Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

Security risk assessment: Group approach to a consensual outcome

Ben Beard
Edith Cowan University

David J. Brooks
Edith Cowan University

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/8

Security risk assessment: Group approach to a consensual outcome

Ben Beard
David J Brooks
School of Engineering and Mathematics, Edith Cowan University
International Centre for Security and Risk Sciences
bjbeard@student.ecu.edu.au
d.brooks@ecu.edu.au

Abstract

AS/NZS4360:2004 suggests that the risk assessment process should not be conducted or information gathered in isolation. This insular method of data collection may lead to inaccurate risk assessment, as stakeholders with vested interests may emphasise their own risks or game the risk assessment process. The study demonstrated how a consensual risk assessment approach may result in a more acceptable risk assessment outcome when compared to individual assessments. The participants were senior managers at a West Australian motel located on the West Coast Highway, Scarborough. The motel consists of four three storey blocks of units, resulting in a total of 75 units. The three main areas of the business are Reception and Management, Housekeeping and Maintenance. The participants were interviewed individually and then as a group. Two activities took place in the study, an individual identification and analysis of risks affecting the facility, followed by a consensual group analysis of the same risks. The individual risk assessment results were collated and compared to the results of the consensus group. This demonstrated that individuals over or under emphasise some risks, dependant on personal affect. The study illustrated that a consensual style of risk information collection and assessment was more acceptable to the group then assessments conducted in isolation.

Keywords
Risk management, risk assessment, consensus, group

INTRODUCTION

It could be considered that the field of risk management is affected by small discrepancies in the information gathering process, resulting in significant impacts on the final outcome of a risk survey. To measure this affect, the research examined two methods of risk data collection in order to find the most appropriate approach. Individual interviews with the stakeholders and risk evaluation by the consultant is considered one method. The second is a facilitated meeting with stakeholders present to develop a consensus decision on risk. The participants for this research study were a motel located in Scarborough, Western Australia. The facility contained three main departments: Housekeeping (HK), Maintenance (M) and Administration (A). The method of data collection will be described and analysed to determine which is more appropriate, based on the results gathered.

RISK MANAGEMENT

Risk management provides a sensible approach to managing risk (Fischer & Green, 2004, p. 130) and a generic guideline is AS/NZS4360:2004 Risk Management (Standards Australia, 2004). AS/NZS4360:2004 is often considered "almost a de facto global standard" (Jay, 2005, p. 2) and has become an international template on dealing with risk, having been used in Canada and United Kingdom, and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005, pp. 2-3). AS/NZS4360:2004 is utilised in diverse disciplines, from financial to engineering and is "widely used by security professionals and risk managers across Australia" (Jones & Smith, 2005, p. 2).

The Australian Standard stages of the risk management process instruct that all relevant stakeholders need to be included in the process. According to the Standard, stakeholders are "those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk" (Standards Australia, 2004, p. 6). Further to this aspect is the need to take a "consultative team" approach (Standards Australia, 2004, p. 19). But it can be argued that the standard does not present the necessity of providing a consensual assessment (Koller, 1999; Koller, 2000), with an appropriate methodology with a consensus based stakeholder meeting.

It could be suggested that without consensus assessment, risk are assessed in isolation. An insular method of data collection and assessment may lead to inaccurate risk management, as stakeholders with vested interests may emphasise their *own* risks or *game* the risk assessment process. Also, assessors may bias the assessment process based on an individuals beliefs, perceptions and experience (Brooks, 2005).

The consensus methodology is supported by Koller (2000, p. 67), when he asserted that "maximum benefit from the risk processes is realized only when multiple opportunities are consistently assessed or compared", with a salient aspect of consistency being the arrival of a *consensus* (Koller, 2000, p. 68). The consensus approach may be supported, particularly for security risk, by the assumption that there is generally limited historical data.

AS/NZS4360:2004 RISK MANAGEMENT

There are defined stages within the AS/NZS4360:2004 Risk Management standard, represented in figure 1.

