Easing the Burden of Security Self-Assessments

Christopher Schmitz[1], André Sekulla[2], Sebastian Pape[1], Volkmar Pipek[2] and Kai Rannenberg[1]
[1] Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security, Germany
[2] University of Siegen, Institute of Information Systems, Germany
e-mail: {christopher.schmitz; sebastian.pape; kai.rannenberg}@m-chair.de
{andre.sekulla; volkmar.pipek}@uni-siegen.de

Abstract

A web-based platform was developed to support the inter-organisational collaboration between small and medium-sized energy providers. Since critical infrastructures are subject to new security regulations in Germany, the platform particularly serves for the exchange of experience and for mutual support in information security. The focus of this work is the security self-assessment component. In order to ease the burden of going through a long questionnaire we have implemented small, motivating modules that are spread across the platform. The data entered is used for an individual risk assessment but also for a fine granular inter-organisational security benchmarking which builds a common added value for the entire community on the platform and strengthens the community building process. We implemented a prototype of the platform and evaluated the it in a focus group.

Keywords

Security Management, Security Self-Assessment, Collaborative Knowledge Management

1. Introduction

Gathering information for risk and security self-assessments can be a cumbersome task. In general, the security managers need to answer an often long collection of questions built on established standards (e.g. Swanson 2001, ISO/IEC 27019, IEC 62443). For instance, the NIST security self-assessment contains more than 200 questions (Swanson 2001). Self-assessments offer advantages over external security audits: they are less expensive, they can be implemented in local organisational routines, and they allow more control on critical information about an organisations' IT infrastructure. But they are also challenging: the actors' bias towards the inner-organisational discourses may leave blind spots. Furthermore, analyses, as well as decisions for counter-measures, require a continuous improvement of competencies with regard to existing as well as future IT infrastructures and the related threats. These challenges are particularly relevant for small and medium-sized enterprises (SMEs) that provide infrastructural services, and which often do not have the capacities to run a full-fledged information security department and rely on external expertise (Dax et al. 2017).

In many areas, individuals and organisations with a local lack of expertise turn to support communities on the internet. These communities are not only valuable in offering their members concrete support to solve a specific problem, they also offer an interaction space to collaboratively consolidate and improve the general knowledge on the issues at stake, and offer additional problem solving strategies (e.g. by means of recommender systems, cf. Ackerman et al. 2013). This approach cannot immediately be transferred to areas with specific vulnerabilities, e.g. information security in power grid infrastructures. Framing conditions like the high sensitivity of the infrastructure-related information, legal or regulatory requirements, and the complexity of dependencies between grid technologies, IT systems supporting their management, and possible threats require a more cautious approach to unlock the helpful dynamics of community processes.

We have developed a platform for security managers supporting small and medium-sized energy providers. The central tool of this platform is a self-assessment component to support security managers to manage the recent legal requirements to monitor and improve the information security of their infrastructures. In our approach, users can model the existing information security measures of their infrastructure (in terms of security controls[1] following ISO/IEC 27001) using security maturity levels[2], which can then be compared and published in an anonymised way to the results from other participating organisations. The platform then provides information (in a Q&A section) on improving with regard to specific controls, as well as a controlled community section in which strategies of improvement can be discussed with other information security managers. We built small modules which are shown in other parts of the platform. Those modules allow the users to answer the questions or update the maturity levels along the way when interacting with other parts of the platform. By making use of motivational elements and showing questions one by one in other parts of the platform, we aim to ease the burden of going through a lengthy list of questions. This is especially the case when respondents update the answers entered and need to decide if the current answer is still valid. Lessons from other platforms showed, that structured processes of information consolidation and improvement through users help the perceived value of the information provided dramatically.

The remainder of this paper is organised as follows: Section 2 discusses related work, Section 3 gives an overview of our platform, and Section 4 discusses the connection of self-assessment with user motivation and community building. Section 5 reports about a brief evaluation. Section 6 concludes and outlines future research.

