Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

Discussion Paper

Why don't you stick to them? Understanding Factors influencing and Counter-Measures to combat deviant Behavior towards organizational IT Standards

by

Sven Dittes[1], Nils Urbach, Frederik Ahlemann[2], Stefan Smolnik, Thomas Müller[2]

in: Proceedings of the 12th International Conference on Wirtschaftsinformatik (WI), Osnabrück, Germany, March 2015

[1] University of Hagen
[2] University of Duisburg-Essen

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: F.-v.-Schiller-Str. 2a, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

Why don't you stick to them? Understanding factors influencing and counter-measures to combat deviant behavior towards organizational IT standards

Sven Dittes[1], Nils Urbach[2], Frederik Ahlemann[3],
Stefan Smolnik[1] and Thomas Mueller[3]

[1] University of Hagen, Germany
{sven.dittes,stefan.smolnik}@fernuni-hagen.de
[2] University of Bayreuth, Germany
nils.urbach@uni-bayreuth.de
[3] University of Duisburg-Essen, Germany
{ferderik.ahlemann,thomas.mueller}@uni-due.de

Abstract. Organizational information technology (IT) standards have become increasingly important for companies. However, insights from practice indicate that employees tend to violate these standards, generating a need for governance and management mechanisms with which to successfully implement them in the organization. The literature reveals a lack of research on organizational IT standards' governance. Drawing on this finding, our research aims at identifying the factors that influence an employee's deviant behavior towards organizational IT standards. We therefore derive a conceptual model deductively from the literature, which we supplement with an interview study. Future research could use quantitative methods to validate this model. Our work enriches IS research and practitioner bodies of knowledge. We do so by first extending our knowledge of an employee's deviant behavior towards organizational IT standard. Second, we provide valuable insights for organizations by providing starting points to improve their standardization efforts.

Keywords: organizational IT standards; deviant behavior; IT governance

1 Introduction and Background

Standardization has become an established approach for organizations to coordinate and organize their resources and processes in order to ensure product and service quality and to raise work efficiency [1, 2]. Companies operating worldwide rely particularly heavily on standards to leverage economies of scale through uniform business processes. Thus, it is not surprising that also most information technology (IT) departments pursue standardization [3]. The importance of organizational standards for IT departments has increased steadily over time, due to the growth, complexity, and increasing costs of the organizational IT in almost all departments in large organizations. A survey by the Boston Consulting Group indicates that organizations with a

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

well standardized IT infrastructure can decrease their IT infrastructure costs by 15% and their overall IT costs by 33% [4]. Another survey of IT leaders from across the world finds that they rate IT standards as one of the three most valuable activities in their companies [3].

Despite the practical importance of organizational IT standards, little, scattered, and rather fragmented research has been done on standards within organizations' IT departments [5, 6]. Besides the richer body of knowledge on non-organizational, industry-related IT standards, such as standards set by international consortia and official bodies (e.g. ISO norms, government standards) [e.g. 7, 8], only a few studies investigate aspects of IT standards within organizations. These internal IT standards might be individually defined rules, or adaptations of industry standards. Based on this understanding of organizational IT standards, we found studies on the standardization of the organizational IT infrastructure [e.g. 9, 10], a research stream dealing with the standardization of business processes [e.g. 11, 12], as well as a body of knowledge on the field of compliance with information security policies, which explains employees' adherence to security policies [e.g. 13, 14]. Van Wessel [15] acknowledges this scattered body of knowledge by defining three abstract domains for organizational IT standards: technological standards (e.g. standards determining the brand and type of servers in data centers), data standards (e.g. specific data structures and their semantics), and process standards (e.g. security guidelines or project management processes). All these different research streams produce independent results that hardly comprise a coherent body of knowledge on organizational IT standardization. However, we assume that the cognitive factors explaining individual employees' behavior when evaluating their (non)adherence to an IT standard are independent of the particular type of standard. Further, we suppose that by applying an IT governance perspective, we can abstract from all these different domains by arguing that it does not matter with which standard domain we deal – all these standards need to be managed and governed similarly so that staff adhere to them and they can yield the desired outcome.

Given these mainly distinct research streams, it is not surprising that we found no generally accepted definition of organizational IT standards. However, in the literature, several approaches seek to define and identify the most important characteristics of an organizational IT standard [e.g. 6, 16]. Based on the literature and the experience we gained during our research, we define an organizational IT standard as any *written rule or guideline within the IT department of an organization based on a clear motivation aimed at harmonizing, optimizing, or securing material and nonmaterial objects when dealing with repeated business or IT processes. A standard is defined, released, and revised by an authority seeking to create an advantage for a particular interest group.* These rules could be based on an industry-related IT standard, common principles, best practices, or on a company's individualized rules. Accordingly, we define IT standardization as the process of implementing and enforcing such an IT standard within an organization.

