

The need for improved alignment between actability, strategic planning of IS and information security

John Lindström, Sören Samuelsson, Dan Harnesk, Ann Hägerfors
Luleå University of Technology, 971 87 Luleå, Sweden, +46 920 491000

john.lindstrom@cdt.ltu.se, soeren.samuelsson@ltu.se, dan.harnesk@ltu.se, ann.hagerfors@ltu.se

Abstract: The purpose of this paper is to high-light problems regarding user actability and security implementations – what are the important mechanisms that affect actability in usage situations? Alignment between actability and strategic IS-planning and security issues is of the essence. However, serious gaps in alignment have been identified concerning strategic IS-planning as well as in development or implementation of security controls, and selection and use of security standards. The analysis of the alignment gaps show that there is a need to bring in the users view on business requirements in IS, or rather what they need to be allowed to do - to be able to work efficiently.

1. Introduction

New and innovative software tools that improve the operations of an organization regarding speed, quality and ability for collaboration internally as well as with external partners are needed by any organization and generally sought for. The goal is to find appropriate and organizationally approved software tools (IS) that increase actability to get better usability and efficiency. Many organizations today do not allow the IS users to work the way they would like to, which hinder the individuals' efficiency as well as impairs the organizations' efficiency and collaboration ability to externals like partners and customers.

Limiting the users' actability leads to impaired usability and efficiency. A few well-known problems regarding this matter are further described in the discussion section of this paper. Alignment is about achieving synergy between strategy, organization, processes, technology and people in order to sustain the quality of interdependence and thus achieve competitive advantage [1]. Aligning business strategy with IS strategy is problematic for organizations and is a key concern of senior management. However, alignment may be a moderating variable between IS use and organizational performance [2].

We have in practice observed that there is often a gap in the alignment between *actability* and:

- strategic planning of information systems (IS)
- security controls
- security standards

If the gap in the alignment is too big, we have observed that users will try to increase their actability by finding ways to bridge or circumvent the limiting factors. This may lead to undesigned systems; "that are informal, have no specification, may not be authorized and operate through informal and undefined interactions between individuals and groups" [3], or ICT-infrastructures not compliant to the decided security controls - creating negative value for an organization from an information security perspective. This problem is also discussed in [4, 5].

Lindstrom and Lundkvist discusses in [4] that there are more IT- and information security controls in large organizations than in small and medium sized enterprises (SME:s). This hinders the usage

of Collaboration Working Environment (CWE) tools when SMEs work together with large organizations. This leads to decreased actability. Also brought up in that paper is that employees that are used to be able to use CWE-tools like Skype or ICQ at home, expect to be able to use something similar at work and will start to find ways to use CWE-tools at work even though not allowed. This paper will continue to build on the work in [4] but from the perspective of alignment between actability to strategic planning of IS, security controls and security standards.

2. Actability, strategic planning of IS and information security

Ågerfalk in [6] states *“that in order to design for usage quality we must have a proper understanding of security aspects and the business, its action structure as well as both internal and external actors and their professional language use. There is a ‘requirements gap’ or at least mismatch between business modeling and system modeling”*. Argued further is that *“the main concept of this dissertation, information system actability, can be used as an ‘intellectual tool’ in bridging the requirements gap”*.

Dhillon in [5] discusses challenges and principles in managing information security. The challenges are classified in four categories:

1. Establishing good management practices in a geographically dispersed environment and yet being able to control organizational operations
2. Establishing security policies and procedures that adequately reflect the organizational context and new business processes
3. Establishing correct structures of responsibility
4. Establishing appropriate information technology disaster recovery plans

The principles are of three classes:

1. Managing the pragmatic aspects of an organization
2. Managing the formal rule based aspects of an organization
3. Managing the technical systems

Dhillon discusses managing information security and states principles that should cover most areas discussed in the challenges, whereas we in this paper discuss an actability alignment problem when managing information security. Dhillon mentions that security should guarantee “useful activities” in principle class 3.

Kankanhalli et al in [7] discusses that organizations become increasingly dependent on IS for strategic advantage and operations, the issue of IS security also becomes increasingly important. In the interconnected electronic business environment of today, security concerns are paramount. Further, small and medium-sized enterprises were found to engage in fewer deterrent efforts compared to larger organizations and organizations with stronger top management support were found to engage in more preventive efforts than organizations with weaker support from higher management. Stated is also that financial organizations were found to undertake more deterrent efforts and have stiffer deterrent severity than organizations in other sectors. Moreover, greater deterrent efforts and preventive measures were found to lead to enhanced IS security effectiveness.

