Measurement and improvement of information security culture

Stig O. Johnsen[a], Christian Waale Hansen[b], Yngve Nordby[b] and Maria B. Dahl[a]
[a]SINTEF, Trondheim, Norway
[b]NTNU, Trondheim, Norway

Abstract: Remote IT based operations of offshore oil and gas installations are increasing in the North Sea. The motivation for remote operation is increased income, cost reductions and more efficient support.

The technology used to support operations is changing from proprietary closed systems to standardised IT systems built on PC's and MS Windows connected to both internal networks and the Internet. In addition the operations and management of the oil and gas fields are increasingly being performed by a network of firms that functions as a virtual organization. The network organizations and the increased vulnerabilities create the need for improved information security.

Our hypothesis is that an important contribution to improved information security (IS) is improved IS culture and improved communication during operations and incident handling. IS culture should be explicitly focused, and actions should be taken to improve IS culture from a purely rule based culture to an ideal learning culture.

We have suggested a method called CheckIT consisting of a questionnaire and a process to improve IS culture based on group discussions. The questionnaire consists of questions and suggested answers based on denial based culture, rule based culture and the ideal learning culture, to enable the participants to explore their culture and identify areas to be improved.

Keywords: Information Security, Safety, Organisational Culture, Action research

1. INTRODUCTION

The amount of e-Operations, i.e. remote operations and remote control of offshore oil and gas installations, is increasing in the North Sea. The main motivations for remote operations are the potential for operational cost reduction and increased income or yield from the fields. However, initial projects that envisioned quick implementations of remote operations and remote support, have not been carried through as easily as expected. Many of the projects have been changed, stopped or delayed substantially.

Questions related to the security and safety of e-Operations has been raised. The technology used in operations is changing from proprietary closed systems to standardized IT systems based on MS Windows, integrated in networks that may be connected to the Internet. The reliance on MS Windows, networking and the Internet increases the vulnerability of the oil and gas operations. If vulnerability is exploited, the result could be a loss up to 3 Mill USD, based on production loss. Since the operations are performed in an environment with increased knowledge regarding vulnerabilities and exploits this could lead to an increased degree of hacker attacks. The increased use of suppliers and increased connectivity leads to a network of actors, which by accident, negligence or purpose can inflict large economic loss on an operator.

The personnel involved in e-Operations projects have a tendency to focus too much on technology, often at the expense of organizational and cultural issues.

Management and operation of the oil and gas fields are increasingly being done by a network of firms, often referred to as virtual organizations. Relocation of operations and the increased use of

subcontractors and outsourcing imply the need for more safe and secure communication and cooperation between different organizations. The virtual organizations and the increased vulnerabilities create the need for common risk perceptions and a common IS culture to reduce the risk associated with remote operations.

Based on studies and interviews conducted with major operators within the oil and gas industry on the Norwegian Continental Shelf, this paper identifies major challenges and proposes solutions related to improvement of IS culture.

1.1 KEY DEFINITIONS

Risk communication

An intentional transfer of information designed to inform individuals about the existence, nature, form, severity or acceptability of risks. In this context we want to target individual groups in order to raise the awareness of risks related to remote operations.

Remote control

Part of the operation is managed and operated from other places. This can cover a wide spectrum of possibilities, from control of parts of the process in a normal situation to total control of the installation in an emergency situation. Central control room operators are present at the installation.

Remote operations

The process is managed and operated from other places. This is the situation for the unmanned installations and is the most radical solution for installations, where all the control room functions and other operation functions are executed from a remote location. Today, this is the case for sub-sea installations.

Safety culture

The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine commitment to, and the style and proficiency of, an organisation's health and safety management. ACSN (1993).

Virtual organisation

A virtual organisation is a group of people from different organisations located at different geographical locations working together in shared interdependent processes to achieve shared objectives within a defined timeframe. The authority and roles/responsibility of the participants are clearly defined. The collaboration is supported by technology that gives the participants common understanding and enables good co-operation among the participants. Johnsen (2005).

1.1 Key challenges

The studies have identified several key challenges related to e-Operations in the oil and gas industry.

One challenge is that proprietary and closed control systems are replaced by standardised ICT systems based on PC's and MS Windows connected to networks and Internet. The vulnerabilities of the control systems have thus increased.