The implementation of organizational IT standards is a costly endeavor involving activities such as identifying areas that require standardization, the specification and documentation of standards, their approval, the training of staff, the monitoring of

their usage, and the resultant reporting. The disregard of and noncompliance with IT standards may affect an organization very negatively. Apart from the financial impacts and the anticipated benefits that are not leveraged, the damage can be significant in terms of credibility, morale, and commitment. Organizations therefore try their best to enforce compliance with organizational IT standards, but often without success. For example, according to a study by Russo, Hightower and Pearson [17], only 6% of organizations maintain that their standardized methodologies are executed as specified.

Workplace deviance research confirms that employees' violation of organizational norms, like organizational IT standards, can imply massive financial losses for a company [18, 19]. Furthermore, information security research indicates that employees violating and neglecting organizational policies are responsible for the majority of security problems [20]. These findings show that, in order to ensure the successful functioning of an organization, it is essential to ensure employees' adherence to the rules and the company policies [2]. By transferring these findings to organizational IT standards, it is crucial to implement governance mechanisms in order to assure the usage and application of these standards. If employees ignore these standards, the targeted benefits, such as cost reduction or quality improvement, cannot be leveraged. The standards' characteristics, which delimit IT standardization from other standardization efforts within an organization, also enhance this need for a comprehensive management and governance of all the standards within an IT department since all the different standards (technical, data, and processes) correlate and interdependent – making IT standardization a very unstable ecosystem.

Drawing on these literature streams, we still found only a very limited number of scientific studies on the governance processes of organizational IT standards [6]. However, some studies do acknowledge the importance of management and governance structures, as well as mechanisms for standardization purposes. For example, Cargill [21] investigates management styles' (regulatory style and laissez faire) different impacts on standardization. Rada and Craparo [22] show that the corporate culture is a major influence when employees need to adapt to management standards. Additionally, van Wessel, Ribbers and de Vries [6] prove the importance of governance for the actual application of IS standards. Finally, de Vries, Slob and Zuid-Holland [5] describe the best practice approaches for a successful company IT standardization. Nevertheless, most of these studies mainly analyze qualitative research data top-down by evaluating the advantages and the drawbacks of different management and governance mechanisms used to help employees adapt to new standards. In our study, we take this idea one step further by, first, evaluating the bottom-up factors that lead to employees' deviant behavior towards organizational IT standards. Second, we conceptualize effective and efficient governance mechanisms that motivate them to adopt these standards. Consequently, our objective is to develop a conceptual model that seeks to understand and explain the cognitive drivers that lead employees to violate organizational IT standards. In a second step, and based on these cognitive drivers, we aim at determining the potential governance and management mechanisms that would avoid such behavior. Our current focus is thus on discovering these factors

and not on statistically validating the strength of their influence. We aim to answer the following research questions:

RQ1: From employees' cognitive perspective, which, are the most important individual-level factors that influence their deviant behavior towards organizational IT standards?

RQ2: Which IT-organizational-level factors influence the individual-level factors to reduce such deviant behavior and, thus, potentially serve as a basis for governance mechanisms?

Since there is already a huge body of knowledge on organizational behavior and misbehavior research, and also a reasonable literature stream on information security policy compliance research, we deductively develop a conceptual model to explain the phenomenon of employees' deviant behavior towards organizational IT standards. In addition, we carried out an interview study to corroborate our findings and ensure their usefulness.

Our work seeks to both contribute to research and to provide implications for managerial practice. We contribute to theory by extending our knowledge of deviant behavior towards organizational IT standards. From a practical perspective, we provide valuable insights for organizations by exploring potential governance and management mechanisms and, therefore, the best starting points from which to conceptualize the comprehensive management and governance of organizational IT standards.

2 Research Method

According to the taxonomy of theory types by Gregor [23], we seek to develop a theory of explanation and prediction (Type IV). We thus chose a deductive research approach by using the existing literature on workplace deviance and information security policy compliance as a foundation to derive the underlying propositions. In addition, we conducted a field study based on interviews in order to corroborate our theoretical findings, as well as to pre-test and ensure the validity of our conceptual model. In respect of a Type IV theory, this approach allows for testing our model's completeness and explanatory power [23]. When dealing with complex and practice-based problems, it is especially important to analyze different actors' experiences in the context of action [24]. We therefore gathered our research data from semi-structured interviews, closely following Eisenhardt [25] recommendations.