[1] A security control describes security requirements that can be fulfilled by performing the corresponding security measures. A control is associated with one or more security measures.

[2] Maturity levels can be used as a measure to quantify a control's protection level. The higher a control's maturity level, the higher is the chance that it is performed in a secure way.

2. Related Work

With the World Wide Web as a breakthrough technology, building knowledge communities became an actual practice in professional contexts (e.g. Lesser et al. 2000). Although these community platforms intended an open, flexible support for problem-solving processes, the delicacy of the social and business-related processes behind the "innocent" knowledge exchange very soon became apparent: Articulating a problem was often considered as uncovering a personal or organisational deficit, solutions that were offered came with unclear quality assurances, and the work of narrowing down a problem as well as developing a solution that would fit all local needs went far beyond simple "Q&A" patterns (Pipek and Won, 2003).

For platforms hosting knowledge communities, several strategies were developed to ease these problems. The idea of "FAQ" (Frequently asked questions) developed to relieve experts from answering the same basic questions over and over. It was combined with processes to keep them up to date (e.g. the "Answer Garden" system, Ackerman and McDonald 1996). Pipek and Won (2003) suggested to focus more on connecting users looking for a problem solution with experts who could help them, less on making knowledge explicit and store it online. For particularly sensitive issues, the anonymity of the person asking for help as well as of persons answering is guaranteed (e.g. patientslikeme.com).

Self-assessment as another technique to counter negative effects of "deficit disclosure", and even allows a continuous monitoring and improvement, has become a heavily discussed approach in learning communities (e.g. Castle and McGuire, 2010). To some extent, self-assessment approaches also help in organisational learning (e.g. in the general improvement of IT infrastructures, e.g. Curley 2004, in approaches of quality management, e.g. Saunders and Mann 2005, and – with regard to information security – e.g. Swanson 2001). But this was never done in combination with online support for knowledge communities. There exist the so-called "Information Sharing Analysis Centres" (ISACs). ISACs are organisations that gather and analyse security-related information from their members and provide them with analysis results and reports. In contrast to them our approach addresses the individual organisation and provides them with individual risk analysis and benchmarking scores. Furthermore, our platform enables a direct knowledge sharing.

3. The SIDATE Platform

Especially SMEs often struggle to achieve an adequate security level, although some of them are obliged to get certified against the ISO/IEC 27001. This holds for instance for energy providers and other critical infrastructures in Germany. A natural solution to support them is to stimulate collaboration. For this, we have built an inter-organisational collaboration platform for energy providers. It enables energy providers to assess their security level and to improve their security also by inter-organisational discussions. We systematically elicited the requirements in several workshops (Dax et al. 2016). The platform consists of four main components aiming to support knowledge sharing between the organisations:

- **Security measures catalogue:** The security measures component is a catalogue of security measures which is maintained by security experts. Users can comment on the measures, suggest new measures and rate them according to their costs, efficacy and usability.
- **Questions and answers:** The Q&A component should support and structure inter-organisational discussions. Registered users can ask security-related questions and can finally mark answers as correct. All users can rate questions and answers and can either sort them by rating or creation date. In order to have a more structured inter-organisational communication threads can be filtered according to tags or security controls.
- **Document sharing:** In the document sharing component the participating organisations can share relevant documents in a structured way, e.g. best practices or official documents specifying the binding legal requirements.
- **Security self-assessment:** The security self-assessment component constitutes the core component of the platform. Using this component, organisations can assess their security risk level in order to better understand their exposure to relevant security risks. Moreover, they can compare their security status (on different abstraction level) with that of similar organisations.