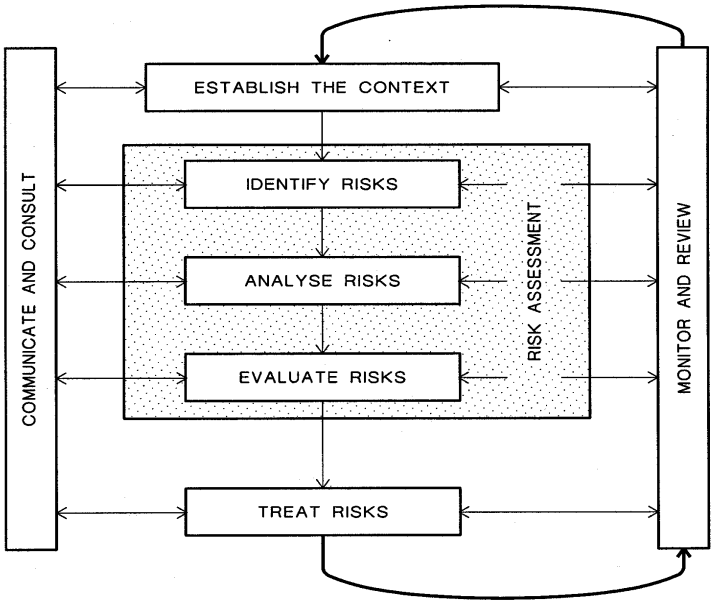

Figure 1 AS/NZS4360:2004 Risk management structure (Standards Australia, 2004).

Establish Context

The first of these stages is *Establish the Context*, where relevant stakeholders must be consulted, the goals and objectives of the survey defined and the facility's layout and culture taken into consideration (Standards Australia, 2004). This stage includes internal, external and risk management contexts.

Risk Identification

The next stage in the risk management process is to identify the risks and this stage will consider how when and why risks could hamper the effectiveness of the facility. Methods of achieving this include brainstorming with relevant stakeholders, consulting outside experts and flow charts (Standards Australia, 2004).

Risk Analysis

After the risks have been identified, the following stage is to *analyse risks*. This stage provides meaning to the information, utilizing tables provided in AS/NZS4360:2004. The risks will be analysed on their perceived likelihood and consequence. Consequence is considered as the "outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain" (Standards Australia, 2004, p. 5) and is rated according to how severe an impact the risk would have on the organisation if realised. Likelihood is defined as a description of the probability or frequency that an event may occur, expressed in a qualitative form (Standards Australia, 2004).

Tables assign each risk with a quantitative value that can then be compared across all risks. Table 1 presents values that may be assigned to likelihood, ranked from the most likely to the least from A to E.

Table 1
Likelihood

Level	Descriptor	Description
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

(Standards Australia, 2004)

Table 2 presents values that may be assigned to consequence, ranked from insignificant (1) to catastrophic (5).

Table 2
Consequence

Level	Descriptor	Example detail description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, on-site release immediately contained, medium financial loss
3	Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release off-site with detrimental effects, major financial loss

(Standards Australia, 2004)

Evaluation of risk

The preceding tables (Tables 1 and 2) are then integrated in the following risk management stage. *Evaluation of risks* creates a matrix (Table 3) that is capable of evaluating any of the analysed risks according to both consequence and likelihood. The matrix table applies a rank to each risk, from extreme to low risk. An extreme risk is considered a risk that requires immediate management mitigation (Standards Australia, 2004).

Table 3: Risk Matrix

	Consequence				
Likelihood	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	High	High	Extreme	Extreme	Extreme

B (likely)	Medium	High	High	Extreme	Extreme
C (possible)	Low	Medium	High	Extreme	Extreme
D (unlikely)	Low	Low	Medium	High	Extreme
E (rare)	Low	Low	Medium	High	High

(Adjusted from Standards Australia, 2004)

Risk treatment

The final risk management stage according to AS/NZS4360:2004 is *treat the risks*. Risk treatment considers mitigation strategies most suited to controlling the risk and may consider *risk reduction*, *risk transfer*, *risk avoidance* or *risk acceptance*. The method utilised will depend on a managerial decision.