The awareness has not equally increased among the different professionals. There is a gap in experience and knowledge between the old automation profession and the ICT profession related to the new ICT vulnerabilities.

Outsourcing and the use of several suppliers has increased. The levels of communication and problem solving between different groups in different organizations are increasing. An improvement of IS culture can ensure that different professions and organizations share a common understanding of the new risks and can cooperate to improve communication, risk mitigation and resolve incidents

Based on the preceding discussion, we suggest that improvement of IS culture could be an important step to reduce the risk of e-Operations. Thus, developing a tool for the improvement of IS culture should be explored further. CheckIT is a result of this work.

2. ORGANIZATIONAL CULTURE

The notion 'Culture' in an organizational context was primarily used by American pragmatists and consultants in the early 1980s. The cultural metaphor was borrowed from anthropology, as it became obvious that organizations, just as nations and tribes, develop unique language, behaviour, rituals and perceptions of the world.

Two main approaches to organizational culture are evident in the literature and among practitioners; the functionalist approach and the symbolic/interpretive approach. Within the functionalist approach, there is a focus on improvement and the links between financial performance and culture. Within the symbolic approach, the focus is on description, and the notion of culture is used to describe and understand organizational life.

The questions of whether culture can be measured, managed and manipulated are fundamental within the functionalist approach to organizational culture. Our assumption in this paper is that culture indeed can be measured, managed and manipulated. But at the same time we have been influenced by the symbolic tradition, in that culture is difficult to change and that actors within the culture must participate in the change process, thus, triangulation has been our approach in that we have combined the best from the functionalistic tradition with the best from the symbolic tradition.

Safety and security culture is a hot topic in safety work, but also one which creates confusion Hale (2000). There is a lack of agreement, both between theoreticians and practitioners within the field, on how to define, measure and approach the concept. We view culture as a property of collectives – e.g. groups, organizations or communities. Moreover, we emphasize action and interaction, rather than theoretical constructs such as attitudes and values. This focus approaches Argyris and Schön's notion of *theories-in-use* – i.e. the values and principles that are reflected in actual actions, as opposed to the values and principles which are claimed (*espoused theory*), see Agyris and Schøn (1996).

In 1986 Shell International Exploration and Production started sponsoring a research program to better understand why accidents occur and what can be done to avoid them. This resulted in Hearts and Minds, a tool for analyzing and improving safety culture. Hearts and Minds enables organizations to understand their safety culture as a whole, but also provide a tool for individuals to understand their personal behaviour in the context of the culture, ref Hudson (2002). The philosophy of the Hearts and Minds, is that development is characterized by gradual development and this requires practice and discussions in a group setting. This also implies a continuous focus on safety; it is not enough to succeed only once. Hearts and Minds is based on previous work by Westrum (1993), who has defined an evolutionary model comprising different levels of safety cultures. We have reduced the levels of safety and security culture in order to improve understanding and communication.

The levels of safety culture we have chosen to exploit fro m Westrum are:

- **The pathological/denial culture** – organizations who fit this characteristic are self organized on a basic level and strive to maintain status quo. They will deny warning signals, punish those who bring them up and try to keep reporting at a minimum. Their focus is doing business, and on maintaining the impression of everything being as normal.
- **The calculative/rule based culture** – These organizations are strongly rule oriented, and driven by management systems. They put great effort into forming and imposing rules, which are intended to cover both unwanted situations and external requirements. They have a limited repertoire of measures when an event occur, and mainly focus on simple deviation handling.
- **The generative culture** – organizations that are generative put great effort into active participation on all levels, and aligning organizational goals with safety oriented goals. They perceive safety and security as an opportunity and an inherent part of the business, rather than an imposition of costs. The company's own and other companies' experiences are actively used to continuously improve the safety performance.

3. CHECKIT

The aim of CheckIT is to assist the various oil and gas companies and other actors in identifying and solving security and safety problems that arise in a network of cooperating firms performing e-Operations. Our experience suggests that the method also can help actors to exploit the opportunity to share best practices and thus improve operational IS.