The work in [7] indicates that users in larger organizations have smaller actability compared to smaller organizations. The empirical study in [7] shows that SME:s were found to engage in fewer deterrent efforts than larger organizations, that organizations with strong support from top management engage in more preventive efforts than those with weaker support, and that financial organizations have a higher level of security. Greater IS security effectiveness was achieved when undertaking more deterrent efforts and stiffer deterrent severity. This paper discusses where gaps in the alignment between actability to strategic planning of IS and security controls may arise - and one contributing factor may be the size of the organization as indicated in [7]

Kolkowska et al in [8] have in their literature review looked at the conflicts between usability and information security. The paper discusses among many things that administrators are struggling to maintain adequate security and at the same time they have to consider users’ (and business) requirements of accessibility, privacy and usability. Further, the paper discusses also that solutions

to problems with configuration and administration of security products are for instance to consider usability in the design and choice of security mechanisms. Suggested is to consider users perception in planning and implementations of access control. Security mechanisms incompatible with these perceptions may be circumvented by users and thereby undermine system security overall. The work in [8] had the perspective of usability and information security, whereas this paper discusses the alignment between actability, strategic planning of IS and information security on a higher level.

Tettero et al. in [9] means that the security requirements are based on the overall security view of the organization, as set out of policies. Also argued is that the requirements must be defined by the users or the management in such a way that they fit the organization. Both approaches are based on the expectation that the actors and clients know all the requirements related to security. This requires education of the actors to express the security requirements.

This paper considers that there are more factors to consider than in [9] affecting actability in IS. This paper also means that it is important to understand how security related factors may affect the actability when using IS.

As a reaction from business process modelling used today where shortcomings concern security requirements, Zuccato in [10] argues for a holistic security requirements engineering process using three different sources:

1. Risk analysis and the security management standard
2. Functional/non functional requirements
3. A holistic set of security requirements.

Zuccato means that combining different sources as risks, business processes, stakeholders and environmental demands get a holistic set of security requirements. We agree with Zuccato that today there are shortcomings regarding security requirements.

3. Methodology

The research presented in this paper is mainly conceptual and based on existing security and IT-alignment literature. However, a few focused discussions with practitioners have verified the identification of a knowledge gap concerning actability in both security and alignment research of today.

The literature review revealed that areas such as strategic planning of information systems, security controls, and security standards are chiefly concerned with characteristics of the areas as such, and less concerned with the relationship between the areas, which would be the alignment between the areas from an actability point of view.

In order to verify the literature review we also did interviews with four (4) project managers and four (4) end-users that have great experience in security implementations in large organizations. The interviews were semi-structured in so that the informants could give input regarding IT-security architectures implementations. Specifically, the informants was able to provide data for what kind of tools different implementations have used, what kind of needs end-user required, how they were using tools for working together and performance of work tasks as well.

The approach of combining conceptual review with semi-structured interviews increased the validity of our research concerning alignment of different security areas. In so doing we aligned our research methodology to the concept of theoretical validity and interpretative validity [11].

Theoretical validity refers to the explanation of the phenomenon studied, and not only a description of the facts or an interpretation of the underlying meaning. This type of validity is concerned with the theories or concepts used to explain the meanings of action are explicitly related to studied phenomenon. Most important is that the chosen theories can be presumed to reveal a true picture of the contextual conditions that is subject of inquiry. Interpretative validity is meaning oriented concept and accounts for the abstractions that is employed by informants rather than theoretical abstractions. By combining these two concepts of validity we were able to create meaning of the phenomenon under study, i.e. actability.

4. Alignment

Alignment is seen to assist a company by positioning the IT strategy in a closer relation to the business strategy. The outcome of this relationship is improved IT effectiveness and higher profitability [12, 13, 14, 15, 16, 17]. Three trajectories have been defined in alignment research: the return on IT-investment, the way that IT can provide direction and flexibility to react on new opportunities, and the social dimension of information alignment.

The research on investments in IT explores alignment via the economic perspective. Both positive and negative effects are identified of the value-relationship between IT and the business. For example, Hitt and Brynjolfson in [18] did not find a positive link between the amount of money spent on IT and profitability of the firms. Also, technology is typically treated as a cost centre or viewed as an expense rather than an enabler of business value [19]. The issue of whether IT brings any value to the business is seen as a matter of return-on-investments. Markus and Soh in [20] argues that IT-assets is something that not necessarily improve organizational performance but if structural factors such as firms size and information intensity is taken into account, then the spending in IT may improve performance. Other research on the value that IT brings to the business has specified that IT increases productivity and customer value [21, 22]. Clearly, when organizations stress the importance of managing customer relationships and how they internally correspond to its environment, the IT value may be enhanced by finding the right fit between external positioning and internal arrangements [23]. Papp in [24] suggests that this can be achieved by setting managerial focus on the relationship between IT and core competences and IT scope.

The second trajectory is concerned with developing competitive advantages and flexibility to react on new opportunities. Research in this group employs a strategic management perspective in which alignment is explored from the perception that the business and IT should contain statements that visualizes how IT is linked to the business. The outcome of strategic alignment is excellence in firm performance [15, 16, 25]. Blili and Raymond in [26] outline a formalized approach for IT alignment in SME:s, in which threats and opportunities and critical success factors are supposed to guide managers in their attempts of making strategic business use of information technology. Often these perspectives are explored via a resource based view of the firm. This is an approach to evaluate the firm's resources as a base for its strategy, and subsequently alignment is viewed as a means to allocate valuable IT resources. In detail, resources include technical, human, and intangible factors [27, 28, 29, 30]. Technical resources are i.e. databases and IT-infrastructure. Human resources are i.e. skills of IS professionals. Intangible resources are i.e. the partnership between IT and business units.

