the ugly,” *Communications of the ACM* (52), pp. 124–129.
- Boudreau, M. C., and Robey, D. 2005. Enacting Integrated Information Technology: A Human Agency Perspective. *Organization science* (16:1), pp. 3-18.
- Corbin, J. M., and Strauss, A. 1990. “Grounded Theory Research: Procedures, Canons, and Evaluative Criteria,” *Qualitative Sociology* (13:1), pp. 3-21.
- Guo, K.H., Yuan, Y., Archer, N.P., and Connelly, C.E. 2011. “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model”, *Journal of Management Information Systems* 28(2), pp. 203- 236.
- Györy, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. “Exploring the Shadows: IT Governance Approaches to User-Driven Innovation,” in *Proceedings of 20th European Conference of Information Systems*, Barcelona, ES.
- Ferneley, E., and Sobreperez, P. 2006. “Resist, Comply or Workaround: An Examination of Different Facets of User Engagement with Information Systems,” *European Journal of Information Systems* (15), pp. 345– 356.
- Fürstenau, D., and Rothe, H. 2014. “Shadow IT Systems: Discerning the good and the evil,” in *Proceedings of Twenty Second European Conference on Information Systems*, Tel Aviv.
- Martin, A. W., Lopez, S., Roscigno, V.J., and Hodson, R. 2013. “Against the Rules: Synthesizing Types and Processes of Bureaucratic Rule-breaking,” *Academy of Management Review* (38:4), pp. 550-574.
- Merschbrock., Christoph., and Figueres-Munoz, Alejandro. 2015. “Circumventing Obstacles in Digital Construction Design—A Workaround Theory Perspective,” *Procedia Economics and Finance* (21).
- Niazkhani, Z., Pirnejad, H., Van Der Sijs, H., and Aarts, J. 2011. “Evaluating the Medication Process in the

- Context of CpoE Use: The Significance of Working around the System," *International Journal of Medical Informatics* (80:7), pp. 490-506.
- Oliveira, M., Mallmann, G. L., and Maçada, A. C. G. 2016. "Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study," in *Proceedings of the European Conference on Knowledge Management, Coleraine, UK*
- Röder, N., Wiesche, M., and Schermann, M. (2014). "A Situational Perspective on Workarounds in IT-enabled Business Processes: A Multiple case study," in *Proceedings of European Conference on Information Systems (ECIS)*, Tel Aviv.
- Silic, M., and Back, A. 2014. "Shadow IT—A view from behind the curtain," *Computers & Security* (45).
- Walterbusch, M., Fietz, A., and Teuteberg, F. 2017. "Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT," *Journal of Enterprise Information Management*, (30:4).
- Zimmermann, S., Rentrop, C., and Felden, C. 2017. "A Multiple Case Study on the Nature and Management of Shadow Information Technology," *Journal of Information Systems* (31:1).