3.1. The development of CheckIT

Our approach in the development of CheckIT has been iterative, and feedback from participating organizations and potential end users has been stressed. The development has been structured as follows:

- Initially, a "state of the art" literature review of safety culture, high reliability organizations, organizational learning and other relevant topics was performed. The aim was to identify important safety culture areas, relevant questions and processes to assess and improve safety and security culture. Important aspects from Hale (2000), Reason (1997), LaPorte (1991) and Hudson (2002) have served as a foundation for the succeeding work.
- Additionally, indicators that characterize IT safety and security was identified, and correlations between good culture, as identified by the questions, and performance was checked. The latter may be related to Itoh, Andersen, Seki (2004), where night train operators' attitudes toward management, operating procedures and other organizational issues that impact on safety are investigated.
- Based on the theoretical foundation, a tentative version was developed and distributed to participating organizations for review and comments.
- The methodology was subsequently discussed and adjusted with relevant industry experts in a two day workshop in Trondheim in February 2005. The industry experts involved, were from the oil and gas industry, the telecom industry, the research/consultancy fields and authorities (National Safety and Security authorities).
- The proposed adjustments from the workshop were implemented in the tool, and a first version of CheckIT was developed and approved by all the participating parties during the spring of 2005.
- The first version of CheckIT has been used in the Oils and Gas industry. We have planned to improve the tool based on our experience in 2005 and 2006.

Thus, the final phase in the development of the tool is the utilization and improvement of CheckIT in the industry. This phase is now during implementation.

A key issue is to ensure that improvement in IS culture has improved IT safety and security as documented by the indicators. Adjusting CheckIT based on the experiences of the users is also an integral part of this phase. Thus, we have not yet been able to document the effect of CheckIT on IS culture or performance. This, however, has been planned to be started in 2005 together with operating companies within the oil and gas industry. We have planned to explore the effect of CheckIT periodically over a period of 2-3 years.

Shell experienced significant improvements in the years since the research started in 1986, Hudson (2002), and the goal with CheckIT is to achieve effects corresponding to the results of the Hearts and Minds program. To document the effect of CheckIT on safety and security we have to identify performance indicators, such as the amount of unwanted incidents, and follow the development of the indicator based on our work improving IS culture.

3.2. CheckIT's theoretical foundation

CheckIt has been based on the foundation of organisational culture, as described by Schein (1992), and the combination of functionalistic and symbolic tradition.

The framework for cultural assessment draws on Westrum's typology of organizational cultures Westrum (1993). A possible development of safety culture from "bad" to "good" (ie from the pathological/denial culture to the generative culture) is described.. Three alternative levels,

corresponding to the levels in Westrum, are described for each question in the tool. The CheckIT methodology is however developed specifically to e-Operations in the oil and gas industry through co-operation with several oil and gas companies.

A key foundation of CheckIT is the ability to exploit and change fundamental values or root causes by establishing meeting arenas where double loop learning and organisational development can be performed as described by Agyris and Schøn (1996). Trough group discussions, root causes should be identified, and the participants should be able to suggest changes throughout the organisation.

With respect to the basic assumptions in an organization, we assume that the behavioural foundation also is influenced by attitudes and values outside the organization, from the society as a whole. I.e. a worker will generally have certain values and attitudes simply as a result of being a part of the society.

CheckIT focuses on the values and routines on the organizational level. In this context, we apply Schein's three-level model to describe the different levels within the organization. CheckIT has a focus on the top two levels of this model, but the group process is important in that it can influence the basic assumptions of the organization, if double-loop learning is achieved.

However, we assume that the basic assumptions, and the culture as a whole, may be influenced by altering routines and behaviour sustained over a long period of time. This corresponds to Rosness'(2001), views on cultural change, where cultural change is an effect of altered patterns of interaction and behaviour.

3.3. Overview of CheckIT

The basic package of CheckIT comprises 31 questions, which can be used to measure, monitor and improve IS culture. These questions are recommended, and constitute a minimum in a cultural survey or an improvement program. Additionally, 34 questions are provided in a supplementary package, which allows the user to configure the survey and/or improvement program according to the specific needs of the organization.

Each question is presented in a short and precise manner, and three alternative answers are presented in a table next to the question. The aim is to develop a rating of the organization on a five-point scale, where alternatives one, three and five are textually presented. This corresponds to Westrums levels, and has previously been implemented in a tool for UIC, the international railway industry - see S.O. Johnsen (2004). The utilization of a five-point scale provides a basis for a normalized score throughout the organization, and makes it possible to compare results and also benchmark against other organizations.