We subsequently applied an iterative approach: We used the literature and theories to build an initial understanding, resulting in a conceptual map. Since there is – to the best of our knowledge – no research on employees' violation of organizational IT standards and due to the general lack of research on organizational IT standards [5, 6], we started off by evaluating the standard violation phenomenon. We came to the conclusion that employees' violation of standards is merely a particular behavior – or, in our case, misbehavior – within an organizational context. Since our research's aim is to study employees' deviant behavior towards organizational IT standards, the organizational behavior research stream, which concentrates on analyzing human behavior in the context of organizations [26], was a valid starting point for the deductive devel-

opment of a conceptual model. In particular, we considered the research stream on workplace deviance – defined as an employee's violation of organizational norms within a company [27] – a very suitable theoretical lens for our study. Workplace deviance research focuses on human behavior in terms of deviance and the violation of norms and standards [28]. Since employees' deviant behavior towards organizational IT standards can be abstracted as deviant behavior within an organization, this stream serves as the basis of our study. Additionally, we also found that a new research stream — the theory of workarounds [29] — is a very suitable theoretical basis for our research endeavor. The theory of workarounds aims at explaining how people decide whether to follow established practices or not [29]. Since the violation of organizational IT standards also describes the behavior of employees deciding not to follow established practices in terms of the rules, this theory serves as an additional theoretical lens for our research.

After we searched for literature describing the IT standard deviance phenomenon more abstractly to allow us to deduce our knowledge from a more general point of view, we also found a suitable research stream dealing with employees' compliance with and adherence to information security policies [e.g. 13, 14, 30]. In terms of our definition of organizational IT standards, we consider information security policies a subset of organizational IT standards. Therefore, we also use information security policy research as a further conceptual basis for our research. In this respect, we mainly draw on the research of Bulgurcu, Cavusoglu and Benbasat [13], who investigated the factors that influence information security policy compliance on an individual level.

During the course of our study, we continuously refined our understanding of the phenomenon by conducting several expert interviews, by adjusting our interview guidelines after each interview, and by applying the new knowledge we gained during the interviews to revise our conceptual model. We performed this iterative process until we arrived at a theoretical saturation when the last interviews did not yield any new significant insights, which meant we had identified the most important influencing concepts. The study sample consists of 21 interviews with experienced IT professionals and practice experts.

Table 1 shows a detailed overview of our case companies and interviewees. We aimed at identifying companies with very complex organizational structures, a high usage of IT within many different departments, and a great need to leverage economies of scale in terms of their IT usage. Consequently, we primarily conducted our interviews within the realm of the automotive industry, focusing only on one major German automotive manufacturer, which enabled us to gain a deep understanding of the actual problems that these companies face in terms of deviant behavior towards IT standards. Furthermore, we carried out additional interviews in six other companies to verify our results. Hereby, we targeted a variation in terms of the industries their sizes, their IT or business structure, and IT or business strategies to avoid any bias (see Table 1).

Table 1. Interviewee Information

#	Industry	Revenues worldwide in €	Employees worldwide (in IT)	No. of inter-views	Interviewees' roles
1	Automo-tive	~ 105,000 bn.	570,000 (9,300)	12	Infrastructure architects (3), team leaders (4), department head of EAM, department head of IT architecture, de-partment head of IT infrastructure, project leader, process manager
2	IT	~ 740 m.	4,800 (67)	1	Team leader
3	Consulting	~ 32 bn.	180,000 (2,500)	2	IT manager, IT support
		~ 87 m.	250 (12)	1	SAP developer
4	Software	~ 253 m.	1,400 (157)	1	IT auditor
		~ 2 m.	14 (6)	1	CEO
5	Insurance	~ 254m.	291 (52)	1	Team leader
6	Energy	~ 474m.	1,991 (37)	1	CIO
7	Construc-tion	~ 800 m.	4,304 (50)	1	CIO

3 Conceptual Model

In the following sections, we present our conceptual model in detail, describing its components and their relationships by means of propositions. First, we describe how we conceptualize employees' deviant behavior towards IT standards. Second, we deduce the most important influencing factors from literature on the individual level. Finally, by means of propositions, we suggest the influencing factors on the IT organizational level that counteract those on the individual level and effect a reduction in IT standard deviance, thus serving as potential management mechanisms. Additionally, we illustrate our model through selected evidence from our interview study. Figure 1 shows the resulting conceptual model indicating all developed propositions.