One of the two overarching steps that should be undertaken at each point in the process is to *Communicate and Consult*. According to the standard this needs to include all stakeholders, to ensure that risk management is being completed to the established context, accurate information is being analysed and that any treatment options are acceptable to the users of the facility (Standards Australia, 2004).

The final stage in the standard, although considered at every stage of the risk management process, is *Monitor and Review*. Monitor and review facilitates constant improvement and accuracy throughout the process. It also measures the effectiveness of any treatment options that may have been implemented (Standards Australia, 2004).

STUDY DESIGN

The study utilised a two stage approach, the first being an individual risk survey. The second stage utilised the initial data from the individual survey, but included a consensus survey. The study design was utilised to measure the affect on the risk assessment outcomes. The individual approach consisted of interviewing each representative of Administration, Maintenance and Housekeeping in the two areas of *identifying the risks* and the *analysis of the risk*, as suggested by AS/NZS4360:2004 (Standards Australia, 2004). The survey collected the data from the different areas and compared the different lists of identified risks, considering only the five highest rated risks from each area.

The second stage, consensus method, followed from this initial process but brought the stakeholders together to provide a consensual agreement. Consensual agreement was sort between the *identified risks* and *rated risks*, resulting in a *ranked* list of risks. These results showed whether or not there were discrepancies between the risk perceptions of the Administration, Housekeeping and Maintenance areas. Finally, the study allowed analysis of whether a consensus style approach is a more appropriate to the risk assessment process.

FACILITY DESCRIPTION

The facility utilised in the study was a motel located on the West Coast Highway, Scarborough, Western Australia. The site consisted of four blocks of units, each three storeys high, with a total of 75 units. The facility also contained several auxiliary areas including reception, maintenance workshop, housekeeping laundry and various storage rooms. Each of these different areas was examined with regards to the various threats and risks they are affected by. The reception and office areas house intellectual property such as customer and employee records, policies and procedures and security measures.

Administration

The office area consists of reception, client bookings and management offices, covering financial, information and organisational facets of the facility. All cash and motel income is processed through this area, as are guest bookings.

Housekeeping

Housekeeping is considered vital to the business continuity of facility as it maintains the rooms in a high quality condition. Additionally guests are kept satisfied with room service, ensuring return business on many occasions. The laundry operates at a full capacity for the majority of the day, with staff typically working a 9:00am to 3:00pm shift, although it does vary according to how busy the motel gets. Key facilities are the laundry and cleaning shed.

Maintenance

Maintenance at the facility provides a similar role to Housekeeping, maintaining facility plant and equipment, and fixtures and fittings. The department is also responsible for gardens and pool area, including room and facility security.

FACILITY RISK ASSESSMENT

Participants from each facility area completed the risk assessment process, initially individually and then by consensual agreement.

Individual Analysis

Individual assessment followed the stages suggested by AS/NZS4360:2004, which included risk identification, risk analysis, risk evaluation and finally, risk ranking. Each participant completed this process individually, with no contact between the other facility participants.

Identification of Individual Risks

The risks facing the facility were identified with the assistance of each area of the business. They have been divided into two categories to assist with risk identification and analysing, both internal risks and external risks. In order to assist identification of external risks, crime statistics for the Western Australian Police region were used (Fischer & Green, 2004; Western Australian Police Service, 2004; Western Australian Police Service, 2004). According to the participants, the facility risks were broad in both categories as it was dependant on the attacker as to how the risk could be treated.

Analysis of Individual Risks

The risks were identified as affecting the facility, but in order to create a range of treatment options they also needed to be analysed so that the effect they have on the facility and the frequency with which they occur could be examined. This approach allowed a rating to be assigned to each of the risks identified to show how significant they are to the facility. According to table 4, the participants individually applied a consequence and likelihood to each identified risk. This analysis allowed the individual risks to be ranked according to the risk matrix (Table 3), resulting in the following risk rankings (Table 4).