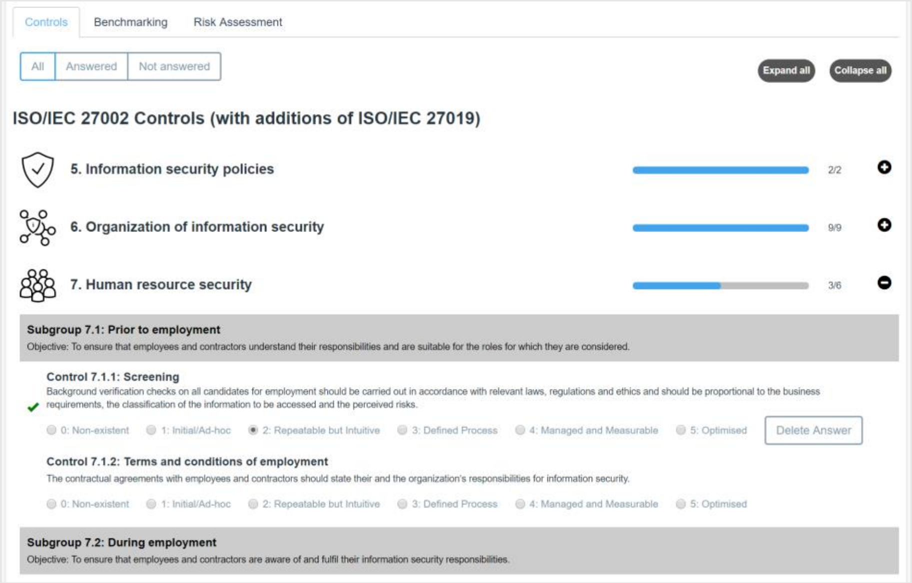
In the following, we focus on the self-assessment component which constitutes the central element of the platform. It consists of the three sections data input, benchmarking and risk assessment that are complemented by three superordinate modules being spread across the platform. We describe them below:

3.1 Data Input Section

The first step of the risk assessment process is to gather the required information. The necessary user data is entered in the data input section (see Fig. 1). The organisations model the security measures of their infrastructure by assessing the maturity levels of the implemented security controls (in terms of controls following the ISO/IEC 27001). Here, the widely known ISO/IEC 27019 security controls (which are more specific security controls for the energy utility industry) are used as questionnaire items. Since they equally address technical and organisational aspects of information security they represent a wide range of security measures that can be implemented in an organisation. The items are structured in the same categories and sub-categories the security managers already know from the original standard. The users are furthermore supported by the feature to show either all controls, only those controls that are not assessed yet or only those controls that have already been assessed which makes sense in order to check in a user-friendly way whether all controls are still up to date.

3.2 Benchmarking Section

The benchmarking section (see Fig. 2) enables organisations to compare their security status with similar organisations. Their maturity levels are juxtaposed (in an anonymised way) with that of other organisations.



ISO/IEC 27002 Controls (with additions of ISO/IEC 27019)

5. Information security policies 2/2

6. Organization of information security 9/9

7. Human resource security 3/6

Subgroup 7.1: Prior to employment
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

✓ **Control 7.1.1: Screening**
Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

○ 0: Non-existent ○ 1: Initial/Ad-hoc ● 2: Repeatable but Intuitive ○ 3: Defined Process ○ 4: Managed and Measurable ○ 5: Optimised Delete Answer

Control 7.1.2: Terms and conditions of employment
The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

○ 0: Non-existent ○ 1: Initial/Ad-hoc ○ 2: Repeatable but Intuitive ○ 3: Defined Process ○ 4: Managed and Measurable ○ 5: Optimised

Subgroup 7.2: During employment
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Figure 1: Data Input Section