3.1 Employees' Deviant Behavior towards Organizational IT Standards

Drawing on workplace deviance research, deviant behavior is conceptualized as "voluntary behavior that violates significant organizational norms" [31], meaning that deviance research usually implies a voluntary action based on an intention [28]. However, our interviews suggest that the violation of organizational IT standards is not always related to an intentional act, but sometimes also to an unintentional act: A team leader from the automotive industry stressed that *"80% [of employees] who*

violate IT standards do not know that they violate them." Therefore we may distinguish, first, intentional behavior as theorized in workplace deviance research and, second, unintentional behavior [32]. We therefore conceptualize both intentional deviance from IT standards and unintentional deviance from IT standards as suitable determinants to explain employees' deviant behavior towards organizational IT standards.

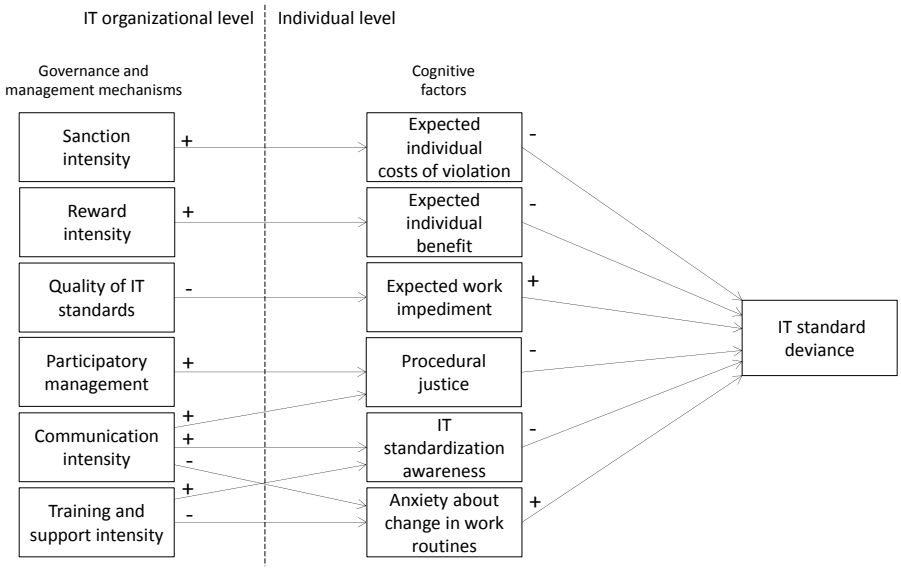

Fig. 1. Conceptual Model

3.2 Influential Factors on the Individual Level

Bulgurcu, Cavusoglu and Benbasat [13] show that the perceived costs of noncompliance have a positive impact on employees' attitudes towards complying with information security policies. These authors define the costs of noncompliance as "the overall expected unfavorable consequences for [sic] noncompliance" [13]. Transferring this knowledge to the phenomenon of employees' deviant behavior towards organizational IT standards, we propose that they are less tempted to violate standards when they expect this behavior to have unfavorable or harmful consequences. Additionally, our interview results showed that organizations enacting a system of incentives and/or punishments are more successful at enforcing compliance with organizational IT standards. Therefore, we propose:

Proposition 1: The expected individual cost of violation is negatively associated with employees' deviant behavior towards organizational IT standards.

Workplace research conceptualizes individualism as associated with rule breaking, such as shortcutting procedures: Employees "prefer to choose short-term personal advantage over long-term corporate consequences" [33]. This finding is also

acknowledged by information security policy research. Bulgurcu, Cavusoglu and Benbasat [13] state that employees' perceived benefit from compliance has a positive impact on actual compliance with security policies. Based on these findings, we propose that if an IT standard provides additional value for an individual who applies it, the individual benefit has a negative effect on the individual's intention to violate IT standards. This proposition is also highlighted by a statement from a CEO in the software industry: *"The individual benefit is a significant influencing factor when we look at the acceptance of IT standards."* Thus, we propose:

Proposition 2: The expected individual benefit is negatively associated with employees' deviant behavior towards organizational IT standards.

Another influencing factor concerning employees' deviant behavior towards IT standards that our interviews highlighted, is summarized by a quote from a team leader in the automotive industry: *"Standards only make sense when they do not hinder."* In the literature, work impediment is defined as "a detriment to an employee's daily job-related tasks and activities" [13]. Literature based on the theory of workarounds stresses the importance of the expected work impediment regarding non-compliance with standards: In their case study, Röder, Wiesche and Schermann [34] discover that policies are ignored, because the employees perceive them as too complex to apply. Information security policy research also stresses that employees often perceive compliance with security policies as a barrier to productivity [35]. By regarding information security policies as just a special type of standard, we transfer this belief to our phenomenon of deviance from organizational IT standards. Based on this and the empirical evidence, we propose:

Proposition 3: The expected work impediment is positively associated with employees' deviant behavior towards organizational IT standards.

