Workshop-based Security Safeguard Selection with AURUM

Thomas Neubauer
Vienna University of Technology
Vienna, Austria
thomas.neubauer@tuwien.ac.at

Markus Pehn
SBA Research
Vienna, Austria
pehn@sba-research.org

Abstract - **Organizations are increasingly exposed to manifold threats concerning the security of their valuable business processes. Due to the increasing damage potential, decision makers are permanently forced to pay attention to security issues and are raising their security investments, but often (i) without considering the efficiency of the investments made, (ii) neglecting to involve people in order to raise security awareness and (iii) without full awareness of the importance of the decision at hand. This paper provides a crucial extension to the established risk management solution AURUM and extends its functionality by introducing the AURUM Workshop, which allows the selection of efficient safeguards based on corporate business processes. It highlights typical problems of (group) decision making and provides a solution to eliminate those shortcomings. Thereby, it supports decision makers in (i) refining the basic infrastructure elements to the specific requirements of the corporation, (ii) focusing on the most relevant risks and (iii) improving their awareness for the problem at hand.**

Keywords-Risk Management, AURUM, Decision Support

I. INTRODUCTION

Security hazards, such as viruses, hacker attacks or data theft, pose major threats to corporate assets and affect profit, shareholder value and a company's reputation. The increasing usage of the Internet leads to a rise in the frequency of security breaches related to information technology. Garg, Curtis and Halper [2] estimated security investments within US companies to reach about $30 billion by 2005. CERT estimated that about 90% of big and medium-sized companies were affected by security incidents in 2006. In May 2009, the New York Times reported on a billion dollar contract the US Government signed with security companies and universities with the aim of being equipped for so-called cyber warfare. Due to the continuous increase of information technology use and its monetary importance, the main questions posed by companies' managers are how to determine the optimum level of security investments and which measures are necessary and efficient.

This work provides an extension to the established risk management solution AURUM (AUtomated Risk and Utility Management; cf. [3], [4], [5], [6], [7], [8], [9]). AURUM provides a risk management solution that allows decision makers to evaluate security investments based on corporate business processes and infrastructure defined in a security ontology. A Bayesian network supports the risk definition, whereas an interactive multiobjective decision support approach is used for selecting safeguards. This paper extends the functionality of AURUM by introducing the AURUM Workshop. The AURUM Workshop provides the missing link between the ontology comprising corporate business processes and infrastructure, the Bayesian network, and the decision support module that allows the interactive selection of efficient safeguards. It takes typical psychological and social influence factors from literature into consideration. Thereby, it supports decision makers in (i) refining the basic infrastructure elements to the specific requirements of the corporation, (ii) focusing on the most important risks (risks with a high frequency, a high impact, or both) and (iii) improving their awareness for the problem (risks) at hand. The remainder of the paper is organized as follows. Section 2 introduces the state-of-the-art related to group decision making, whereas Section 3 gives a deeper insight into the psychological and sociological factors of group decision making. Section 4 introduces the AURUM Workshop. Sections 5 and 6 focus on describing the roles and the methods needed in the Workshop process. Finally, the Workshop process is described in detail in Section 7.

II. GROUP DECISION MAKING

Groups of persons are commonly employed in a various ways: to counterbalance individual subjectivity of goal and preference systems, assist creativity, compensate for complexity, and to increase members' identification with a decision (cf. [10], [11]). According to Frech [11], groups are similar to teams and characterized by "face to face contact of more than two persons over a longer time period oriented toward a goal identical to all members".

He argues that within a group, certain phenomena can be observed:

- A sense of togetherness also referred to as cohesion.
- The emerging of certain rules and restrictions in formal and informal interaction.

Staehle [12] uses these psychological facts to explain the difference between groups and teams. He defines a team as a focus-oriented work group with a stronger cohesion (team spirit) and stronger internal psychological relations. The role structure is more oriented to a team leader vs. member situation and the time span of working as a group is normally shorter. The designation of a team as "work group" leads to a point where teams are working toward a common goal, and individual preferences have to be shelved. This common goal leads to a higher level of cohesion in combination with high conflict potential. Groups bound by instructions,

characterized through the goal of achieving a common purpose, will be discussed below. Autonomic groups are not part of these considerations (cf. [13] for a definition and further discussion of autonomic groups).

A. Structure of Group Decisions

A group decision is the result of a group decision process (GDP). Laux [14] describes this process as two stages: the information process and the choice process (cf. [10], [13]). Paschka [15] divides the information stage into:

- Problem definition: Measure methods to elicit goal values. The problem definition can be predetermined by the management. A common approach is a comparison of actual and targeted business results that ends in a clear formulation of the problem's context.
- Detailed specification of the goal system: This means mainly the annulment of goal conflicts, approaches and intervention techniques in order to refine preference orders. A diversification of goal conflicts can be found in [16].

Paschka's choice stage consists of the following steps (cf. [14]):

- Determination of alternatives for action: These are multiple different methods, mostly selected via voting or exclusion approaches (or both), which also include decision finding based on these techniques (cf. [17]).
- Realization: Methods and techniques, for example project management to execute the decision.
- Control: Methods and techniques to compare the received results.

Once the information has been gathered, a discussion about possible alternatives and their results has to be carried out, usually leading to a voting process and a decision. This phase may possibly be influenced by members who try to further their individual preferences (cf. [14]). A participant of a group decision process is described through a set of variables (cf. [15]):

- Individual goal function and preference order: Depending on job position, knowledge, and interest in topic.
- Probability judgment: Depending on an individual's processing of given indicators, knowledge of the topic, and experience in similar situations.
- Information amount: Inside the group, external information will be presented through indicator values, but there is still the possibility that the amount of information certain group members have differs because of differences at the information processing level (prognostic function, cf. [14]) and external experience/knowledge (information structure) that is not available to the whole group (for example: secret strategic preferences of the management).

Based on these individual attributes it is obvious that, especially at the beginning of the information phase, each group member has different preferences and accordingly, a different preference order.

B. Application of the Group Decision Making Process to IS Safeguard Evaluation

Table I shows the application of the above described GDMP, according to Paschka and Laux, to information security by mapping the actions to the process.

TABLE I. APPLICATION OF IS SAFEGUARD EVALUATION TO THE GDMP

Phase of GDMP	Security Safeguard Evaluation Action(s)
Problem definition	Definition of cost and resource categories; Definition of tactical goals according to security policies.
Detailed specification of the goal system	Specification of strategic and tactical goals: analysis of the goal system and preference order (importance valuation of the goals) referring to the definition s made in the problem definition phase; Definition of assets, vulnerabilities, threats leading to risks.
Determination of alternatives	Definition of proper safeguards following the specified risks over a valuation scheme.
Realization	Implementation through physical, technical and administrative controls.
Control	IS control mechanism such as internal or external audits.