In addition, there are work in IT alignment that differs from the above mentioned discourses. Some work build on the underlying social assumption that there are shared norms and harmony of interest between parties that influence the relationship, which leads to, for example, trust issues that is not conveyed by the strategic management and the economic perspective. Research in this group show an alternative view of alignment by extending the focus beyond strategic planning and transaction costs to include issues, such as, knowledge sharing among groups of humans [31]. Reich and Benbasat in [32] also emphasize the social dimension of information alignment as they study factors for alignment between business and information technology objectives. Examples of these factors are: work experience among IT managers, and education level. Konsynski and Tiwana in [33] emphasize the need for new perspectives on IT alignment and argue for a move from alignment to aligning, meaning that an inter-firm relationship is an ongoing process and not a discrete event where managers' mechanistically use classical notions of strategy formulation. While such new ideas, or rather focus of interest, are emerging in research of IT alignment it is still biased by the strategic management focus and the intra-organizational focus.

We have developed a model used to discuss the gap in alignment between actability to strategic planning of IS, security controls and security standards, bearing in mind the alignment theories and looking at the alignment from an IT- and information security perspective.

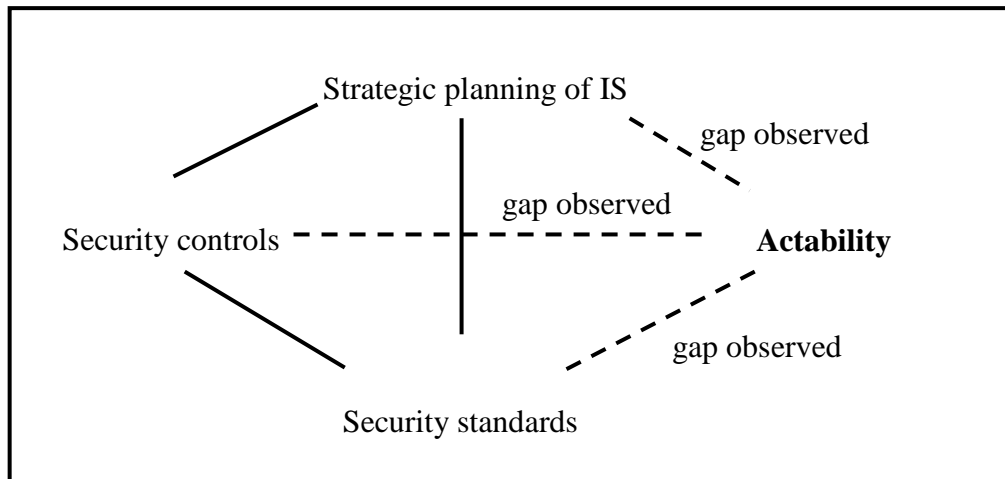


Figure 1: Alignment gaps between user actability, strategic IS-planning, security controls and security standards from an information security perspective

4.1 Actability, usability and efficiency

Actability has been defined by Goldkuhl and Röstlinger [34] as “*an information system’s ability to perform actions, and to permit, promote and facilitate the performance of actions by users, both through the system and based on information from the system, in some business context. The ‘degree’ of actability possessed by a certain IS is always related to the particular business context.*” Goldkuhl and Ågerfalk in [35] adds that “*The business context includes actors’ pre-knowledge and skills relating both to the IS and the business task to be performed. Therefore, IS actability is **not a static property of an IS**, but depends on the social structures surrounding it. Please note that the issue is not whether usability should be considered part of actability, and actability an extension of usability, or vice versa. The issue is to make information systems more actable and thus more usable.*”

The theory of information systems actability includes a distinction between three type of IS usage situations; *Interactive usage situation* (where users performs actions interactively together with and through the system, like in a sales man’s dialogue with a customer using an IS sales tool), *Automatic usage situations* (where the system performs actions by itself based on predefined rules), and *Consequential usage situations* (where users performs actions based on the information from the system).

According to Goldkuhl and Röstlinger [34] a computerised system “*is an action system. It is both an instrument for performance of action and a support tool for humans to perform their actions. Information systems should be actable*”. Also Ågerfalk in [36] sees actability as an important information system quality “metric” – a concept that goes beyond usability. Cronholm et al. in [37] present actability as a concept that builds on usability to take the social context of human-computer interaction into account.

One definition of *usability* that is closer to the user actability perspective is that of ISO 9241-11 [38]: “*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*”. This definition includes context of use. A deeper comparison between the concepts of actability and usability is made by Levén in [39], Cronholm, Ågerfalk and Goldkuhl in [37], Goldkuhl and Ågerfalk in [35], Ågerfalk in [40], and Ågerfalk, Karlsson and Hjalmarsson in [41].