Additionally, our field study highlights another interesting influencing factor. An infrastructure architect from the automotive industry believes that the most crucial problem is participation during the definition of IT standards: *"You see the so-called not-invented-here phenomenon – meaning that standards are violated because employees are not involved in the definition phase."* This phenomenon can be related to the procedural justice concept in the literature. Procedural justice is defined as the extent to which a decision process is perceived as fair [36]. Having originated in the context of court decisions, the procedural justice concept found its way to organizational research [37]. In this context, procedural justice is also used in deviance research [e.g. 38]. Colquitt [39] finds that although team members may be dissatisfied with a decision, they accept it if they believe procedural justice has occurred, for example, if their opinion was considered during the decision process. Transferring this knowledge to the problem of employees' deviant behavior towards organizational IT standards, we propose that the employees' intention to violate an IT standard is less if they are involved in the standardization process during which they share their thoughts and expertise. Thus, we propose:

Proposition 4: Procedural justice is negatively associated with employees' deviant behavior towards organizational IT standards.

As already mentioned, our field study indicates that many employees do not know that they deviate from organizational IT standards. That is, they did not have information on the prevailing IT standards and, consequently, they unintentionally deviated from these standards. Information security policy research pays attention to this phenomenon by conceptualizing information security awareness as an important influence on compliance [40]. Drawing on this research, we introduce the concept of IT standardization awareness and define it as a state in which an individual in an organization is aware of relevant organizational IT standards. IT standardization is a gradual state, as individuals sometimes only know that a standard exists, but are not aware of its applicability or contents. The IT standardization awareness phenomenon was confirmed in our interviews. A team leader from the automotive industry stated that: *"90% of employees in my department do not know that there is this document of standard prescriptions."* Thus, we propose:

Proposition 5: IT standardization awareness is negatively associated with employees' deviant behavior towards organizational IT standards.

Ajzen [41] defines habit as the development of former recurrent behavior. Thus, the more experience people gain through the application of a past behavior, the more likely they are to adopt this behavior as a habit. Because habit describes an unknown and subconscious process that motivates the intention to perform a certain behavior, we conceptualize it as an automatic comparison of a particular IT standard with former behavior patterns. In our field study, a CIO's statement relates to such a behavior: *"The most common question is: Why should we do that? We have done this for years now and it works. Thus, many employees are unwilling to change and reject concepts like IT standards, which require a business change."* Consequently, we conceptualize anxiety about expected changes in work routines as the fear that the application of a particular standard will vary from a former behavior pattern. Thus, if adherence to an IT standard requires a certain behavior that does not match the former behavior and is not similar to the former behavior patterns, this anxiety will have a distinct positive influence on the intention to violate the IT standards. Owing to this theoretical and empirical support, we propose:

Proposition 6: Anxiety about changes in work routines is positively associated with employees' deviant behavior towards organizational IT standards.

3.3 Management and Governance Mechanisms on the IT Organizational Level

Hollinger and Clark [42] underline the influence of sanctions on deviant behavior. They find that the perception of both the certainty and severity of organizational sanctions is related to employee theft. Since we abstract employee theft as a violation of the organizational rules, we can relate this to our research. Additionally, information security policy research shows the importance of sanctions for compliance. Bulgurcu, Cavusoglu and Benbasat [13] conceptualize the influence of sanctions on the perceived costs of noncompliance. In addition, our interview study underlines the importance of sanctions: An infrastructure architect from the automotive industry an-

swered the question about the greatest obstacles in terms of IT standards as: *"Currently it does not matter if somebody does not adhere to a standard."* Further, this infrastructure architect mentioned that a possible solution would be to implement *"obstacles which are so enormous that it is not worth [deviating from the standards]."* Based on the literature and these findings, we conceptualize sanction intensity as the severity and certainty of punishment when violating an organizational IT standard, which adds to the expected noncompliance costs and propose:

Proposition 7: Sanction intensity is positively associated with the expected individual cost of violation.

Rewards are defined as tangible or intangible compensation given to an employee in return for a particular behavior [13]. Puhakainen and Ahonen [35] acknowledge the influence of a reward system on compliance with information security policies. Workplace deviance research also stresses the negative influence of a reward system on deviant behavior [e.g. 43, 44]. Bulgurcu, Cavusoglu and Benbasat [13] conceptualize rewards as related to employee' perceived benefits. Moreover, the theory of workarounds emphasizes the connection between a reward system and the perceived need for a workaround [29]. Thus, we conceptualize reward intensity as the appreciation an employee receives in return for adhering to organizational IT standards, which adds to the expected individual benefit:

Proposition 8: Reward intensity is positively associated with the expected individual benefit.