Table 4
Individual departmental ranked risks

	Site departments				
Risk rank	**Housekeeping**		**Administration**		**Maintenance**
1	Lack of Staff	(A4)	OS&H (Fraudulent claims)	(B4)	OS&H (Workplace)
2	Syringes left in room	(B4)	Theft (Motor vehicles)	(C4)	Accidents (FP&E)
3	Confronting trespassers	(A3)	Burglary (Administration)	(C4)	OS&H (Lifting)
4	OS&H (Slip hazards)	(B4)	Fraud (Extended credit)	(C4)	Easily accessible FP&E
5	Verbal conflict with guests	(B3)	Armed robbery (Administration)	(C4)	Vandalism & Theft

Administration

Administration identified many internal and external risks, mostly in the areas of finance and security. External risks identified included vandalism, trespass, burglary and theft from all areas, robbery, computer based attacks,

malicious code and various types of assault. Internal risks covered theft by employees of all areas, and several types of fraud, ranging from extended credit to accounting. All of the Administrative risks were assessed as extreme risks, with the majority of consequences being major or higher, and the likelihood ranging between possible and likely.

Housekeeping

The risks identified by Housekeeping were generally parochial, being those affecting only housekeeping staff. External risks were trespass, vandalism, theft of housekeeping and grounds related equipment, speeding and dangerous behaviour in car parks, abuse from trespasser, broken glass in pool and spa areas, and security of rooms and keys. Internal risks that were identified are theft by staff, lack of staff scrutiny and accountability to security, and several OS&H risks in various contexts. Night time risks were excluded by the interviewee, as they do not work after *normal working hours*. In the assessment, OS&H related risks were given an *extreme* rating and guest relation risks were given *high* ratings. All consequences were rated *very highly* and likelihood at mid range on the scale.

Maintenance

Risks identified by maintenance emphasis Fixed Plant and Equipment (FP&E) and maintenance based tasks. The security function falls under the domain of maintenance and as suggested by the participant, he identified only a few security risks as he had confidence in their security system. External risks identified were vandalism, the roadside exits of the motel, unsecured rooms, theft from laundry and parked cars, unsecured telephone, electricity and gas FP&E, and OS&H threats to guests in one block. Maintenance believed that there were no internal risks, as the facility had a strong relationship with employees. In the risk assessment, maintenance risks were not analysed according to AS/NZS4360:2004, but only ranked in a perceived order by the participant.

Consensual Analysis

The consensual stage utilised the risk assessment data collated at the first individual stage. The first stage produced individual assessed and ranked risks (Table 4). For the second stage participants were brought together and asked to reassess and rank the top five individually rated risk from stage one. Individual participants were asked to come to a group consensus on their reassessment and risk rankings. The outcome of this stage produced the consensus ranked risk list (Table 5).

Table 5
Consensual ranked risks

Ranked position	Consensual ranked risks
1	OS&H (Workplace)
2	OS&H (Fraudulent claims)
3	OS&H (Slip hazards)
4	Lack of Staff
5	Verbal conflict with guests[2]
6	Fraud (Extended credit)[3]
7	OS&H (Lifting)
8	Accidents (FP&E)
9	Vandalism and Theft[1]
10	Confronting trespassers
11	Burglary (Administration)
12	Armed Robbery (Administration)
13	Theft (Motor Vehicles)
14	Easily accessible FP&E
15	Syringes left in rooms

A number of considerations were raised and discussed by the participants during stage two. FP&E terminology was not known to the other participants. Housekeeping put *lack of staff* risk at the top of their individual list, but this was reduced to position four in the consensual ranking. Maintenance believed that *armed robbery (administration)* risk should be placed near the top of the consensual list but administration disagreed, resulting in a final ranked position at 12. All participants agreed that OS&H risks were considered high, resulting in OH&S risks occupying the top three consensual risks rankings.