Thus, usability promotes an important perspective but needs to be extended and reinterpreted in order to put more emphasis on the business context in which the interaction is taking place. Information systems should be usable not only in the context of interaction but also in the context of business action (for all actors involved). In order to design for usage quality and actability we must

have a proper understanding of both security aspects and the business; its action structure as well as both internal and external actors and their professional language use.

Adler and Winograd in [42] means that the importance regarding *efficiency* is how well a system supports higher level cognitive processes including the social interaction within an organization. *Efficiency from an actability terminology* is primarily comprised of the actors' and organizations' ability to create values by conducting actions both within and outside the organization.

4.2 Strategic planning of IS

Strategic planning of IS can be defined as by Ward and Griffiths in [43] like "*the planning for long-term management and optimal impact of information,- in all its forms, information systems (IS) and information technology (IT), incorporating manual and computer systems, computer technology and telecommunications. It also includes organizational aspects of the management of IS/IT throughout the business.*"

Information technology has long been advocated to be a critical resource and as such understood as an enabling technology for organizations to accomplish business objectives at the micro level [44].

When considering the processes and information needs in an organization it is essential to have an understanding of the organization's current structure, relationship and the people it is composed of. These organizational dynamics form an important input to the planning process. It is necessary to understand the environment and its skills, resources, values, culture and social interactions, as well as the management style and its relationship with the external environment. These aspects become increasingly important when the magnitude and pace of change have implications for all aspects of the business [45]. If considered, these aspects may improve the actability.

Constantine in [46] means that "*the richest information and most advanced functionality is of limited value if it is not useful and easily used within the context in which it is needed*". The users' situation needs to be factored in during the strategic planning of IS as otherwise an organization may get advanced IS that is not supporting the users in an optimal way (i.e. increasing their actability) or just have very limited usefulness.

Other research shows that there is alignment problems between more entities in the model described in figure 1. Doherty and Fulford discuss in [47] that the alignment between strategic planning of IS and security policies (i.e security controls) is often missing, whereas if addressing the alignment it could give six benefits raising the security level. Further nothing is mentioned about actability in the model they introduce.

Sipponen discusses in [48] that there are problems in the alignment between strategic planning of IS and security standards in the aspect of action research where information on how the objectives of security standards are attempted to be met in organizations where they are applied. The four security standards analyzed do not state what is needed regarding strategy and alignment and are only baselines.

4.3 Security controls

One definition of IT- and information *security controls* is that of [49] where the controls are divided into three different parts: administrative, technical (logical) and physical, which combined should work in a synergistic manner to protect an organization's assets against risks. Reducing or mitigating risk is part of the risk management process of any organization, where the intention is to mitigate the risks an organization faces using different perspectives as business impact, cost/benefit, customer or partner confidence etc.

Höne and Eloff discuss in [50] that the alignment between security policies (i.e. security controls) and security standards is good since security standards provide a starting point for determining what the information security policy should consist of. However, the security standards are not comprehensive in their coverage and tend to rather address the processes needed for successfully

implementing the information security policy. Also stated is that the information security policy must fit with the organization's culture and must therefore be developed with this in mind.

The combination of security controls used in an organization should be based on risk management, and senior management needs to decide a level of security where the risk mitigation is acceptable since it is not possible for most organizations to reduce or handle all risks. Handling all risks is too costly and time consuming to do, especially in a dynamic environment affected by both internal and external changes. Straub and Welke in [51] describe a planning model for management decisions to cope with system risks, which could be used by organizations to help select an efficient combination of security controls to manage and reduce system risks.

4.4 Security standards

IT- and information *security standards* can be defined as by Wool in [52] that “*security experts have long been saying that secure systems, and especially security standards, need to be designed through an open process, allowing review by anyone. ... Unfortunately, even openly designed standards sometimes result in flawed ... systems. A standards body involves many parties with conflicting agendas, many of them powerful corporations. Furthermore, a standard is not measured by excellence or novelty. It should be a working design that is an acceptable compromise between the interests of all the parties involved. In short, a standards body is not an environment that encourages scientific discourse. Finally, even supposedly open standards bodies sometimes have onerous requirements that may discourage scientists from participating*”.

Sipponen in [53] means that information security management standards, focus on the existence of processes and not the content of what it is securing. Information security management standards like ISO 17799, GASPP and SSE-CMM which are widely used and advocated by researchers and practitioners have a limitation in that they focus on ensuring that security processes exist while being unconcerned about how these security processes can be accomplished in practice.

We have looked at what is stated in some of the most common standards on the alignment between actability to strategic planning of IS, security controls and security standards. The reason for doing this is to find out if there is any guidance to also include the aspect of actability in the security work.

Many standards and frameworks like NIST, ISO 17799, and CISSP states that usability should be considered together with business requirements. However, nothing regarding actability has been found. This could be explained by the fact that usability is attributive in nature while actability is relational oriented. Security standards are often also used as input to for instance security policies (security control). Below are some more specific statements found in the NIST, ISO 17799 and CISSP.