The first part of the presented survey is what is considered to cover the minimal aspects of Information Security culture, and as such what small organizations could use without further configuration. Larger corporations may define topics of special interest, and thus choose to include questions further exploring these fields of interest.

Based on requests by the organizations that were involved in developing CheckIT, a package of 34 supplementary questions that explores specific topics of interest is also included. These were not considered to be of enough importance to be included in the basic package, but may be included or exchanged for other questions if the survey is to cover certain topics in further depth.

3.4. The specific questions

Generally, the topics covered by CheckIT have been based on two sources:

- Topics uncovered during the literature review
- Specific requests from cooperating organizations

The experts from the workshop have also participated in an iterative development of the tool, with revisions and comment both prior to, during and after the workshop. To improve understanding and

identify possible improvements of IS culture, we have exemplified *denial based* culture, *rule based* culture and *best practice* for each question.

Many of the questions are based on work within the field of safety culture and HRO; Hudson (2002), Reason (1997) and LaPorte (1991) have all had influence. Central topics include management involvement, commitment and communication. This comprises leading by example, identifying all involved parties, establishing clear responsibilities, and establishing a common risk perception, common manners of communication, and ultimately building a common understanding. A focus on error free communication may have a positive influence on these aspects, ref LaPorte (1991).
The reporting of incidents and learning from these are also integral parts in building a good IS culture. This implies that an open discussion exists between the staff and management; if this is not the case, incidents will never be reported and used for learning. The learning aspect also comprises general training and system insight in addition to be able to perform double-loop learning.

The examples in each question have been developed, tested and verified trough interviews and workshops. The work has so far verified the relevance of the questions, and also identified what has been considered best practice in the alternatives.

3.5. Using CheckIT

We propose two main strategies for the use of CheckIT; both related to improvement of the IS culture. The first strategy aims at directly improving the culture of the organization by using the tool. The second strategy aims at diagnosing the culture of the organization.

Each approach has different pros and cons, and may provide more or fewer answers depending on the type of organization examined, the nationality of the subjects and other aspects affecting the willingness and openness toward such surveys. Further guidance of what strategy to choose, and how to prepare, may be given once the results from different approaches and on participants from different cultures have been studied, and conclusive recommendations can be provided.

3.5.1. Recommended use of CheckIT

The suggested approach includes the following steps, which are also described in figure 1:

1. *Identify key indicators.* Identify key indicators and common goals to be explored together with management, get management commitment to accept the necessary analyses and possible changes, establish, and establish learning arena.
2. Assessment of safety and security culture via a questionnaire to identify challenges
3. Discuss and reflect on questionnaire in group setting, to identify areas to be improved
4. *Identify actions* and adjust based on good co-opting processes. (a co-opting process is used to describe a decision process involving both management and work-force where the issues are discussed freely prior to a decision.)

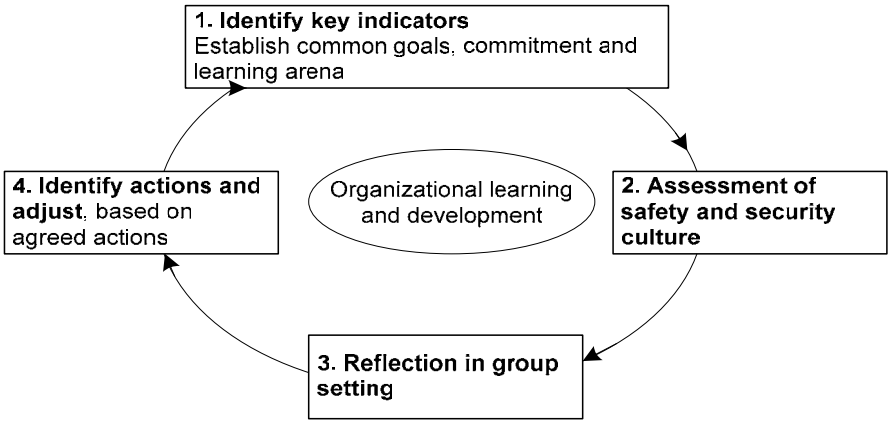


Figure 1: Suggested approach to foster organizational learning

The assessment of IS culture should be carried out by using the questionnaire. For each question there are three described alternatives to be used representing differences in culture. The three described cultural levels are:

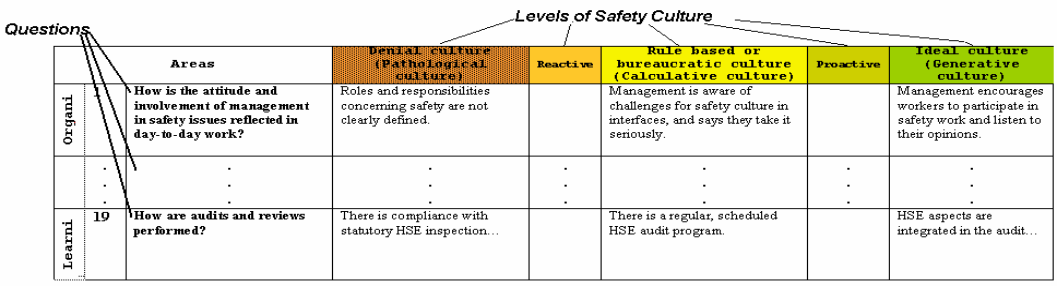
- Denial culture (Level 1)
- Rule based culture (Level 3)
- Proactive /Generative culture (Seen as "Best practice" – Level 5)

This assessment should be done in two steps. First the individual participants will complete the questionnaire on their own, and then subsequently in the work-group. The idea is to evaluate the organization at each question, and then place it within one of the IS culture levels in the range from 1 to 5.

The participants should identify areas where the IS culture could be improved. Reasons to improve the culture are a cultural level too far from "best practice" or because the differences in "cultural levels" between the actors in the network are significant and could lead to misunderstanding or even an incident/accident.

The aim of the questionnaire is to help the organisations to identify and improve safety culture.

The structure and layout of the questionnaire is illustrated in Figure: 2.



		Areas	Denial culture (Pathological culture)	Reactive	Rule based or bureaucratic culture (Calculative culture)	Proactive	Ideal culture (Generative culture)
Organi	1	**How is the attitude and involvement of management in safety issues reflected in day-to-day work?**	Roles and responsibilities concerning safety are not clearly defined.		Management is aware of challenges for safety culture in interfaces, and says they take it seriously.		Management encourages workers to participate in safety work and listen to their opinions.
	. . .	. . .	. . .	. . .	. . .	. . .	. . .
Learni	19	**How are audits and reviews performed?**	There is compliance with statutory HSE inspection…		There is a regular, scheduled HSE audit program.		HSE aspects are integrated in the audit…

Figure 2 Layout of the CheckIT Questionnaire

The questions to be elaborated are documented in the appendix. Examples of one question, and the related descriptions of the three major "cultural levels" are as follows:
Question: How is experience feedback used in the organisation?
The suggested descriptions and examples of the major "cultural levels" are:

- **Denial culture (Level 1):** Many incidents are not reported. A database of serious incidents reports exists but it is incomplete and not considered being useful. The system does not have open access. Management is not informed about serious incidents.
- **Rule based culture (Level 3):** There is a database with detailed descriptions of near incidents and incidents, which is used internally. Efforts are made to use it actively, but it is not yet fully established as a useful tool.
- **Proactive /Generative culture (Seen as "Best practice" – Level 5):** The company's own and other companies' experiences are actively used to continuously improve our own safety performance as well as the industry as a whole. Interfaces are seen as an important learning arena. Simulators are used as a training tool to gain experiences cross interfaces and create understanding.

The use of the method has proven not too resource demanding. The effort needed in an analysis is around 2 to 3 day's effort from the involved organization. The main activities are listed in Table 1:

Effort	Activities
½-1 Day	Preparation and organization – identify relevant key indicators and identify people to attend the workshop, fill out questionnaire in advance.
1 Day Workshop	Assessment and reflection of IS culture, performed by an experienced team. Actions – as agreed in team-work.
½-1 Day	Follow up of agreed actions, to insure that action is taking place by the proper responsible person. Document improvements in IS culture and IS in general. Show the development of key indicators.