C. Structural Characteristics of Groups

Adler [18] describes cultural perspectives and background via a classification scheme:

- Homogeneous team/group: All members have the same cultural background
- Token team/group: All members expect one have the same cultural background
- Bicultural team/group: Two cultures that are represented by at least two members each
- Multicultural team/group: Three or more persons with different cultural backgrounds

Martirossian [19] describes homogeneous groups as more efficient for executing well-defined tasks, whereas more heterogeneous ones tend to find a greater number of feasible results. According to Adler [18], the monitoring effort increases with the degree of cultural difference. The problem solving approach as well as the communication mode can show large differences, which can be an opportunity but can also create risks in terms of misunderstandings and a lack of respect for personal attributes and behavior. The moderator can pick out the best of the available behaviors without harming group members, which can increase efficiency (cf. [18]).

Martirossian [19] argues that the *group size* is an important criterion. While big groups require a high degree of communication to include all members at a certain level, small groups are easier to handle in terms of communication, but bear risks like a lack of information or ideas. The workshop solution provided in this work tends to

involve a variety of different members, which requires good preparation and an experienced coordinator open to different problem solving structures.

Group leadership [19], which can be "people-oriented" and/or "goal-oriented", is an important criterion in a group. People-oriented leaders focus more on satisfying the group, while goal-oriented leaders place more emphasis on production and results. Both factors are important, as a balanced solution is recommended to hold a good Information Security Workshop. In a workshop situation, where the aim is to achieve optimal solutions, it is of utmost importance to structure the group with a view to the points described above. A certain degree of heterogeneity in team members' job positions (security experts as well as employees from outside the security field) and possibly their cultural background has to be handled with respect to balanced process leadership, which should be both goal and people-oriented to a certain degree.

III. PSYCHOLOGICAL AND SOCIOLOGICAL INFLUENCE FACTORS

Decision makers, no matter whether they act on their own or as part of a group, are usually confronted with a variety of psychological and social issues that have a major influence on their decisions (cf. e.g., [20]).

A. Basic Phenomena

1) *Confirmation trap*: Humans aspire towards consistency, which induces them to insist on the correctness of their actions and to ignore, eliminate or distort contrary information. Insist on belief effect: Works similarly to the confirmation trap mentioned above. Humans try to maintain their view of the world by ignoring, eliminating or distorting contrary information. Availability heuristic: Humans are able to remember some things better than others (cf. [21]). Possible reasons are emotional involvement, time, and spatial and sensory proximity [22], leading to an incorrect interpretation of these events by exaggerating their frequency, importance, etc. Anchoring and adjustment: The anchor is a basis for classifying new information based on a person's experience (cf. [23]). A lack of information often leads to the use of an arbitrary anchor, which causes a misclassification in relation to the anchor. Hindsight bias: After an event, people frequently believe that they predicted it correctly. There are a few theories concerning the origins of this mechanism:
   - Relations were built after the event that do not or did not exist in reality.
   - The theory of distorted answers (cf. [24]), which was formulated as a result of questioning eyewitnesses, shows that when people are confronted with irritant information, the capacity for remembering the facts decreases.
   - The third theory is based on the abovementioned anchor heuristic, where the event is positioned too close to the anchor.
2) *Distortion by reasons of process variation*: People are generally inconsistent in their behavior. Lichtenstein and Slovic [23] as well as Tversky and Kahneman [25] have shown that this relation is not universally valid, and that logical procedure orientation and inductive behavior are only partially predetermined. Question structure: The formulation of the question is of vital importance to the processing and argumentation process inside respondents' minds.
3) *Prospect theory*: The frame in which a situation is embedded in terms of winning or losing dictates the expectations of the situation. If a loss is expected, a small benefit will be seen as a gain, whereas if a high benefit is expected, a small benefit will be handled as a loss (cf. [20]).
4) *Presentation of information*: Subjects are able to remember and categorize well presented information much better than badly presented information (cf. [20]).

B. Basic Phenomena in the Context of Group Decisions

The difficulty in mapping the basic phenomena to the group level is related to the nescience of specific group characteristics. In a group typically more resources, such as knowledge, power and financial capital are available.

- Availability heuristic at group level: Auer-Rizzi [20] takes it for granted that discussion of a prior case used as a prototypical example can affect the considerations in a positive or negative way.
- Anchoring at group level: Anchoring remains individual at group level; no group anchor is constructed, but rather individual anchors.
- Prospect theory at group level: Participants who see a situation as a gain are willing to take higher risks than others [25].
- Hindsight bias at group level: According to Stahlberg [26] there are no differences compared to the individual level if anchoring was used to provide the base of hindsight bias.

C. Influence of Majorities on Minorities and Vice Versa

The theory of social comparison (cf. [27]) postulates the human need to reassess own opinions. This mindset leads to behavioral uncertainty and the need for orientation towards reference points represented through

- a majority and the opinion it holds, or
- a strong individual opinion maker who persuades other participants of his view and, thereby, founds a majority.

According to Festinger [27] influencing majorities are one of the main reasons for distortion inside groups. An important factor within this theory is the divergence between physical and social reality. Physical reality is defined through the verifiability of facts, allowing everyone to check for themselves: e.g., financial data, statistics, etc. Social reality describes the common point of view

represented by a group or a strong majority. Asch [28] shows that in situations of divergence between social and physical reality, a tendency toward social reality is noticeable.

In contrast, Moscovici and Faucheux [29] showed that minorities can also influence the majority, if the minority argues with strong self-confidence and forcefulness. This refers explicitly to the behavior and not to fuzzy skill definitions (cf. [30]). In this case the majority tends to reflect on its point of view and often changes its opinion. Typical examples of this are influences on organizational hierarchies from outside the group structure. This arises for two reasons: A person who is accustomed to leading and can argue strongly also tends to be dominant within a group. Second, the behavior of subordinates is oriented towards their leader for reasons of personal benefit. This means expecting to gain favor by holding the view of the boss, and can occur consciously or unconsciously (cf. [31] for the theory of sociometric leader choice).

D. Readiness to Take Higher Risks at Group Level

People are ready to take higher risks at group level than in individual decisions (cf. examples [32], [33] and experiments [34], [35]).