NIST

Souppaya et al. in [54] stresses that “*the testing configuration of the IT product should match the deployment configuration. In some cases, a security control modification can have a negative impact on a product's functionality and usability, or on other products or security controls. Consequently, it is important to perform testing to determine the impact on system security, functionality, and usability, and to take appropriate steps to address any significant issues*”.

Wack et al. in [55] states about psychological acceptability “*...the security mechanisms in place should present users with sensible options that will give them the usability they require on a daily basis. If users find the security mechanisms too cumbersome, they find ways to work around or compromise them.*”

ISO 17799

The ISO 17799:2005 [56] standard states that information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment and business opportunities.

ISO 17799 is a code of practice for information security management and the structure of ISO 17799 is that it provides a list of security requirements an organization should satisfy if they want to undergo certification. The requirements are grouped in ten key controls. The idea behind the key controls is that an organization should have a balanced approach towards security covering the most critical areas.

Information security is achieved by implementing a suitable set of controls. These controls need to be reviewed and improved to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

CISSP

One "practioners industry frameworks" is the CISSP (Certified Information Systems Security Professionals) guidelines of the (ISC)²-organization¹. In one of the most popular books used to prepare for the certification exam [49] the following were found:

- An example of security management states that needed when securing an environment is still to allow the necessary level of functionality so productivity is not affected.
- The Availability in the CIA-triad (Confidentiality, Integrity and Availability) should "ensure reliability and timely access to data and resources to authorized individuals".

It could be argued whether the impact from security standards on user actability is direct or indirect. A security standard may have direct impact via a system security policy, for instance password policy, or indirect via an organizational security policy.

5. Discussion

Our focus is horizontal rather than vertical, i.e. the relations are important for actability rather than fit between formulas such as strategic planning of IS and security standards. Thus the concept of alignment is better suited for our purposes than the concept of usability. There is a body of literature concerning actability and one concerning usability in connection with our other key concepts; strategic planning of IS, security controls and security standards. The combination of these key concepts with actability makes it possible for us to further explore alignment gaps.

According to our literature review, IT-Alignment is seen to assist a company by positioning the IT strategy in closer relation to the business strategy of a company. The outcome of this relationship is better IT effectiveness and higher profitability [12, 13, 14, 15, 16, 17] and identifies two trajectories in alignment research: The return on IT-investment, and the way that IT can provide direction and flexibility to react on new opportunities.

Our problem discussion on alignment between actability and the different levels of security follows the IS management trajectory which aims to explain how organizations can act and react on changes in the environment. In that respect, this paper outlines the importance of, not only, considering the strategic levels when discussing alignment, but also to incorporate technical and matters of standardization in such discussion.

There is a need to include groups of users with advanced requirements on user actability during planning of IS and implementations of security controls and security standards. The users' requirements on actability, i.e. the business requirements, need to be factored into the process during the initial requirement gathering, during the implementation and testing, as well as after a period of practical use when having found out limitations and missing functionalities needed.

Users in larger organizations often have smaller actability than users in SME:s. As it seems like organizations more and more use IS to get a strategic advantage, the security concerns grow accordingly. SME:s engage in fewer deterrent efforts, especially when top management is not

¹ For more information on CISSP and the (ISC)²-organization, please visit: <https://www.isc2.org/cgi-bin/index.cgi>

explicitly supportive of such efforts [7]. Organizations with strong support from top management seem to engage in more preventive efforts than those with weaker support [7]. One question that arises is if it is possible to keep the users' actability in an organization as the organizational size grows and the dependency to IS increases, or if it is too hard or costly to do?

Theoretical support for alignment of usability, strategic planning of IS and information security is vast. A proper understanding of the business, its actors and conditions is necessary in strategic IS-planning and development of security controls and standards. Understanding of the organizational dynamics, skills, resources, values, culture, social interactions, management style and external environment is important for the planning processes. Any added functionality in IS must be useful and easily used within the context in which it is needed.

The information security policy must fit in with the organization and its culture and both users and business requirements should be considered when deciding on security controls and standards.

When implementing security controls and standards, testing of their impact is needed to get a good or at least acceptable result. If possible, users should be presented with options that give them the actability they require. Security controls must be implemented and security levels must be set so that the necessary levels of functionality are acquired and productivity is not negatively affected.

We have however in practice identified, both in own research and reports from other research efforts, a number of alignment gaps. Alignment between strategic planning of IS and security policies is often missing. Alignment between strategic planning of IS and security standards is poor due to the standards not providing guidelines for alignment. Many organizations today do not allow the IS users to work the way they would like to, which hinder the individuals efficiency as well as impairs the organizations' efficiency and collaboration ability to externals like partner and customers. Security standards do not provide support alleviate solutions to this problem since they mostly focus on security processes rather than how the processes can be realized.