Our interview study shows that quality in terms of the consistency between different standards, the description of a standards and selection process, as well as requirement analyses is a major influence on the expected work impediment. An infrastructure architect from the automotive industry stressed the importance of the quality of IT standards: *"If I were to comply with all our standards, nothing would work anymore."* The literature does not pinpoint a clear theoretical tendency regarding the quality of standards' influence on the expected work impediment. However, since we have strong evidence from our interview study, we suggest that the quality of IT standards is a measure to assure that the work impediment that IT standards cause is minimized:

Proposition 9: The quality of IT standards is negatively associated with the expected work impediment.

Since the level of procedural justice within the IT standardization process is conceptualized as having a major positive impact on adherence to organizational IT standards (see Proposition 4), it is important to find a measure to enhance and support employees' perception of procedural justice in order to reduce the number of standard violations. The literature has proved that participation is a major influence on procedural justice [45]. Therefore, we conceptualize participatory management as an approach to increase employees' perception of procedural justice:

Proposition 10: Participatory management is positively associated with procedural justice.

Additionally, we conceptualize communication intensity as the degree to which an organization communicates its organizational IT standards and ensures that individuals have sufficient information to identify the relevant standards in a job situation. In our field study, we also discovered empirical evidence of communication activities' importance: Almost all the interviewees rated communication as one of the most influential factors for improving organizational IT standards' compliance rate. Since we propose that IT standard awareness has a major influence on deviant behavior towards organizational IT standards, it is essential to overcome this lack of awareness about them by implementing communication mechanisms. Further, Fussell, Kraut, Lerch, Scherlis, McNally and Cadiz [46] highlight the connection between communication measures and the awareness, while Kashanchi and Toland [47] stress that communication increases awareness. Therefore, we propose:

Proposition 11a: The communication intensity is positively associated with IT standard awareness.

Moreover, research on procedural justice also proves the influence that communication activities have on procedural justice [45], meaning that open communication about IT standards and the standardization process increases an employee's feeling of procedural justice. Thus, we propose:

Proposition 11b: The communication intensity is positively associated with procedural justice.

Besides, communication is also said to be a powerful management mechanism when dealing with change management [48]. In order to overcome anxiety about changes in work routines (Proposition 6), it is essential to use change management mechanisms. Therefore, we also propose that by using communication measures, it is possible to reduce anxiety about IT standards having a major impact on employees' daily work routines:

Proposition 11c: The communication intensity is negatively associated with anxiety about changes in work routines.

In our interview study, employees often talked about the importance of support measures in terms of training. For example, a project leader from the automotive industry stressed: *"I would say that support is the most important influence."* Additionally, when questioned about his company's reason for employees accepting standards, a team leader in the automotive industry answered: *"Because standards are understood and properly taught."* The literature on information security policy research stresses that campaigns and education are important for complaint behavior, because they improve awareness of security policies [35, 49]. Thus, we conceptualize training and support intensity as the degree to which an organization supports its employees when introducing new organizational IT standards, thus ensuring that they have an adequate skillset to cope with these standards in their daily work. Therefore, we propose:

Proposition 12a: The training and support intensity is positively associated with IT standard awareness.

Similar to communication intensity (Proposition 11c), training and support measures are also defined as potent change management mechanisms [48], meaning that providing employees with the right training measures, thus leading to a sufficient skillset to cope with and use organizational IT standards, decreases their anxiety that applying such standards will have a negative impact on their daily work. Kotter and Schlesinger [50] also confirm this assumption by proposing that providing training is most helpful when dealing with fear and anxiety. Our interview data too stresses the importance of change management mechanisms, such as training and support in terms of a change in work routines: A team leader stated that: *"It is easier to adopt changes within one's comfort zone; further, proper change management is essential for big changes."* Thus, we propose:

Proposition 12b: The training and support intensity is negatively associated with anxiety about changes in work routines.

4 Discussion and Conclusion

Our study investigates the factors that influence deviant behavior towards organizational IT standards. Our research builds, first, on organizational behavior research, in particular workplace deviance research and, second, on information security policy research. In addition, field study interviews substantiate our deductive findings from the literature. The resulting conceptual model includes six factors that influence employees' deviant behavior towards organizational IT standards on the individual level and six factors on the organizational level, which could thus be potential governance and management mechanisms to improve adherence to organizational IT standards.

In sum, our research contributes to theory in several ways. To the best of our knowledge, it is the first attempt to conceptualize the antecedents of deviant behavior towards organizational IT standards. Our model offers a set of constructs that can explain individuals' deviant behavior towards such standards, as well as a set of concepts on the organizational level that influences this behavior. Our work also has significant managerial implications. By using our model, managers can better understand the drivers of IT standards' acceptance and rejection. This understanding can help managers design effective change management programs and governance mechanisms.