- Allocation of responsibility: The risk level of group decisions increases with the number of liable participants (cf. [35]). A certain degree of anonymity arises as well, and risk aversion decreases with the degree of individual liability.
- A person who is willing to take higher risks has more influence: Individuals who tend towards risky decisions from the start argue more convincingly and are more successful at persuading others (cf. [36]).
- Social comparison: Brown [37] holds the view that risky decisions are preferred because of the social phenomenon that people willing to take higher risks have a better reputation. While this theory is not applicable in every situation, it often results in the unconscious attempt to take a little bit more risk than the other group members, which in turn leads to a positive evaluation of this person by the others.
- Strong arguments: According to Burnstein and Vinokur [38], group members are influenced by arguments that seem to be cogent, even in the case the argument or position being criticized is new and valid. Individual preferences as well as the characterization of the person and agreement with the person raising the argument can influence the rating of the argument.

E. Groupthink and its Criticism

Under certain circumstances, groups of sensible, smart, even shrewd men and women think and act in a way that can only be described as "collective stupidity" [32]. The most important psychological phenomenon in this area contains distortion mechanisms at individual and group level and results in a usually negative effect on decision finding.

The groupthink theory (cf. [39]) contains some preconditions that have to be met for groupthink to occur:

1) *High cohesion*: The phenomenon appears only in groups with a high or medium level of cohesion, due to the impossibility of individual members with a different view prevailing against the majority (cf. [40]). The main problem is the lack of disagreement and discussion in strong cohesive groups and the resulting isolation of opposition (cf. [20]).
2) *Compartmentalization* makes it easier to isolate oneself from external and new circumstances or restrictions. A compartmentalized group does not allow the influence of group harmony.
3) *Direct leading*: A patriarchic leader is not willing to accept disagreement.
4) The absence of *standardized decision procedures* leads to conformity and the loss of social control in the group's work.
5) Intragroup social and ideological homogeneity usually leads to homogeneous solutions of low impact due to the absence of opposition. The participants' goal is to achieve consensus at any price.
6) *Provocative and situational context*: Pressure on people with low self-esteem has a significant influence on the decision. Pressure to succeed leads to a high degree of conformity with group leaders' preferences. Low self-esteem arises from previous failures, excessive decision-making problems and moral dilemmas (cf. [40]).
7) *Tendency towards agreement*: People normally strive for harmony for reasons of conflict reduction within their environment.

Janis [33] characterizes the *symptoms of groupthink* with three, possibly overlapping, categories:

1) *Category 1 - overestimation of the group's own capabilities*: On the one hand, this is expressed by the illusion of invulnerability: the group holds the opinion that nobody and nothing is able to thwart them, which results in an extreme readiness to take risks. On the other hand, it results in the group's opinion that it upholds high moral and ethical standards, which creates a dilemma, as the group believes that everything it does is correct and, therefore, on a high ethical level.
2) *Category 2 – narrow-mindedness*: Everyone who holds a different view is excluded from the discussion. Further, stereotyping of opponents as well as collective resistance against warnings and different arguments is characteristic. Decisions that have already been taken are defended without considering new information and its implications.
3) *Category 3 - pressure toward uniformity*: This is mainly self-censorship that expresses itself in the tendency to keep doubts and misgivings to oneself.

Criticism of the groupthink theory is founded in part on the fuzzy definition of cohesion (cf. [40]). Classical conformity studies describe humans' aspirations towards a state of normative group conformity, where conformity within the group grows with an increasing degree of cohesion. Critics

address the case of different group norms: if the group norm does not prescribe the keeping of harmony but rather critical questioning, groupthink would be diminished. Furthermore, Janis holds the view that groupthink does not occur in groups with low cohesion. Schulz-Hart [40] disagrees and shows examples in which groupthink occurs in extreme situations or conditions such as compartmentalization outwards, homogeneity, directive leadership or extreme stress.

Janis only focuses on homogeneity of preferences, other forms are not accounted for. He does not explain how company-wide framework conditions can lead to unanimity. No methods are described for measuring low self-worth or hopelessness, and literature definitions disagree on contextual levels. In addition, there are some statements in Janis' work where the action-reaction relation is not sufficiently explained. Other issues include that there is no explanation of how overestimation of one's own capabilities and insularity can arise, because the pursuit of harmony or agreement cannot be used as an explanation [40]. There is also no clear specification what sort of consequences are caused by different preconditions. In response to the criticism Hart (cf. [32]) adds de-individualization. This concept is based on the work by Zimbardo [41] and defines unsocial, shortsighted behavior of groups and masses towards individuals with the goal of inducing groupthink. An opposing approach to explaining typical groupthink symptoms and the associated decision distortion was established by Whyte (cf. [42]), who bases his considerations on the prospect theory of Kahneman and Tversky [21]. Schulz-Hart [40] argues that the fiascos described by Janis [33] are founded on risk ignoring in case of loss expectancy and describes the groupthink characteristics as only cumulative values.

F. Decision Autism

According to Schulz-Hart [40] the distortion mechanism of decision autism occurs if a decision maker is controlled by self-affirmation tendencies. The symptoms are divided into 3 categories:

1) *Self-centered symptoms*: These are, first, a feeling of infallibility, which leads to a high degree of decision confidence and mental simplification of the problem area. Second there is self-reassurance, where any doubts are minimized by distorting them. The third is an increase in self-esteem, i.e., an increase of subjective confidence in oneself and one's opinion, combined with decreasing esteem for others and their opinions.
2) *Social symptoms*: Sniezek and Buckley [43] argue that social symptoms are not only of relevance within a group, but also for each individual, and lead to decision autism due to the fact that each individual acts in a social environment. Out of the whole range of social effects and symptoms, this refers to the ones who create selective communication. In this context, Schulz-Hart [40] has identified the following: more support for preferred discussion topics, selective attention, supporting likeminded people, and downplaying doubts. He also lists pressure on people who disagree, self-proclaimed mind guards and collective rationalization as symptoms resulting from personal attitudes that are only influenced at group level.
3) *Symptoms within the decision process*: Each step of the decision process potentially contains symptoms of decision autism (cf. [44]):

- Identification of the problem: Ignoring inconvenient problems, preference for supporting case studies.
- Generation of alternatives: Generation of fewer alternatives and focusing on the preferred one.
- Evaluation of alternatives: Distorted rating caused by selective information search, self-affirmation in evaluating information and rapid rejecting of divergent alternatives.
- Deciding: Lack of scrutiny of decisions.
- Implementation of the decision: Implementation without "what if" scenarios in mind.
- Control mechanisms: Excessive decision control.