Users might need or would like to use software tools that for security reasons are deemed as not approved. For instance, the Sarbanes-Oxley Act requires a paper trail of all instant messaging (IM) traffic for corporations under the supervision of the United States Securities and Exchange Commission (US SEC), browser and http protocol problems, web mail security, IM-tool flaws, unsecure voice over IP (VoIP), H.323 and session initiation protocol (SIP) vulnerabilities [4]. These user needs should not be ruled out before a check has been conducted if there are appropriate security solutions that handle the issues or if there are other similar software tools without the security issues that could be used instead. Organizations need to get better to exploit possibilities to improve actability and not by default rule out new opportunities by stating that "our security policy will not allow that".

Another question is how should small groups with a larger need of actability be handled within an organization? One example is groups with very outgoing tasks and that work on an international basis. Another example may be sales executives, industrial or academic researchers that likely have a much larger need than internal administrators. As mentioned earlier, if actability is impaired it is likely that some users will try to increase their actability by bridging or circumventing the limiting factors if they need it to do their work. This may lead to undesigned systems or IT infrastructures non compliant to the decided security controls – leading to negative value for the organization looking at it from an information security perspective. From other perspectives like efficiency, the increased actability from undesigned systems may however be considered as beneficial.

Looking at the alignment gaps discussed in figure 1 from a rather practical point of view, we can find examples of gaps in our own working environments like:

- Actability - strategic planning of IS: The user's needs or requirements (business requirements) on IS are not part of the process of strategic planning of IS. Strategic planning of IS need to look beyond the properties of IT and acknowledge human action as a vehicle to sustain compliance with user needs.
- Actability - Security controls: Security policies do not allow the usage of IM-tools like Skype, ICQ and poorly selected and configured antivirus, boot protection software etc. that

hangs the personal computer or almost makes work outside of the ordinary LAN impossible limiting the users' work (that depend on an IS-environment with good actability to be able to conduct the daily business). Thus security controls need to take into account user needs as well as be well developed and implemented in the organization.

- Actability - Security standards: The organizational information security policy states that the security management should comply with the ISO 17799 standard (or the Swedish adaptation called BITS), rendering the users to work in an environment where actability is not part of the (important) input to the security processes affecting the users. It could be explained by the fact that security standards are universal concepts without connection to contextual settings. Security standards are attributive and therefore easy to use when guiding policy writings, often used for check-outs to ensure comprehensiveness of policies, for example in certification matters.

6. Conclusions

The alignment problem high lighted in this paper needs to be considered by any organization to both keep their users happy and working efficient, as well as maintain an IS environment that complies to the organizational security controls and selected security standards. Actability need to be considered in the strategic planning of IS, development or implementation of security controls, and selection and use of security standards. Otherwise, the problem with poor alignment is likely to arise leading to impaired actability.

If the users need or would like to use software tools that for security reasons are not approved, they should not be ruled out before it has been investigated if there are appropriate security solutions that handle the issues or if there are other similar software tools without the security issues that could be used instead. Organizations need to get better to exploit possibilities to improve actability and not by default rule out new opportunities by stating that "our security policy will not allow that".

It seems that there is a need to bring in the users' view on business requirements in IS, or i.e. what they need to be able to do to work efficiently, and in the security related work in organizations when users' actability is affected. As this is a problem, we need to get better at implementing security and security processes in practice [53] as otherwise security will be something that frustrates users and makes them find ways around the security controls [4].

7. Future work

How to avoid frustrated users, impaired productivity and deficiencies in efficiency by investigating the gap in alignment between actability, strategic planning of IS, security controls and security standards is an interesting area for further research. Of interest is also if and how different situations, contexts and user groups could be used to decrease the alignment gaps at design and development of new IS, change of existing IS, and implementations of security controls in an existing IS/IT environment.

Avison et al in [57] have created a model to measure alignment, and it would be interesting to use if adapted to measure alignment regarding actability.