Our results suggest that the importance and severity of each variable's influence on a particular employee's deviant behavior are highly dependent on this person's personality and job characteristics. This could lead to new and very interesting research avenues: Investigating the influence of job characteristics, such as an employee's level of command and experience in terms of moderators, on our conceptual model might be a fruitful path.

Further, our future research endeavors will be aimed at conducting a confirmatory survey by applying quantitative methods [51, 52]. As some of our constructs are new, or are modifications of existing constructs from the literature, this may involve the development and refinement of measurement models. Our model includes two levels of investigation, therefore we intend to approach large corporations instead of indi-

viduals to gain access to organizational-level variables as well as individual-level variables. Based on the results of the quantitative validation of our conceptual model, we will derive the most promising governance and management mechanisms in order to improve organizational IT standardization. Such mechanisms might be the introduction of a lifecycle model for organizational IT standards in order to manage standardization endeavors, or measurement values in order to monitor and steer the standardization processes, or change management practices in order to introduce new organizational IT standards.

References

1. Kondo, Y.: Innovation Versus Standardization. The TQM Magazine 12, 6-10 (2000)
2. Tyler, T.R.: Promoting Employee Policy Adherence and Rule Following in Work Settings-the Value of Self-Regulatory Approaches. Brooklyn Law Review 70, 1287-1312 (2005)
3. CIO Dashboad, http://www.ciodashboard.com/it-strategy/analytics-governance-standards/ (Accessed: 04.11.2013)
4. bcg.perspectives, https://www.bcgperspectives.com/content/articles/information_technology_it_organization_from_it_complexity_to_commonality/ (Accessed: 21.11.2013)
5. de Vries, H.J., Slob, F.J., Zuid-Holland, V.G.: Best Practice in Company Standardization. International Journal of IT Standards and Standardization Research 4, 62-85 (2006)
6. van Wessel, R., Ribbers, P., de Vries, H.: On the Effects of Is Company Standards on Business Process Performance. In: The 4th Conference on Standardization and Innovation in Information Technology pp. 254-267. (2005)
7. Schmidt, S.K.: Coordinating Technology: Studies in the International Standardization of Telecommunications. MIT press (1998)
8. Backhouse, J.H., Carol W.; Silva, Leiser: Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard. MIS Quarterly 30, 413-438 (2006)
9. Akkermans, H., Van der Horst, H.: Managing IT Infrastructure Standardisation in the Networked Manufacturing Firm. International Journal of Production Economics 75, 213-228 (2002)
10. Hanseth, O., Braa, K.: Hunting for the Treasure at the End of the Rainbow: Standardizing Corporate IT Infrastructure. Computer Supported Cooperative Work 10, 261-292 (2001)
11. Münstermann, B., Eckhardt, A., Weitzel, T.: The Performance Impact of Business Process Standardization: An Empirical Evaluation of the Recruitment Process. Business Process Management Journal 16, 29-56 (2010)
12. Wüllenweber, K., Beimborn, D., Weitzel, T., König, W.: The Impact of Process Standardization on Business Process Outsourcing Success. Information Systems Frontiers 10, 211-224 (2008)
13. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly 34, 523-548 (2010)