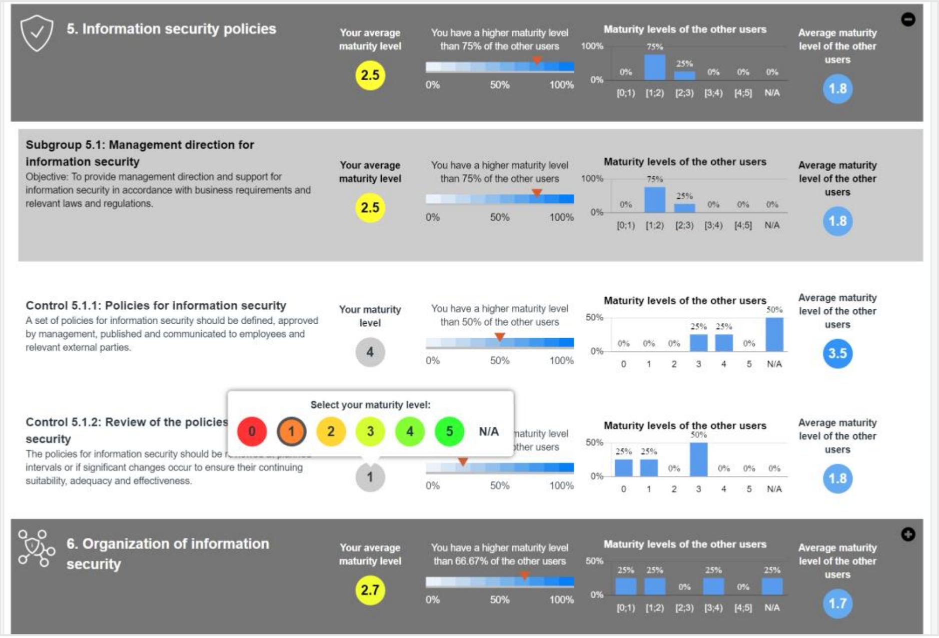
For each control, the organisation's maturity level is shown along with the average maturity level by the other organisations. For a more in-depth analysis, the distribution of maturity levels per control is also presented as well as a relative benchmarking score which indicates how well the organisation performs compared to the others. In this section, one can also re-assess the maturity levels. The benchmark is shown on different abstraction levels: on a control level and on the aggregated levels of the control groups and sub-groups of the ISO/IEC 27019. The groups and sub-groups are presented in the same structure as in the original standards, like in the data input section.

3.3 Risk Assessment Section

In the risk assessment section a scenario-based risk analysis is conducted to calculate the organisation's security risk score as well as the risk for a collection of relevant attack scenarios. This supports the security managers in identifying the most critical risks they are exposed to. Describing the risk assessment framework and the other data sources would go beyond the scope of this work.

3.4 Superordinate Modules

Additionally, we have implemented three superordinate modules directly supporting the self-assessment component. The modules are displayed in other components of the platform aiming to connect the different parts of the platform in order to stimulate the users to frequently assess respectively to re-assess security controls.



5. Information security policies

Subgroup 5.1: Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Control 5.1.1: Policies for information security

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Control 5.1.2: Review of the policies

security

The policies for information security should be r

intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Select your maturity level:

6. Organization of information security

Your average maturity level
2.5
You have a higher maturity level than 75% of the other users
0%
50%
100%
Maturity levels of the other users
100%
0%
0%
75%
25%
0%
0%
0%
[0;1)
[1;2)
[2;3)
[3;4)
[4;5]
N/A
Average maturity level of the other users
1.8
Your average maturity level
2.5
You have a higher maturity level than 75% of the other users
0%
50%
100%
Maturity levels of the other users
100%
0%
0%
75%
25%
0%
0%
0%
[0;1)
[1;2)
[2;3)
[3;4)
[4;5]
N/A
Average maturity level of the other users
1.8
Your maturity level
4
You have a higher maturity level than 50% of the other users
0%
50%
100%
Maturity levels of the other users
50%
0%
0%
0%
0%
25%
25%
0%
50%
0
1
2
3
4
5
N/A
Average maturity level of the other users
3.5
0
1
2
3
4
5
N/A
aturity level
ther users
1
0%
50%
100%
Maturity levels of the other users
50%
0%
25%
25%
0%
50%
0%
0%
0%
0
1
2
3
4
5
N/A
Average maturity level of the other users
1.8
Your average maturity level
2.7
You have a higher maturity level than 66.67% of the other users
0%
50%
100%
Maturity levels of the other users
50%
0%
25%
25%
0%
25%
0%
25%
[0;1)
[1;2)
[2;3)
[3;4)
[4;5]
N/A
Average maturity level of the other users
1.7