IV. Overview of the AURUM Workshop

The AURUM Workshop is a process for supporting risk management. It is used to determine, refine and review security-relevant data needed as input for the AURUM risk management framework. The main characteristics of the AURUM Workshop are:

- Moderated: The workshop comprises three methods - Brainstorming/Discussion, Evaluation, and Selection - that are used by the moderator to get objective results from the workshop participants.
- Role based: Each process participant has a specific role that determines his tasks.
- Group based: Each process participant is a member of a small group of three or more people. By splitting one big group into several small groups, the approach aims to avoid psychological issues such as the "influence of majorities" and groupthink.
- Clear task structures: The process categorizes its tasks in three groups, where each is a basic type of task instances.
- Clear voting structures: The process provides a way to model consensus of opinions, which is based on the clear structures of the voting process.
- Awareness building: The AURUM Workshop aims to improve the security awareness of its participants in order to build an understanding of relevant risks, and options for their mitigation.

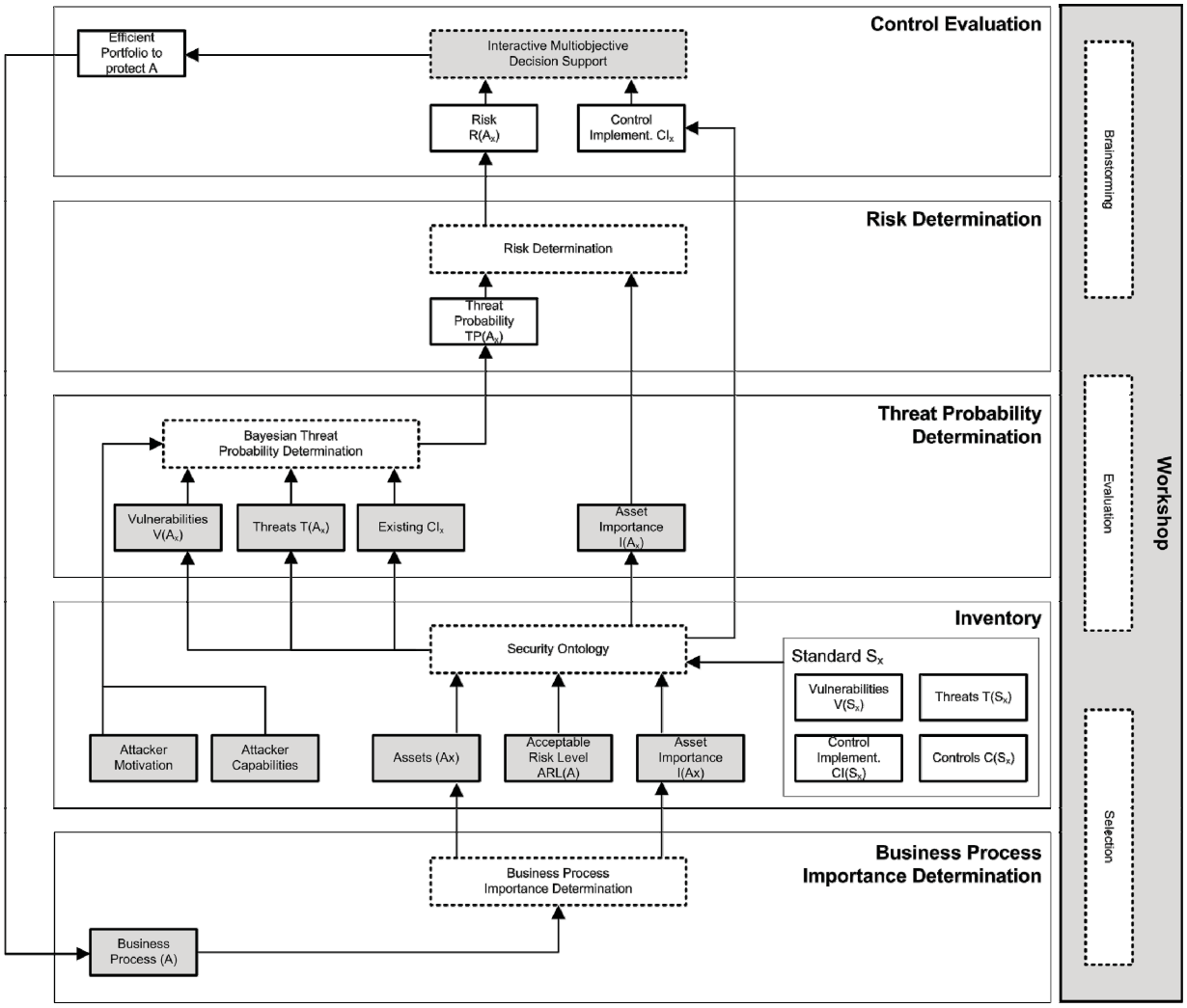

Figure 1. AURUM Workshop Process.

Figure 1 shows the overall scheme of the AURUM process and the integration of the AURUM Workshop. The gray squares denote activities and methods that are part of the workshop process. The workshop supports decision makers in going through the risk management process step by step. It supports the following risk management phases defined in AURUM: (i) Business Process Determination, (ii) Inventory, (iii) Threat Probability Determination and (iv) Control Evaluation. In the briefing phase, which is carried out prior to the workshop, the moderator selects a number of volunteers from different departments for the required roles.

V. ROLES

Heterogeneous group configuration can lead to impacts on decisions. To address this problem, this section outlines the roles used in the AURUM Workshop. A short description outlines each role's tasks and responsibilities, followed by a list of recommended skills for each role. We describe the main tasks of the role during the workshop and the interaction with other process participants (specifically whether and how they exchange knowledge and experience for task execution).

A. Moderator

Short Description: Ideally, a security consultant familiar with the AURUM process and the business area should be selected as moderator. It is highly recommended that the role of the moderator is assumed by an external consultant familiar with the process and its typical problems. If there is a high number of participants, two moderators can be selected.

Recommended Skills: High familiarity with AURUM, the ability to nurture security awareness and build an understanding of security in the participants' minds,

consideration of psychological issues that can occur in group decision processes.