14. Pahnila, S., Siponen, M., Mahmood, A.: Employees' Behavior Towards IS Security Policy Compliance. In: 40th Annual Hawaii International Conference on System Sciences. IEEE, (2007)
15. Van Wessel, R.: Toward Corporate IT Standardization Management: Frameworks and Solutions. Information Science Reference (2010)
16. de Vries, H.J.: Standardization: A Business Approach to the Role of National Standardization Organizations. Springer (1999)
17. Russo, N.L., Hightower, R., Pearson, J.M.: The Failure of Methodologies to Meet the Needs of Current Development Environments. In: Proceedings of the British Computer Society's Annual Conference on Information System Methodologies, pp. 387-393. (1996)
18. Murphy, K.R.: Honesty in the Workplace. Thomson Brooks/Cole Publishing Co (1993)
19. APA Center for Organizational Excellence, http://www.apaexcellence.org/resources/goodcompany/newsletter/article/249 (Accessed: 30.04.2014)
20. Warkentin, M., Shropshire, J., Johnston, A.: The IT Security Adoption Conundrum: An Initial Step toward Validation of Applicable Measures. In: AMCIS 2007. (2007)
21. Cargill, C.F.: Information Technology Standardization: Theory, Process, and Organizations. Digital Press (1989)
22. Rada, R., Craparo, J.: Standardizing Management of Software Engineering Projects. Knowledge, Technology & Policy 14, 67-77 (2001)
23. Gregor, S.: The Nature of Theory in Information Systems. MIS Quarterly 30, 611-642 (2006)
24. Benbasat, I., Goldstein, D.K., Mead, M.: The Case Research Strategy in Studies of Information Systems. MIS Quarterly 369-386 (1987)
25. Eisenhardt, K.M.: Building Theories from Case Study Research. Academy of management review 14, 532-550 (1989)
26. Griffin, R., Moorhead, G.: Organizational Behavior. Cengage Learning (2011)
27. Robinson, S.L., Bennett, R.J.: A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study. Academy of Management Journal 38, 555-572 (1995)
28. Robinson, S.L., Bennett, R.J.: Workplace Deviance: Its Definition, Its Manifestations, and Its Causes. Research on negotiation in organizations 6, 3-27 (1997)
29. Alter, S.: Theory of Workarounds. Communications of the Association for Information Systems 34, (2014)
30. Vroom, C., Von Solms, R.: Towards Information Security Behavioural Compliance. Computers & Security 23, 191-198 (2004)
31. Bennett, R.J., Robinson, S.L.: Development of a Measure of Workplace Deviance. Journal of applied psychology 85, 349 (2000)
32. Malle, B.F.: How People Explain Behavior: A New Theoretical Framework. Personality and social psychology review 3, 23-48 (1999)
33. Mars, G.: Human Factor Failure and the Comparative Structure of Jobs. Disaster Prevention and Management 6, 343-348 (1997)
34. Röder, N., Wiesche, M., Schermann, M.: A Situational Perspective on Workarounds in IT-Enabled Business Processes: A Multiple Case Study. In: Proceedings of the 22nd European Conference on Information Systems, pp. 1-16. (2014)

35. Puhakainen, P., Ahonen, R.: Design Theory for Information Security Awareness. Oulu University Press (2006)
36. Lind, E.A., Tyler, T.R.: The Social Psychology of Procedural Justice. Plenum Press, New York (1988)
37. Konovsky, M.A.: Understanding Procedural Justice and Its Impact on Business Organizations. Journal of management 26, 489-511 (2000)
38. Aquino, K., Lewis, M.U., Bradfield, M.: Justice Constructs, Negative Affectivity, and Employee Deviance: A Proposed Model and Empirical Test. Journal of Organizational Behavior 20, 1073-1091 (1999)
39. Colquitt, J.A.: On the Dimensionality of Organizational Justice: A Construct Validation of a Measure. Journal of applied psychology 86, 386–400 (2001)
40. Siponen, M.: Five Dimensions of Information Security Awareness. Computers and Society 31, 24-29 (2001)
41. Ajzen, I.: The Theory of Planned Behavior. Organizational behavior and human decision processes 50, 179-211 (1991)
42. Hollinger, R.C., Clark, J.P.: Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. Social Forces 62, 398-418 (1983)
43. Salin, D.: Ways of Explaining Workplace Bullying: A Review of Enabling, Motivating and Precipitating Structures and Processes in the Work Environment. Human relations 56, 1213-1232 (2003)
44. Vardi, Y.: The Effects of Organizational and Ethical Climates on Misconduct at Work. Journal of Business Ethics 29, 325-337 (2001)
45. Chawla, A., Kelloway, E.K.: Predicting Openness and Commitment to Change. Leadership & Organization Development Journal 25, 485-498 (2004)
46. Fussell, S.R., Kraut, R.E., Lerch, F.J., Scherlis, W.L., McNally, M.M., Cadiz, J.J.: Coordination, Overload and Team Performance: Effects of Team Communication Strategies. In: Proceedings of the 1998 ACM conference on Computer supported cooperative work, pp. 275-284. ACM, (1998)
47. Kashanchi, R., Toland, J.: Investigating the Social Dimension of Alignment: Focusing on Communication and Knowledge Sharing. In: ACIS 2008 Proceedings, pp. 2. (2008)
48. Calvert, C.: A Change-Management Model for the Implementation and Upgrade of ERP Systems. In: ACIS 2006. (2006)
49. Thomson, M.E., von Solms, R.: Information Security Awareness: Educating Your Users Effectively. Information management & computer security 6, 167-173 (1998)
50. Kotter, J.P., Schlesinger, L.A.: Choosing Strategies for Change. Harvard business review 86, 130 (2008)
51. Churchill Jr, G.A.: A Paradigm for Developing Better Measures of Marketing Constructs. Journal of Marketing Research 16, (1979)
52. Moore, G.C., Benbasat, I.: Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information systems research 2, 192-222 (1991)