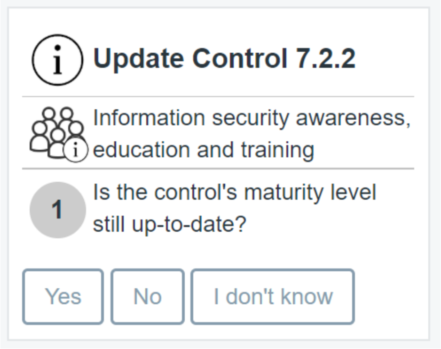
Figure 2: Benchmarking Section

Figures 3 and 4 show their graphical use interfaces. By requesting to keep the data complete and up-to-date we try to keep the entire data on a representative level.

1.) A control that has already been evaluated may have an obsolete maturity level and should be updated to obtain a more representative status. Therefore, the first module (see Fig. 3) requests the user to update resp. to re-assess a security control at regular intervals. This is also important from the perspective of information security management systems, since they require constant and iterative handling of information security measures.

2.) In case of missing maturity levels the second module requests the user to evaluate the security controls that have not been evaluated yet. In particular, the aim is to ensure that the data is complete. The more controls have been evaluated, the better the outcomes of the risk assessment and the better they can be compared with other results. The presented controls are further prioritized with regard to their information value for the risk assessment, e.g. to enable a new attack scenario in the risk assessment. The module also indicates such information.

3.) The third module, shown in Figure 4, is positioned in the security measures catalogue. While a user is viewing such a measure in detail, he or she gets asked to evaluate the respective security control for the self-assessment component. Again, this should improve the data completeness and up-to-dateness.

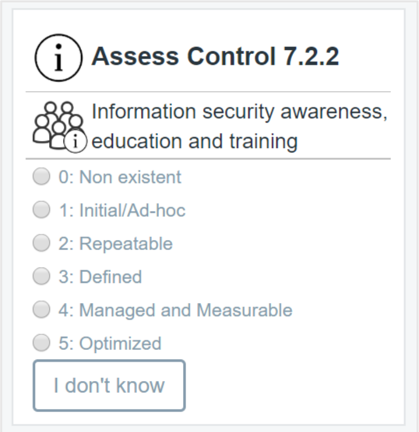


Update Control 7.2.2

Information security awareness, education and training

1 Is the control's maturity level still up-to-date?

Figure 3: Update Control Module



Assess Control 7.2.2

Information security awareness, education and training

○ 0: Non existent
○ 1: Initial/Ad-hoc
○ 2: Repeatable
○ 3: Defined
○ 4: Managed and Measurable
○ 5: Optimized

Figure 4: Assess Control Module

4. Usability Aspects

To improve interaction and activity in the SIDATE platform, the interaction between users need to be carefully planned. Looking at the individual user, a good usability and interesting collaboration anchors need to be provided. But it is also important to have the further development of the associated community in mind.

4.1. Motivating Updates and Additional Input

One way to increase activity on the online platform is to keep the entry barriers as low as possible (Girgensohn and Lee, 2002). The self-assessment tool serves as a guided entry to model the maturity level of an organisation’s IT security. Later changes can be easily made as soon as a user is logged in on the platform without the questionnaire. He can easily add further data and information to his information security status without having to navigate directly into the associated self-assessment module in order to additionally reach the subordinate category in such a way that he can evaluate the corresponding control.

Section 3 described the self-assessment component in more detail. The component does not include any community functions itself. Since this component may contain sensitive data, functions for exchange and interaction between users could be counterproductive. They could lead to falsified data or no input of the requested data being carried out. The modules presented below are primarily intended to ensure that the dataset entered is complete and up-to-date. This enables the self-assessment and the benchmarking to work properly on these data and make meaningful comparisons. Only after the own data has been entered, the other users' ratings become visible as a direct comparison. This should again increase the motivation to enter complete data.