Verbal conflict and abuse risk were rated highly by all participants, elevating this risk from the individual fifth placed ranking to a consensual fifth ranking. The participants agreed that security risks had a lower likelihood even through the initial risk assessment task was considered a security risk survey. Finally the participants had significant level of discussion on possible cost of loss and flow on costs with regards to risks with less tangible consequences.

RESULTS AND INTERPRETATIONS

Results from both the individual and consensual risk assessments were gathered, with results developed and presented from each stage. On completion of each stage, the risk assessments outcomes were compared and contrasted. Considering the risk rankings from both individual and consensual assessments the following outcomes were obtained. The top individually ranked risks remained within the top five consensual rankings (20%). But two of the second individually ranked risks were relocated within the bottom three consensual rankings (13%). Risk lack of staff was initially ranked fifth in an individual assessment, but remained at this position with the consensus ranking.

The consensual approach highlighted that each of the participants placed the risks that they identified higher than those of the other departments. The consensual activity generated a lot of discussion on the weaknesses and strengths of the facility; and this discussion allowed an increased and common understanding on aspects like site issues, experience and expectations. Common understanding could be further demonstrated by a number of risks being redefined during the consensus stage, with all participants agreement.

Maintenance initially put FP&E related risks at the top of their individual risk list, but this was quickly squashed by Administration to lower risks. Maintenance appeared to be particularly focused on maintenance issues, demonstrating a parochial approach to their individual assessments.

Administration demonstrated a holistic approach in the consensual risk stage on several occasions, considering that issues and needs of each area were addressed. This approach showed a holistic approach to the facility's risks, although three of their individual assessed risks were relocated to the bottom five consensual risks.

OS&H risks were considered by the participants to be of paramount importance, even through the original risk assessment task was began as a security survey. This redefined the risk assessment task, increasing the tasks breadth and reducing effectiveness. An issue that AS/NZS4360 clearly articulates when establishing the context of the risk management process (Standards Australia, 2004). It could be suggested that the facilitator should have provided and maintained clearer goals and boundaries during the assessment tasks, demonstrating the importance of *defining the context* stage.

Table 6
Comparison between individual and consensus rankings

Ranked Position	*Consensual Ranked Risks*	*Administration Ranked Risks*	*Housekeeping Ranked Risks*	*Maintenance Ranked Risks*
1	OS&H (Workplace)			1
2	OS&H (Fraudulent claims)	1		
3	OS&H (Slip hazards)		4	✓
4	Lack of Staff		1	
5	Verbal conflict with guests[2]	✓	5	
6	Fraud (Extended credit)[3]	4		
7	OS&H (Lifting)	✓	✓	3
8	Accidents (FPE)			2

9	Vandalism and Theft[1]	✓	✓	5
10	Confronting trespassers		3	
11	Burglary (Administration)	3		
12	Armed Robbery (Administration)	5		
13	Theft (Motor Vehicles)	2	✓	✓
14	Easily accessible FPE			4
15	Syringes left in rooms		2	

Notes:
1. *Vandalism* risk changed to *Vandalism and Theft* risk by consensus.
2. *Verbal abuse from guests* risk changed to *Verbal conflict with guests* by consensus.
3. *Fraud (Extended Credit)* defined as letting guests stay and accepting payment on vacation of rooms, also changing from daily to weekly payment is an issue.
4. ✓ = Risk identified individually, but not ranked.

All participants believed that the risks concerning OS&H were very important and were therefore ranked highly. This appeared to show that the wellbeing of the facility's employees, as well as fear of litigation, concerned the area managers greater than financial and security risks. The focus of OH&S was despite the fact that the facilitator set the scope of the activity as security based risks. It was agreed by all parties that security risks would have a higher consequence, but in most cases the likelihood was significantly lower in comparison to other types of risks.

The risk of *Armed Robbery (Administration)* was initially placed at the top of the list by the maintenance supervisor, with disagreement from the Administration manager. During the course of the activity the *Armed Robbery (Administration)* risk was slowly moved down the list as discussion and consensus took place.