Main Tasks and Interaction: The moderator has one of the main roles in the AURUM Workshop. He has to administrate groups and data input: (i) He defines small groups, creates user accounts and assigns roles to all process participants. (ii) Data exchange Data input tasks are mostly brainstorming, which involves naming and the need for merging and deleting. (iii) Data input: The moderator can choose whether he wants to join one of the small groups. In that case, he must input data like all other process participants. Due to the complexity and number of tasks the moderator has to deal with, this is not recommended. (iv) Regulation of interaction: The AURUM Workshop is characterized by highly interactive tasks where the moderator is the main interaction controller: he opens the tasks, users input data and discuss, and then he closes the task.

Involvement in Group: The moderator leads and guides the participants through the workshop. In this respect it is also not impossible for the moderator to be a member of a group, but because of the number and complexity of the tasks it is not recommended. Additionally, prior knowledge and his position of respect with regard to the other process participants can cause group dynamic issues.

B. Management Member

Short Description: This role is ideally assumed by members of middle or high level management who contribute to the group with structural and process knowledge. It must be taken into consideration that the dynamics between majorities and minorities within the group can cause problems with established authority relations outside the group. Therefore, it should be attempted to form groups at the same or similar levels of hierarchy. The presence of management members is an indispensable cornerstone of an accepted process execution at management level, due to their knowledge of cost restrictions and running processes. Before process execution, it is essential to ensure management support and therefore sufficient presence of management members.

Recommended Skills: (i) Process knowledge: Management members have to be aware of the strategic goals of internal or external business processes so as not to lose sight of integration problems that could be caused by new security controls. (ii) Knowledge of cost structures: The best security control set is worthless if it cannot be implemented due to cost restrictions. Including cost considerations from the beginning can eliminate unrealistic economical security control estimations. This requires a high degree of interaction with members in "security" roles concerning possible safeguard costs, and therefore security members with some knowledge of costs. (iii) The ability to present decisions and their costs at management level is indispensable for the adoption of the developed solutions. To build this understanding in management members' minds, it is necessary to impart knowledge about effects of security incidents before process execution. (iv) The task "category voting", in particular, has to be executed under guidance of the group's management member, who should have knowledge about cost and value categories the company uses and the ability to give the other process participant an idea of these categories..

Main Tasks: A rating task is done by the individual user and indicates an assignment of numerical values that were voted upon. Of special interest for management members is the task category of voting, where they contribute with data input as well as performing the leading role because of their special knowledge about cost and process structures.

Involvement in Group: Each management member is directly integrated in exactly one group. The interaction with members of other groups happens through discussion tasks. Each management member is involved in all group decisions and has the leading role in category evaluation.

C. Expert Member

Short Description: Depending on the problem area, an expert member can come from a different department. In our considerations these mostly concern information security employees, but generally this could be any department that tries to evaluate security claims and corresponding safeguards. An expert member fills the gap between the structural and cost knowledge of management members and the user experience of the key process user. Other process participants improve the expert's knowledge by giving him a broader view of the issues. Security expert members are essential for identifying the problem space and ideally help to understand problems at other business levels. It is highly recommended that the importance of team-oriented work is borne in mind in selecting the expert member. Expert members who are not willing or able to share knowledge and responsibility are a destructive power and impede the process.

Recommended Skills: (i) Infrastructural knowledge to handle the asset identification is one of the main skills an expert member must have. This also holds true for experience with past incidents affecting the assets in question and their occurrence rates, which is essential for refining probability ratios. (ii) Technology knowledge: The ability to identify and estimate possible synergy effects and effectiveness of safeguard candidates. Records and statistics can be of additional help in these steps. (iii) Cost knowledge, which is important in interacting with the management members. Without feasible estimations about possible safeguard implementation costs, the management is unable to consider cost restrictions in the evaluation process. It is rarely possible to give even a rough estimate because of the difficulty of determining issues like installation, maintenance, etc.

Main Tasks: A rating task is performed by an individual user and is an assignment of numerical values to tasks that were voted upon. Of special interest for expert members is the task asset voting, where they input definition data because of their special infrastructural knowledge, as mentioned above. Risk voting is also performed only by the expert members and deals with the estimation of occurrence rates.

Involvement in Group: Each expert member is directly integrated in exactly one group. The interaction with members of other groups happens through discussion tasks as described above. Each expert member is involved in all group decisions.

D. Key Process User

Short Description: In addition to the structural and expert knowledge provided by management and expert members, users must also contribute to the process. The participation of key process users also enhances acceptance of the decided actions and their costs at employee level. In the selection of key process users, it is recommended that their prior knowledge and openness to new approaches are taken into consideration. Candidates with negative attitudes towards new ideas can cause major acceptance problems. It is essential to understand that if the key process users are not convinced of the approach, they will not be able to communicate the idea and need for information security measures at their business level.

Recommended Skills: (i) Experience with main business processes and tasks to enable use of user know-how within the process considerations. This, in particular, takes data input problems into consideration at the task execution level, as well as experience with the use of previous information security measures. (ii) Ability to defend unwelcome decisions at execution level founded on in-depth knowledge about their necessity. This is based upon the introduction to security problems and possible consequences at the briefing held prior to the process.

Main Tasks: A rating task is done by the individual user and indicates an assignment of numerical values to voted tasks. In the current version this is only done manually to get an asset ranking and to evaluate the incident occurrence rate; the rating of the other steps occurs automatically via the number of mentions. Discussions are lead by the moderator, who is the only one who can perform data changes on that basis. Unlike the other roles, the key process users themselves do not have any tasks in which they assume a leading role.

Involvement in Group: Each key process user is directly integrated in exactly one group. The interaction with members of other groups happens through discussion tasks as described above. Each key process user is involved in all group decisions.

VI. WORKSHOP METHODS

The workshop comprises three methods that are used by the moderator to generate data necessary to carry out the risk management process (see Table II): Brainstorming, Evaluation, and Selection.