The asses control module (Fig. 4) indicates that when the corresponding control is evaluated, a new attack scenario is activated within the risk analysis of the self-assessment module. This should increase the motivation to enter complete ratings and unlock a kind of success because “individuals are more likely to gain self-based achievement rather than enjoyment in the process of sharing knowledge" (Yang and Lai, 2010). Hence, while users are viewing such a measure in detail they get asked to evaluate the respective security control for the self-assessment module and the benchmarking process. Again, this should improve the up-to-dateness and data completeness and is implemented through the related control module.

4.2. Supporting the Community Building Process

The activity of the users of a platform is an important aspect of the community building process. Beside the user activity, another goal of an online platform for cooperation is the creation of added value for all parties involved. Girgensohn and Lee (2002) describe the so-called socio-technical-capital as "a resource produced as a side effect of technology-mediated social interaction". Resnick (2001) notes that it can be accumulated and made available to create value for people. It should influence the users among themselves in such a way that they interact more with each other. To encourage users to participate further, it is recommended to "repeat social interaction" (Kollock, 1996) which is implemented in particular with the help of additional modules directly related to the presented self-assessment module. It is intended to encourage users to constantly interact with the platform. The self-assessment itself has no functions for direct interaction between the users but the small modules have indirect effects on further interactions on the entire platform, as they allow for an anonymous comparison with the results others have provided.

If there is a need for an improvement in their own information security landscape, users can start to enter and participate in online discussions that are specific to the controls where deficits may be rooted in. It is not necessary to disclose that there are deficits in a user's own organisation but the discussions can aim for a general optimization with regard to that control. It remains (formally) open whether a participant is looking for or providing expertise – this positioning is left to the discourse itself. The aim is to awake the interest to exchange ideas with other users of the platform in order to learn from their experiences and to profit from the resulting social-technical-capital. Thus, with the help of the self-assessment module and the associated superordinate modules, a community building process is initiated that increases the activity of all interaction methods integrated on the platform.

5. Evaluating the Platform in a Focus Group

To evaluate the platform, we have conducted a workshop with ten experts from eight small or medium-sized energy providers. Due to the legal requirements, the majority of the organisations were certified against ISO/IEC 27001 so they successfully went through all the necessary processes. Therefore, most of the participants had good security know-how. One of them was a trainer for ISO/IEC 27001 security auditors.

We have presented the most relevant platform features in a live demo. The attendees could always interrupt the presentation and ask questions to make sure they understood everything. Afterwards, the experts were invited to discuss the platform in a moderated discussion. We asked them for general feedback and for suggestions for improvement based on their own experiences. We also stimulated discussions among the experts and moderated it in the way to work out the most relevant aspects.

The participants emphasised the simple structure and the user-friendly design of the platform. Their comments and the way they discussed the platform and its functions also clearly demonstrated they understood the purpose of the different functions and how to use them. Apart from those usability aspects, many of the comments were addressing the ISO/IEC 27001 certification. There was consensus among the experts that the platform was helpful for an internal pre-audit before the official ISO/IEC 27001 audit starts. They argued for instance that the organisations have to conduct a risk analysis prior to the official audit anyway, and such a self-assessment would be very helpful for SMEs who often struggle to identify and assess the risks they are exposed to. The experts also agreed that the approach to go through the ISO/IEC 27019 controls makes a lot of sense because this is what the auditor finally checks.

The users' positive evaluations on both the platform's usability and its general ideas have a positive effect on the users' activity and it strengthens the community building process which helps the entire community. To further improve the platform the experts suggested integrating a recommender feature that derives optimal security measures and recommends a list of actions to the security team. According to the benchmarking component, it would be useful to have a benchmarking with companies already certified against ISO/IEC 27001.