Finally, 20% of the individually assessed risks remained in the top four consensual risk rankings. But 13% of the second placed individually assessments risks were relocated to the bottom three consensual risk rankings. With the majority of risk management processes, a line has to be drawn to consider which risks are mitigated and which are not. Where this line is drawn has many factors, based on financial, resource, technical, social, cultural and management considerations. But this statistic could suggest that if the top five consensus risks were considered for mitigation, only 20% of the individually assessed risks would have been mitigated. Therefore resources may have been wasted and valid risk excluded.

This study, in the context of this facility, demonstrated that individuals over or under emphasise risks, dependant on personal affect and parochial considerations. The study also illustrated that a consensual style of risk identification, analysis and evaluation is produces more holistic risk assessments then assessments conducted in isolation.

LIMITATIONS OF THE STUDY

The study presented a number of limitations, including the small sample size, sequential utilisation of the source data, limited quantitative analysis and the participant's consideration of risk outside the risk assessment context. Although the sample size was small, the study appeared to produce effective results from the analysis, but a larger study with control data would be more appropriate. The second stage source data utilised the first stage data. This approach could have skewed or biased the second stage data. A larger sample size would have allowed the use of separate data sources, without sequential utilisation between the individual and consensual stages.

The study applied limited quantitative analysis in both stages of the study. There was no reliability or validity measure during the study, reducing the robustness of the overall outcome. Finally the participants were allowed to drift outside the risk assessment context, demonstrated through their focus on OH&S risks. Although not necessarily a limitation, this would require better risk management context boundaries placed to ensure that future studies did not follow a similar drift.

CONCLUSION

Opinions of risk data can be unrealistic or over emphasised and this will skew the final outcomes of the assessment. For this reason the method of initial data collection is important to the overall process. An individual interview based approach to risk identification and analysis involves the stakeholders of the facility submitting their opinions in isolation. A consensual approach requires all major stakeholders to be present at the same time and to agree upon the identification and analysis of risks. The results from this research paper show that the approach of a consensus meeting is a more effective method of risk evaluation than individual. The individual interviews showed that a person who has a vested interest in an area of a business will overemphasise the risk to that area and mitigate the risks to other facets of the same organisation. The 3 individual risk assessments completed with the supervisor's assistance show differing results each emphasising their own area. The consensus method shows a much more rounded result with the Identification and Analysis of risks more accurately defined and the most important risks given the highest ratings.

REFERENCES

Brooks, D. J. (2005). Is CCTV a social benefit? A psychometric study of perceived social risk. *Security Journal*, *18*(2), 19-29.

Comfort Inn and Suites. (2000). *West Beach Lagoon Induction Package*. Scarborough, Western Australia: Unpublished.

Fischer, R. J. & Green, G. (2004). *Introduction to security*. (7th ed.). Boston: Butterworth Heinemann.

Jay, C. (2005). Big debacles help shape a new science. *The Australian Financial Review*, p. 2.

Jones, D. E. L. & Smith, C. L. (2005). *The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management*. 2005 Recent Advances in Counter-Terrorism and Technology Summit, Canberra: Australian Homeland Security Research Centre.

Koller, G. (1999). *Risk assessment and decision making in business and industry: A practical guide*. Boca Ratan: CRC Press.

Koller, G. (2000). *Risk modeling for determining value and decision making*. Boca Raton: Chapman and Hall/CRC.

Standards Australia. (2004). *AS/NZS4360:2004 Risk management*. Sydney: Standards Australia International Ltd.

Standards Australia. (2004). *HB436:2994 risk management guidelines: Companion to AS/NZS4360:2004*. Sydney: Standards Australia International Ltd.

Western Australian Police Service. (2004). *Crime statistics search: Scarborough September 2004 to August 2005*. Perth, WA: Western Australian Police Service.

Western Australian Police Service. (2004). *Monthly reported crime statistics: 2004/05 north metropolitan region*. Perth, WA: Western Australian Police Service.

COPYRIGHT

Ben Beard and David J Brooks ©2006. The authors assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for the personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites one the World Wide Web. Any other usage is prohibited without the express permission of the author