Table1: Activities and effort in CheckIT analysis.

Improvement of IT security and safety is not an activity that can be done only once, it is a continuous process. We propose that a CheckIT survey should be performed each year. The development of key indicators should be assessed each period, and the effect of CheckIT should be assessed.

3.5.2. Alternative use of CheckIT – to identify only present status

CheckIT can be used to identify only present status. This could be done by two different approaches. Both have been suggested and tried out by participating organizations during development of the method. The alternative approaches are:

1. Performing a purely quantitative survey, without trying to improve the IS culture. This opens for statistical exploitation of the given data and cross examining against demographics within the organization. It is important to keep in mind that each question was developed to uncover certain relevant aspects of information security, and one should be careful not to group questions not connected, as the average score may cancel out findings otherwise of interest.

2. The questions may be used as cues for an interview guide. By choosing a battery of questions and elaborating these with different participants from within the organization, one may be able to uncover opinions, views and even solutions that otherwise would never have been expressed. This requires thorough preparation by the team conducting the interviews, but may also yield the best results as employees who usually not willingly give their opinions may be more engaged and take more of an interest in the problems addressed.

4. CONCLUSION

The increased amount of e-Operations has caused increased vulnerabilities within the oil and gas industry. The new technology introduced, and hereby new work processes create the need of building and continuously improving a culture for security and safety.

Our studies have shown that a focus on improving the IS culture may have a positive effect on safety and security performances. We have proposed a tool, CheckIT, which may be used for the assessment and improvement of IS culture.

Further work includes applying CheckIT to companies in the oil and gas industry, to identify areas for improvement and over a period of 2 to 3 years to identify if the IS culture has been improved and if the actual safety and security has been improved.

REFERENCES

ACSN (1993) Third report of the Advisory Committee on the Safety of Nuclear Installations - Organising for Safety - Health and Safety Commission, 1993 - ISBN 0-11-882104-0.

Agyris and Schøn (1996) C .Argyris & D. Schon, *Organizational learning II: Theory, method and practice*. Addison-Wesley, 1996, Reading, Mass.

Hale (2000) . A. Hale, A., *Editorial – Culture's confusion*, Safety Science, Vol. 34, pp. 1-14, 2000.

Hofstede(1991) G. Hofstede, *Cultures and Organisations: Software of the Mind*, McGraw-Hill, 1991.

Hudson (2002). P. Hudson.& G.C. van der Graaf, *Hearts and Minds: The status after 15 years Research*, Society of Petroleum Engineers (SPE 73941) International conference on HSE in Oil and Gas Exploration and production, Kuala Lumpur 20.-22. march 2002.

Itoh, Andersen, Seki (2004), *Track maintenance train operators' attitudes to job, organisation and management and their correlation with accident/incident rate*, Cognition, Technology and Work, Vol. 6(2), pp. 63-78

Johnsen (2004). S.O. Johnsen, I.A. Herrera, E. Jersin, R. Rosness, J. Vatn, M. Veiseth, M. Tungland, C.E.B. Bergersen, *The Track to Safety Culture (SafeTrack), a toolkit for operability analysis of cross border rail traffic, focusing on safety culture*, Sintef report STF38 A04414, ISBN 82-14-02731-4

Johnsen (2005) - Johnsen S., Askildsen A., Hunnes K. "Challenges in remote control and co-operation of offshore oil and gas installations in the North Sea" Esrel 2005.

Reason (1997). J. Reason, *Managing the Risk of Organizational Accidents*, Ashgate, 1997, Aldershot.

LaPorte (1991). T. R. LaPorte and P.M. Consolini, *Working in practice but not in theory: theoretical challenges of "high reliability" organisations*, Journal of Public Administration Research and Theory, 1991.
R.Rosness (2001). R. Rosness, *Safety Culture: Yet another buzzword to hide our confusion?*. Internal SINTEF-paper (2001), available at: www.risikoforsk.no

Schein (1992). E.H. Schein, *Organizational Culture and Leadership*, Jossey-Bass, 1992, San Francisco.

Westrum (1993). R.J. Westrum, Cultures with Requisite Imagination, in: Wise, Stager and Hopkin (Eds.) *Verification and Validation of Complex Systems: Human Factors Issues*, Springer, Heidelberg (1993).