6. Conclusion and Future Work

Security self-assessment frameworks support security managers to assess their organisation's security level. Applying those frameworks can be a cumbersome task since many of them are based on long questionnaires. Apart from that, additional information and inter-organisational discussions, e.g. with regard to the selection of security measures, can often be helpful especially for SMEs who often do not have the capacities to run a full-fledged security department. In order to address these issues, a web-based collaboration platform for security management was developed, supporting energy providers. The security self-assessment component constitutes the central feature of the platform. It helps security managers to identify relevant attack scenarios and allows them to benchmark their security status with that of similar organisations. Complementarily, small modules were implemented that are spread across the platform. They allow the users to complete or update the data needed for the self-assessment along the way when interacting with other parts of the platform. By making use of motivational elements and showing questions one by one in other parts of the platform, we aim to ease the burden of security self-assessments (e.g. going through a long questionnaire).

Furthermore, we have implemented a prototype of the platform and have evaluated it in a focus group, concentrating on usability aspects but also on the conceptual ideas of the platform. The next steps are to address the experts' feedback and to work on a recommender function for security measures based on the results of the security risk analysis. Another open task is to analyse how to design the inter-organisational sharing of recommended measures in a privacy preserving way.

7. Acknowledgement

This research was supported by the German Federal Ministry of Education and Research (grant numbers: 16KIS0239K, 16KIS0240). We thank Leon Alexander Herrmann and David Bug for their contribution to the prototype implementation.

8. References

Ackermann, M. S., McDonald, D. W. (1996), „Answer Garden 2: Merging Organizational Memory with Collaborative Help", *CSCW'96*, ACM Press, pp97-105.

Castle, S. R. and McGuire, C. (2010), "An analysis of student self-assessment of online, blended, and face-to-face learning environments: Implications for sustainable education delivery", *International Education Studies*, Vol. 3, No. 3, p36.

Curley, M. G. (2004), Managing information technology for business value: practical strategies for IT and business managers (IT best practices series), Intel press.

Dax, J., Ivan, A., Ley, B., Pape, S., Pipek, V., Rannenberg, K., Schmitz, C. and Sekulla, A. (2017): "IT Security Status of German Energy Providers", Technical Report, Cornell University, arXiv.

Dax, J., Ley, B., Pape, S., Schmitz, C., Pipek, V. and Rannenberg, K. (2016): Elicitation of Requirements for an inter-organizational Platform to Support Security Management Decisions, *10th Int. Symposium on Human Aspects of Information Security & Assurance*, HAISA 2016, Frankfurt, Germany, Proceedings.

Girgensohn, A., Lee, A. (2002), "Making Web Sites Be Places for Social Interaction", *CSCW'02*, New Orleans, Louisiana, USA.

Kollock, P. (1996), "Design Principles for Online Communities", *Harvard Conference on the Internet and Society,* Cambridge, MA.

Lesser, E. L., Fontaine, M. A. and Slusher, J. A. (eds.) (2000), *Knowledge and Communities.* Butterworth-Heinemann, Oxford, UK.

Pipek, V. and Won, M. (2002), "Communication-oriented Computesr Support for Knowledge Management", *Informatik/Informatique - Magazine of the Swiss Informatics Societies,* Vol. 1, pp39–43.

Resnick, P. (2001), "Beyond Bowling Together: SocioTechnical Capital", *J.M. Carrol (ed.), Human-Computer Interaction in the New Millennium, Addison-Wesley,* pp647-672.

Saunders, M. and Mann, R. (2005), "Self-assessment in a multi-organisational network", *IJQRM*, Vol. 22, Issue 6, pp554-571.

Swanson, M. (2001), "Security Self-Assessment Guide for Information Technology Systems", *NIST Special Publication 800-26*.

Yang, H.-L. and Lai, C.-Y. (2010), "Motivations of Wikipedia content contributors", *Computers in Human Behavior*, Vol. 26, Issue 6, pp1377-1383.