8. References

- [1] R. Hsaio and R. Ormerod; A New Perspective on the Dynamics of IT-Enabled Strategic Change, *Information Systems Journal*, 8(1), pp21-52, 1998
- [2] Y. Chan, S. Huff, D. Barclay and D. Copeland; Business Strategy Orientation, *Information Systems Research*, 8(2), pp125-150, 1997
- [3] P. Checkland; *Systems Thinking, Systems Practice*. Chichester, UK: Wiley, Publisher: John Wiley & Sons Ltd, April 22 1981, ISBN-10: 0471279110
- [4] J. Lindström and A. Lundkvist; CWE from an SME Perspective; from the proceedings of the 12th International Workshop on Telework in Lillehammer, Norway, Aug 2007
- [5] G. Dhillon; Challenges in managing information security in the new millennium", in Dhillon, G. (Eds), *Information Security Management*, Idea Group Publications, Hershey, pp1-9, 2001
- [6] P. J Ågerfalk; *Information Systems Actability: Understanding Information Technology as a Tool for Business Action and Communication*. Doctoral Dissertation. Department of Computer and Information Science, Linköping University, 2003, Printed in Sweden by UniTryck, ISBN: 91-7373-628-7. (Nominated for ACM SIGMIS Doctoral Dissertation Award Competition 2003)
- [7] A. Kankanhalli, H. Teo, B. C. Y. Tan and K. Wei; An integrative study of information systems security effectiveness, *International Journal of Information Management*, Volume 23, Number 2, pp139-154(16), April 2003
- [8] E. Kolkowska, J. Aderud and P. Oscarson; Conflicts between usability and information security – a literature review; Proceedings of the 26th Information System Research Seminar in Scandinavia (IRIS 26). Haikko Manor, Finland, 9-12 august 2003
- [9] O. Tettero, D. Out, H. Franken and J. Schot; Information security embedded in the design of telematics systems. *Computers & Security*, 16(2):145-164, 1997
- [10] A. Zuccato; *Holistic Information Security Management Framework for electronic commerce*, Doctoral thesis, 2005, ISBN 91-85335-63-0
- [11] J.A. Maxwell; Understanding and Validity in Qualitative Research, *Harvard Educational Review*, (62:3), pp279-300, 2002
- [12] M. E. Porter; From competitive advantage to corporate strategy, 15–31, *Harvard Business Review* 1987
- [13] J. N. Luftman; *Competing in the Information Age: Strategic Alignment in Practice*, Oxford University Press, New York. 1996
- [14] C. U. Ciborra; De Profundis? Deconstructing the concept of strategic alignment, *Scandinavian Journal of Information Systems*. 9(1), pp67-82, 1997
- [15] M. Levy, P. Powell and P. Yetton; SMEs: Aligning IS and the Strategic Context, *Journal of Information Technology*, 16, pp133-144, 2001
- [16] P. B. Cragg, M. King and H. Hussin; IT Alignment and Firm Performance in Small Manufacturing Firms, *Journal of Strategic Information Systems*, (11), pp109-132, 2002
- [17] D. Avison, J. Jones, P. Powell and D. Wilson; Using and validating the strategic alignment model, *Journal of Strategic Information Systems* 13, pp223–246, 2004
- [18] L. M. Hitt and E. Brynjolfsson; Productivity, business profitability, and consumer surplus: three different measures of information technology value, *MISQ* 20 (2), pp121–142, 1996
- [19] N. Venkatraman; Beyond Outsourcing: Managing IT Resources as a Value Center, *Sloan Management Review*, Spring 38 (3), pp51–64, 1997
- [20] C. Soh and M. L. Markus; How IT Creates Business Value: A Process Theory Synthesis, from the proceedings of the 16th International Conference on Information Systems, pp29-41, December 1995
- [21] P. P. Tallon and K. L. Kraemer; Executives' Perspectives on IT: Unraveling the Link between Business Strategy, Management Practices and IT Business Value, from the proceedings of Americas Conference on Information Systems (ACIS2002). 2002
- [22] P. Weill, M. Broadbent and D. St Clair; *Strategic Alignment*, Oxford University Press, New York. 1996
- [23] C. U. Ciborra; *Teams, Markets and Systems: Business Innovation and Information Technology*, Cambridge University Press. 1993
- [24] R. Papp; *Strategic Information Technology: Opportunities for Competitive Advantage*. IDEA Publishing, 2001
- [25] J. C. Henderson and N. Venkatraman; Strategic Alignment; A Model for Organizational Transformation Through Information Technology, in Kochan, T.A. and Useem, M. (eds.). *Transforming Organizations*. New York: Oxford University Press. 1992
- [26] S. Blili and L. Raymond; Information Technology: Threats and Opportunities for Small and Medium sized Firms, *International Journal of Information Management*. 13, pp439-448, 1993
- [27] P. G. W. Keen; Information technology and the management difference: a fusion map, *IBM Systems Journal* 32 (1), pp17–39, 1993