Y. Nordby, C.W. Hansen (in norwegian), *"Informasjonssikkerhet, atferd, holdninger og kultur"*, Tapir, Trondheim, 2005, ISBN 82-7706-222-2

Appendix A: Questionnaire – some of the questions having been developed

Questions	Employees/ Managers	Question:	**Denial culture (Level 1)**		**Rule based culture (Level 3)**		**Proactive /Generative culture (Seen as "Best practice" – Level 5)**
1	E/M	*To what extent is senior management involved and committed to information security?*	The management does not focus on information security and employees are given little information regarding this.		The management focus on information security, when there is an occurrence of an incident. They inform the employees, but there is one-way communication.		The management continuously focus on information security. There is a two-way communication with employees and partners regarding information security.
2	E/M	*To what extent are employees and suppliers involved in developing information security?*	The management and those responsible for the information security develop and decide the requirements and routines for information security without involving the employees or suppliers.		The management when developing the routines for information security uses report and suggestions from the employees and suppliers.		Employees and suppliers are directly involved in the process of developing procedures for information security and they are considered an important resource in this work. Some employees have been given responsibility regarding information security.
3	E/M	*To what extent are rules and procedures continuously adjusted to reduce the risks related to information technology?*	The companies make safety procedures when required by authorities. Rules are used by management to keep a retreat open, and in that way disclaim responsibility when accidents occur. Rules are not always used to increase safety, but also used politically.		There are many procedures, serving as 'barriers' to prevent incidents. The stringency of the rules is at the minimum required by authorities. Procedures are adjusted or "bent" to enable quick fixes or do the job faster.		Procedures are seen as an opportunity to improve the safety and security, and they are continuously refined in order to make them more practical. Common procedures are used cross interfaces, and are developed in cooperation with other organisations.

4	M	*To what extent are unwanted incidents analysed and used as a learning experience?*	Unwanted incidents are rarely investigated. Only serious incidents with large potential loss are investigated.		The incident is analysed to establish new routines in order to avoid such incidents in the future. Little are being done to investigate the root cause of the incident.		The incident is used as a learning opportunity. The organisation as a whole is trying to learn from the incident. Management and employees are discussing the incident in a meeting arena where ideas and experience can be exchanged.
5	E/M	*To what extent are reporting of unwanted incidents appreciated?*	There is no feedback, and I don't know if anything has been done to improve what I reported. I usually prefer to solve the problem by myself. I never get feedback if I report an unwanted incident.		I only report incidents if they are serious and may have direct consequences for my work. I report to my superior and he/she report back to me that my report has been received and that someone will take care of the problem.		I know to whom I shall report and that all reports of unwanted incidents are taken seriously. I will be informed if action is taken to solve what I reported. I always report unwanted incidents regarding information security.
6	E/M	*To what extent are individuals blamed if an accident or unwanted incidents occurs?*	Individuals or partners ar blamed in the case of unwanted incidents regarding information security.		A combination of technical and personal factors is seen as the reason for the occurrence of unwanted incidents. The system as a whole is often blamed.		Who to blame is rarely an issue in such incidents. Individuals or partners are therefore rarely blamed.
7	M	*To what extent are experience transferred between your company and other companies?*	Few experiences are shared with other companies. Information security is regarded as an internal affair in the company.		There is little focus on measuring information security for comparison with other companies.		The company a part of a network for information security in order to learn from other companies' practice regarding information security.
8	M	*How is experience feedback used in the organisation?*	Many incidents are not reported. A database of serious incidents reports exists but it is incomplete and not considered being useful. The system does not have open access. Management is not informed about serious incidents.		There is a database with detailed descriptions of near incidents and incidents, which is used internally. Efforts are made to use it actively, but it is not yet fully established as a useful tool.		The company's own and other companies' experiences are actively used to continuously improve our own safety performance as well as the industry as a whole. Interfaces are seen as an important learning arena. Simulators are used as a training tool to gain experiences cross interfaces and create understanding.
Last	E/M	What is your opinion of this questionnaire?	Time consuming, unnecessary and not relevant.		OK. Not very interesting, but I did learn something from it.		Interesting. It made me see a new perspective and I gained knowledge.