1) *Brainstorming:* Brainstorming enables a group of decision makers to quickly assess the data relevant for the information security of their organization. The system supports the decision makers as they enter as many items as they judge appropriate.
2) *Evaluation:* Based on Grünbacher (cf. [45]) we use a border criterion voting mechanism for rating the items gathered during brainstorming. Each participant decides upon the importance and ease of implementation of the so-called win conditions. The system calculates a medium value depending on the degree of consensus.
The voting results are underlined with a traffic light system to signal the degree of controversiality using the colors red (<50% consensus), orange (>=50 and <=75% consensus) and green (>75% consensus). The borders are variable and arise from task-dependent mathematical methods: (i) Taking numerical values as input, the standard deviation of the input values from the different decision makers is used to determine the threshold and, thus, the degree of consensus. (ii) Taking the number of votes as input, the number of votes related to the total number of voters determines the threshold and, thus, the degree of consensus. To avoid disagreement, e.g., out of ignorance, the voters are instructed not to vote if they do not know. The evaluation process can be summarized as follows:
   a) A set of possible win conditions arising from brainstorming phases are the input for voting.
   b) Each possible win condition is voted on in the categories of business importance and ease of realization. To avoid distortion from blind votes, the members are instructed not to vote if they do not know.
   c) The average of each condition over the two categories will be displayed, and a red/green colored marking indicates the degree of consensus.
   d) A structural discussion helps to clarify reasons for disagreement and convey tactical knowledge known to individuals to the rest of the group [45].
3) *Selection/Discussion:* During a group discussion based on the ratings' analysis, the group decides which items are to be selected. If judged necessary, the brainstorming and rating steps can be repeated. Discussion tasks have to be carried out after voting in order to resolve any disagreements. The degree of consensus or disagreement an issue receives determines how it is handled in the discussion, with the moderator acting as a mediator. Of course, the nature of group discussions is always to some extent undefined and it is difficult to determine concrete rules. Therefore, a moderator with high psychological and didactic competence is required. Nevertheless, some general suggestions are made below to aid the moderator in this complicated task.

It is suggested to address orange and red color items by questioning:

- Ask an individual member why he or she thinks that a point is important or not. The points that he or she mentions will certainly be agreed or disagreed with by several members, forming the basis for the discussion.
- Allow constructive interruptions but make sure to guard against domination by a few members (cf. Chapter 4.5, especially the problem of "majorities and minorities").
- If only one person has mentioned a specific issue, do not ask this person why he or she thinks that it is important. Instead ask another member in order to avoid the human

tendency to wait for explanations (cf. Chapter 4.5); possibly he or she will bring up issues nobody has thought about.

In the end a generally accepted solution/rating should be found. If this is not possible after an adequate amount of time, the only possibility for the moderator is to overrule the disagreeing parties with a compromise. This must be considered a last option and should be avoided whenever possible.

TABLE II. CHARACTERISTICS OF TASK TYPES

	Brainstorming Task	**Evaluation Task**	**Selection/Discussion Task**
Executors	Participants in a specific role (instance dependent).	Participants in a specific role (instance dependent).	All participants.
Input	List of issues which have to be rated mathematically.	The question what is imaginable for ... ; i.e., a brainstorming request.	A list of issues from a prior voting task, containing items on which the participants do not agree or agree only in part.
Output	List of numerical values assigned to issues.	A list of written issues with a certain degree of consensus.	Changes in the input list which represent a more accepted output list, and/or more sophisticated user.

VII. THE AURUM WORKSHOP PROCESS

This section explains the phases of the AURUM Workshop in detail. Each step is described according to the three criteria of input, output, and sub-steps. The sub-steps list the necessary internal tasks and explain the reason and the type of task for each one, breaking down a quite complex process step into manageable and understandable topics.

A. Workshop Briefing

After reviewing and selecting workshop participants according to their profile and the requirement definition in section 7.2, the members are briefed on the goals of the process: (i) Definition of the risk analysis context and goals: This first step aims at defining the scope of the workshop and its goals. This is required for the orientation of the process and the definition of criteria and to measure its success. (ii) Selection of workshop participants: In order to raise the efficiency of the workshop session in terms of quality and quantity of the workshop output, the moderator must select participants according to their knowledge, their suitability. Participants should be selected to cover the whole spectrum of security problems and include a manager in charge of the decisions to emerge from this process. (iii) Psychological issues: With knowledge of psychological dynamics in group decisions, the participants may be able to avoid typical problems. (iv) AURUM Workshop process: Participants are informed about the process steps, especially input and expected output data. This has to happen in a way that ensures the members understand their roles and, therefore, their integration in the process, including issues such as voting mechanisms, group structuring, etc. (v) Terminology: For successfully conducting the workshop part of the process, it is essential to impart knowledge of basic security terms and how they relate.

The following section outlines suggestions for briefing the workshop participants, especially concerning issues arising from related work. The main points of concern during the execution of the process are the following:

- Why the workshop is carried out: Which goals and prospects regarding process output exist and how this approach differs from previous ones.
- Characterization of the business unit: The participants have to be informed about affected business. If most participants (especially non expert members) have only limited knowledge about the field in question, a short introduction is suggested. It is assumed that sufficient knowledge about business concerns will help to understand problem complexity and needs. In case of a general information security safeguard evaluation this point can be ignored, focusing more generally on process goals.
- Explaining MOSEP workflow: Participants have to be informed about the individual steps (cf. chapter 8.6); in particular, input and expected output data are important for seeing the overall picture in terms of risk assessment (cf. chapter 3).
- Understanding of security terms and their mashing: It is essential for performing the workshop part of the process to impart knowledge of basic security terms (cf. chapter 2) and how they relate.
- Building security awareness: The awareness problem was discussed in chapter 6. Participants have to understand difficult terms, like "social engineering", "human asset" etc., to perform a more feasible evaluation.
- Building awareness of possible psychological influence: With knowledge of psychological dynamics in group decisions (cf. chapter 4.5), the participants may be able to avoid typical problems.

The participants are asked to perform an interactive knowledge exchange through question/answer interaction. Each moderator uses different methods of interaction and communication, depending on personal experience and preferences.

B. Phase 1: Business Process Importance Determination

Description: This step aims to identify the most relevant business processes. For this purpose, the expert group is asked to execute a brainstorming and evaluation task. Gross discrepancies (foremost red-colored items) have to be discussed by the workshop members, and result in an accepted list of processes ranked by their importance.
Steps:

- Business Process Selection: The decision makers select the business processes to be evaluated. This step includes the discussion of the selected processes and their ranking in the event of a low degree of consensus. In order to resolve such problems, the moderator should discuss the following questions with the workshop participants: "Why were certain processes mentioned?" and "Why did certain members vote high and others low for the importance of an issue?"
- Business Process Importance Determination: The decision makers determine the importance of the selected business processes within the corporation, and their need for protection.

Main Question: What should be protected?
Output: An accepted list of business processes ranked by importance.