- [28] J. Peppard and J. Ward; Beyond strategic information systems: toward an IS capability, *Strategic Information Systems* Vol. 13, pp167–194, 2004
- [29] B. H. Reich and I. Benbasat; Factors that Influence the Social Dimension of alignment Between Business and Information Technology Objectives, *MIS Quarterly*, Vol. 24, No.1, pp81-113, 2000.
- [30] G. Bassellier and I. Benbasat; Business competence of information technology professionals: conceptual development and influence on IT-business partnerships, *MIS Quarterly*, (28:4), pp394–673, 2004
- [31] K. M. Nelson, and J. G. Coopridge; The Contribution of Shared Knowledge to IS Group Performance, *MIS Quarterly*. Vol. 20, No. 4, pp409-432, 1996
- [32] B. H. Reich and I. Benbasat; Measuring the linkage between business and information technology objectives. *MIS Quarterly*, Vol. 20 no. 1, pp55-81, 1996
- [33] B. Konsynski and A. Tiwana; The improvisation – efficiency paradox in inter-firm electronic networks: Governance and architecture considerations, *Journal of Information Technology*, Vol 19, Issue 4, pp234-243, 2004
- [34] G. Goldkuhl and A. Röstlinger; Towards an integral understanding of organisations and information systems: Convergence of three theories, from the proceedings of the 5th International Workshop on Organisational Semiotics, Delft accepted to the 3rd European Conference on Knowledge Management (3ECKM), Dublin, 2002
- [35] G. Goldkuhl and P. J. Ågerfalk; Actability: A Way to Understand Information Systems Pragmatics, In *Coordination and Communication Using Signs: Studies in Organisational Semiotics 2*, (Eds, Liu K, et al.) Boston: Kluwer Academic Publishers, 2002, pp85–113. An earlier version was presented at the 3rd International Workshop on Organisational Semiotics (WOS'3). Stafford, UK, July 4, 2000.
- [36] P. Ågerfalk; Researching the applicability of actability, Towards an Improved Understanding of Information Systems as Tools for Business Action and Communication, from the proceedings of the Conference for the Promotion of Research in IT at New Universities and University Colleges in Sweden, 23–25 April 2001, Ronneby, Sweden, Vol. 1: Scientific Contributions, (Ed, Bubenko J A, jr.), pp216–225.
- [37] S. Cronholm, P. Ågerfalk and G. Goldkuhl; From Usability to Actability, from the proceedings of the 8th International Conference on Human-Computer Interaction (HCI International'99), 22–27 August 1999, Munich, Germany
- [38] ISO 9241-11; Guidance on Usability, 1998
- [39] P. Levén; Från användning till handling.: Om kvalitet i ett marknadsorienterat informationssystem (in Swedish), Licentiate thesis, 1995, ISSN: 0282-0579
- [40] P. J. Ågerfalk; Actability Principles in Theory and Practice, from the proceedings of the 8th International Working Conference on the Language-Action Perspective on Communication Modelling (LAP 2003), 1–2 July 2003, Tilburg, The Netherlands, (Eds, Weigand H, et al.), pp95–114. An earlier version appeared in Proceedings of the Third Conference for the Promotion of Research in IT at New Universities and University Colleges in Sweden (Promote IT 2003), 5–7 May 2003, Visby, Sweden.
- [41] P. J. Ågerfalk, F. Karlsson and A. Hjalmarsson; Exploring the Explanatory Power of Actability: The Case of Internet-Based Software Artefacts, In *Organisational Semiotic: Evolving a Science of Information Systems*, Proceedings of the IFIP WG 8.1 Working Conference on organizational semiotics: Evolving a Science of information systems, pp1-20, 23-25 July 2001. Montreal, Canada, (Eds, Liu K, et al) Norwell, MA: Kluwer Academic Publishers
- [42] P. Adler and T. Winograd; The Usability Challenge. Chapter 1 in *Usability: Turning Technologies into Tools*, edited by Paul S. Adler and Terry Winograd. Paul Adler and Terry Winograd (eds.) Usability: Turning Technologies into Tools Oxford, 1992
- [43] J. Ward and P. Griffiths; *Strategic planning for information systems*, Wiley. 1996
- [44] M. J. Earl; *Management strategies for information technology*, Prentice-Hall. 1989
- [45] J. Ward and J. Peppard; *Strategic planning for information systems*, Wiley. 2002
- [46] L. Constantine; Enterprise Information Systems for use: From Business Processes to Human Activity, from the proceedings of the International Conference of Enterprise Information Systems, ICEIS'07, Madeira, Portugal 2007
- [47] N. F. Doherty and H. Fulford; Aligning the information security policy with the strategic information systems plan, *Elsevier - Computers and Security* 25, 2006
- [48] M. Sipponen; Technical Opinion – Information security standards focuses on the existence of process, not its content, *Communications of the ACM*, Aug 2006/Vol. 49. No 8, 2006
- [49] S. Harris; All-in-one CISSP certification exam guide, second edition, pp50-51, 2003, ISBN 0-07-222966-7
- [50] K. Höne and J. H. P. Eloff; Information security policy – what do international information security standards say?, *Computers & Security*, Vol. 21 (5), pp402 – 409, 2002

- [51] D. W. Straub and R. J. Welke; Coping With Systems Risks: Security Planning Models for Management Decision Making, MIS Quarterly, Vol. 22, Issue. 4, pp441-469, 1998
- [52] A. Wool; Inside risks: Why security standards sometimes fail, Communications of the ACM, Volume 45 Issue 12, 2002, Publisher: ACM Press, ISSN:0001-0782
- [53] M. Sipponen; Information Security Management Standards: Problems and Solutions, The DATA BASE for Advances in Information Systems 69 Volume 38, Number 1, February 2007.
- [54] M. Souppaya, J. P. Wack and K. Kent; Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers, NIST Special Publication 800-70, May 2005.
- [55] J. Wack, M. Tracy and M. Souppaya; Guideline on Network Security Testing Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-42, October 2003.
- [56] ISO/IEC 17799:2005; Information Technology – Security Techniques – Code of Practice for Information Security Management
- [57] D. Avison, J. Jones, P. Powell and D. Wilson; Using and validating the strategic alignment model, Journal of Strategic Information Systems 13, pp223-246, 2004