C. Phase 2: Inventory

Description: This step aims to identify the most relevant assets. For this purpose, the expert group is asked to execute a brainstorming and evaluation task. Gross discrepancies have to be discussed by the workshop members, and result in an accepted list of assets ranked by their importance. Note that this phase can be supported by the AURUM security ontology, which already contains a wide selection of assets. Thus, decision makers only need to review the assets proposed by the ontology and the discussion can focus on the issues where little consensus exists.
Steps:

- Assets: This step includes the discussion of the assets corresponding to the selected processes.
- Asset Importance Determination: The decision makers determine the importance of the selected assets, and, thus, their need for protection. The decision makers can use a suggestion made by the system that is calculated based on the importance of the business processes (cf. [6]).
- Acceptable Risk Level: Level of risk judged to be outweighed by corresponding benefits or one that is of such a degree that it is considered to pose minimal potential for adverse effects.
- Attacker Capabilities: This step aims to evaluate and define the capabilities of potential attackers.
- Attacker Motivation: This step aims to evaluate and define the motivation of potential attackers.

Main Question: Which assets exist, and which of them are really worth protecting?
Output: An accepted list of assets ranked by their importance, the acceptable risk level for each business process, the attacker capabilities, and the attacker motivation.

D. Phase 3: Threat Probability Determination

Description: This step aims to determine and review vulnerabilities, threats and existing countermeasures. It aims to evaluate possible threats and their causes. The basic data for this purpose is the asset list assembled in process step 1. First, the possible threats for each asset have to be determined, which happens through group voting. The result is a list of threats, in which each threat has to be argued by listing dangers (also group voting), which produces a list of vulnerabilities for each threat. The vulnerability and the threat determination have to be concluded by a discussion task based on the degree of consensus in the two voting steps. For this purpose, the expert group is asked to execute a brainstorming and evaluation task. Gross discrepancies have to be discussed by the workshop members, and result in an accepted list of vulnerabilities and threats ranked by their importance. Note that this phase can be supported by the AURUM security ontology, which already contains a wide selection of vulnerabilities and threats based on established security standards such as ISO 27001 or NIST SP 800. Thus, decision makers only need to review the assets proposed by the ontology, and discussion can focus on the issues where little consensus exists. In this case voting can be limited to selection tasks, the vulnerabilities follow automatically and only have to be adapted to the specific business needs.
Steps:

- Vulnerabilities: Based on the list of threats, the next step deals with determining the causes for each threat.
- Threats: This sub-step attempts to evaluate a set of corresponding threats for each asset. The execution as voting task requires brainstorming on behalf of the group and input concerning problematic circumstances. The moderator aggregates the data to obtain the list of threats for each asset that is the output of this sub-step.
- Existing countermeasures: This step aims to review and evaluate existing countermeasures.

Main Question: Which dangers are the individual assets exposed to?
Output: Accepted lists of threats and corresponding vulnerabilities.

E. Phase 4: Control Evaluation

Description: Based on the risk evaluation, the set of possible administrative, technical and physical controls required to avoid such incidents must be determined. This is achieved by voting, followed by a discussion. The output is a set of controls for each risk. Alternatively, it is possible to define only the requirements for control. Concrete products can be determined in the post-workshop evaluation step.
Steps:

- Criteria Definition: This step defines a set of criteria concerning business conditions and possibly related enterprise-wide controlling mechanisms.
- Interactive Selection: This step supports decision makers in determining the solution that best fits their ideas and objectives, choosing from the possibly hundreds (or even thousands) of Pareto-efficient alternatives of countermeasure portfolios identified previously. The procedure starts with an efficient portfolio and allows the decision maker to iteratively move in solution space towards more attractive alternatives until no "better" portfolio can be found. The system provides immediate feedback about the consequences of different choices in terms of the remaining alternatives and, thereby, allows the decision maker to evaluate different investment scenarios. The system provides the decision maker with ample information on the specific selection problem and ensures that the finally selected solution will be an optimal (i.e., Pareto-efficient) one.

Main Question: Which countermeasures are possible?
Output: Accepted lists of countermeasure portfolios for protecting the selected business processes.

VIII. Conclusion

Managers regularly have to cope with a wide spectrum of potential risks and, therefore, the decision of selecting the most appropriate set of security safeguards. Moreover, they are challenged by legal and economic requirements leading to the demand to carry out risk assessment on a regular basis. This paper proposed an approach called AURUM Workshop for integrating the advantages of workshops into the established risk management solution AURUM. It provides decision makers with a stepwise method for risk assessment by taking into account and mitigating typical psychological and social influence factors that usually occur in (group) decision processes. Decision makers are supported by a moderator who provides professional advice during the entire process and reduces the influence of individual opinions on the whole decision. AURUM Workshop is intended to not only evaluate data, but also to impart security awareness to the participants in order to build an understanding of relevant risks, and options for their mitigation. It supports decision makers in identifying and focusing on the most important risks and provides intuitive interactive decision support for evaluating different protection scenarios.

Acknowledgment

This work was performed at the Vienna University of Technology and the research center Secure Business Austria funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria, and the City of Vienna.

References

[1] Workshop-Based Risk Assessment for the Definition of Secure Business Processes; Thomas Neubauer and Markus Pehn; International Conference on Information, Process, and Knowledge Management (eKNOW'10), IEEE Computer Society, 2010, pp. 74-79.

[2] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of it security breaches," *Information Management & Computer Security*, vol. 11/2, 2003, pp. 74–83.

[3] A. Ekelhart, T. Neubauer, and S. Fenz, "Automated risk and utility management," in *2009 Sixth International Conference on Information Technology: New Generations*. IEEE Computer Society, 2009, pp. 393–398.

[4] A. Ekelhart, S. Fenz, and T. Neubauer, "Ontology-based decision support for information security risk management," in *International Conference on Systems, 2009. ICONS 2009.* IEEE Computer Society, March 2009, pp. 80–85.

[5] ------, "Aurum: A framework for supporting information security risk management," in *Proceedings of the 42nd Hawaii International Conference on System Sciences, HICSS2009*Los Alamitos, CA, USA: IEEE Computer Society, January 2009, pp. 1–10, 978-0-7695-3450-3.

[6] S. Fenz, A. Ekelhart, and T. Neubauer, "Business process-based resource importance determination," in *Proceedings of the 7th International Conference on Business Process Management (BPM'2009)*. Springer, 2009, pp. 113–127.

[7] T. Neubauer and C. Stummer, "Extending Business Process Management to Determine Efficient IT Investments," in *Proceedings of the 2007 ACM Symposium on Applied Computing*, 2007, pp. 1250-1256.

[8] T. Neubauer, A. Ekelhart, and S. Fenz, "Interactive selection of ISO 27001 controls under multiple objectives," in *Proceedings of the Ifip Tc 11 23rd International Information Security Conference, IFIPSec 2008*, vol. 278/2008. Boston: Springer, July 2008, pp. 477–492.

[9] T. Neubauer and C. Stummer, "Interactive selection of web services under multiple objectives," *Information Technology and Management,* vol. 11(1), 2010, pp. 25-41.

[10] E. Kahle, *Betriebliche Entscheidungen*Oldenburg, vol. 6, 2001.

[11] M. Frech, Arbeit in und mit Gruppen in Kasper, H. and Maierhofer, W.(eds.) Personalmanagement-Führung - Organisation. Wirtschaftsverlag Ueberreuter, 1996.

[12] W. Staehle, Management - Eine verhaltenswissenschaftliche Perspektive. München, 1991.

[13] E. Saliger, Betriebswirtschaftliche Entscheidungstheorie. Oldenburg, 2003.

[14] H. Laux, *Entscheidungstheorie*. vol. 6 Springer, 2007.

[15] R. Paschka, *Multipersonalität bei Mehrfachentscheidungen*. Deutscher Universitätsverlag, 1995.

[16] J. Bidlingmaiyer, *Unternehmerische Zielkonflikte und Ansätze zu ihrer Lösung*. Zeitschrift für Betriebswirtschaft, 38, No.3, 1968, pp.149 - 179.

[17] B. Roy, Decision Aid and Decision Making in Costa, C. A. Bana e (ed.): Readings in Multiple Criteria Decision Making. Berlin, 1990.

[18] K. Adler, International Dimensions of Organizational Behavior 4th Edition. Ohio, South Western/Thomson Learning, 2002.

[19] J. Martirossian, *Decision Making in Communities: Why Groups of Smart People Sometimes Make Bad Decisions*. Community Association Press, A Division of Community Association Institute, 2001.

[20] W. Auer-Rizzi, Entscheidungsprozesse in Gruppen - kognitive und soziale Verzerrungstendenzen. Wiesbaden, DUV, 1999.

[21] A. Tversky and D. Kahneman, "Availability: A heuristic for judging frequency and probability." *Cognitive Psychology*, vol. 5, 1973, pp. 207–232.

[22] R. Nisbett and L. Ross, *Human Inference: Strategies and Shortcomings of Social Judgment.* Englewood Cliffs: Prentice Hall, 1980.

[23] P. Slovic and S. Lichtenstein, "Comparison of Bayesian and Regression Approaches in the Study of Information Processing in Judgment," *Organizational Behavior and Human Performance*, vol. 6, 1971, pp. 649 – 744.

[24] M. McCloskey and M. Zaragoza, "Misleading postevent info and memory of events: Arguments and evidence against memory impairment hypothesis." *Journal of Experimental Psychology: General*, vol. 114, 1985, pp. 1 – 16.

[25] A. Tversky and D. Kahneman, "The framing of decisions and the psychology of choice," *Science*, vol. 211, 1981, pp. 453 – 458.

[26] D. Stahlberg, A. Maas, and D. Frey, "We knew it all along: Hindsight bias in groups." *Organizational Behavior and Human Decision Processes*, vol. 63, 1995, pp. 46–58.

[27] L. Festinger, "Informal social communication," *Psychol. Rev.*, vol. 57, 1950, pp. 271–282.

[28] S. Asch, "Studies of independence and conformity: a minority of one against an unanimous majority." *Psychol. Monogr.*, vol. 70, 1956, p. 9.

[29] S. Moscovici and C. Faucheux, *Social influence, conformity bias and the study of active minorities*, t. E. In: Berkowitz, L. Advances in experimental social psychology, Ed. Academic Press, New York-London, 1972.

[30] R. D. Mann, "A review of the relationships between personality and performance in small groups," *Psychol. Bull.*, vol. 56, 1959, pp. 241–270.

[31] R. F. Bales and P. Salter, "Role differentiation in small decision making groups" in Parsons, T. and Bales, R. F.: "Family, socialization, and interaction process," *Free Press, Glencoe/Illinois*, vol. 1, 1995, p. 1.

[32] P. Hart, *Groupthink in government: A study of small groups and policy failure*. Amsterdam, Swets & Zeitlinger, 1990.

[33] I. Janis, *Groupthink. Psychological Studies of Policy Decisions and Fiascoes.* Boston: Houghton Mufflin, 1982.

[34] J. Stoner, "A comparison of individual and group decisions involving risk." Ph.D. dissertation, School of Industrial Management, M.I.T., 1961.

[35] M. Wallach, N. Kogan, and D. Bem, "Group influence on individual risk taking." *J.Abnorm. Soc. Psychol.*, vol. 65, 1962, pp. 75–86.

[36] B. Collins and H. Guetzkow, A social psychology of group processes for decision making. Wiley, New York, 1964.

[37] Brown, R. (1965). Social psychology. New York: Free Press.

[38] E. Burnstein and A. Vinokur, "Testing two classes of theories about group-induced shifts in individual choice." *J. Exp. Social Psychology*, vol. 13, 1973, pp. 315–332.

[39] H. Franke, Problemlösen in Gruppen: Veränderungen im Unternehmen zielwirksam realisieren, 3, Ed. Leonberg:Rosenberger Fachverlag, 1998.

[40] S. Schulz-Hart, Realitätsflucht in Entscheidungsprozessen - von Groupthink zum Entscheidungsautismus. Ber: Verlag Hans Huber, 1997.

[41] P. Zimbardo, "The human choice: Individuation, reason and order versus deindividuation, impulse and chaos," *In: Arnold W. J. and Levin D. (Eds.): Nebraska symposium on motivation, University of Nebraska Press, Lincoln*, vol. 17, 1969, p. 1.

[42] Whyte, G., & Sebenius, J. K. (1997). The effect of multiple anchors on anchoring in individual and group judgment. Organizational Behavior and Human Decision Processes, 69, 75–85.

[43] J. Sniezek and T. Buckley, "Cueing and cognitive conflict in judge-advisor decision making." *Organizational Behavior and Human Decision Processes*, vol. 62, pp. 1995, 159–174.

[44] R. Aldag and S. R. Fuller., "Beyond fiasco: A reappraisal of the groupthink phenomenon and a new model of group decision processes," *Psychological Bulletin*, vol. 113, 1993, pp. 533–552.

[45] P. Gruenbacher and R. Briggs, "Surfacing tacit knowledge in requirements negotiation: Experiences using EasyWinWin," *Proceedings of the 34th Hawaii International Conference on System Sciences*, vol. 34, 2001, pp. 1–8.