Session No. 662

Using ANSI/ASSE Z690.2-2011 [ISO31000] to Assess the Maturity and Adequacy of your Risk Management System

J.F. (Jim) Whiting, MSc., Dip.Ed., CPEng, SMIE(Aust)
Managing Director, Principal Risk Engineer
risk@workplaces pty ltd
Brisbane, Australia

Introduction

The new risk management standard ANSI/ASSE Z690.2 [identical to ISO 31000] now allows an organization of any size and business activity to assess the maturity and adequacy of its risk management system (RMS). Many organizations currently have at least informal management practices and processes which include the fundamental components of risk management as detailed in Z690.2. However, confidence and assurance that those practices and processes are adequate, mature, and effective is often lacking. Even if an organization has not already adopted a formal risk management process for particular types of risk or business circumstances, it can and should decide to carry out a regular critical review of its existing RM practices and processes in the light of the new standard's requirements.

This paper details how assessment tools are constructed and used to review/assess/even audit how well the organization conforms/complies with the standard and hence provides a measure of maturity and adequacy of the organization's own system. The process is best called a **Conformity Assessment.**

Part 1 The Z690.2 Standard and Its Application

With the adoption of the ISO 31000:2009 RM Standard, the ANSI / ASSE Z690.2 : 2011 standard is identical to it. They are *"Principles and Guidelines"* Standards rather than "*Specification*" Standards. As such they were not intended to be used for formal external assessment for *"Certification"* purpose,s as many organizations do with ISO 9001 [Quality] and ISO14001 [Environment]. Nevertheless the RM Standard does provide an excellent basis for construction of a maturity assessment tool described.

"Specification" standards such as ISO 9001 and ISO 14001 use terminology such as *"shall"* to specify conformance requirements, whereas Z690.2 - uses terminology such as *"should"*. In that way the RM standard does still detail what an adequate and mature RM system should be. For example, the standard states in *Clause 3(b) Principles* that:- ***"****an organization* ***should*** *at all levels comply with the principle that Risk Management as an Integral Part of all Organizational Processes."*

Consequently the assessment tool includes questions requiring the organization to provide information/evidence that risk management is not a stand-alone activity separate from the main activities and processes of the organization. To demonstrate conformance, the organization needs

to answer the questions: how risk management is part of the responsibilities of each level of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

The practical conformity assessment tool described in the paper consists of 3 sets of comprehensive evidence-seeking questions designed for each detailed expectation of the standard, viz *Principles*, *Framework*, and *Proces*s. It can be used internally or externally as a first or second or even third party audit tool. It can be tailored to any activity and risk domain.

Although a first party conformity review/assessment/audit can often be subjective in nature, the tool used rigorously can yield rating measures of maturity and adequacy that do help improve objectivity and precision in evaluating the current status of a system.

If performed diligently, first party audits and self-assessments can provide:

- feedback to everyone in the organization that will allow them to have confidence and assurance that the RM system is both being implemented and achieving effectiveness, and;
- a measure of the organization's evolutionary continuous improvement effort to assess the return on investment for sustaining that effort.

The standard and the conformity assessment tool described in this paper can be applied throughout the life of an organization or a project, and to a wide range of activities, including strategies, decision-making, operations, processes, functions, projects, products, services and assets. As a benchmark measurement at any given time, they provide an effective means of following change management and continuous improvement. They can be used by any public, private or community enterprise, association, group or individual. Therefore, this standard is not specific to any industry or sector. As well, this standard and conformity assessment tool can be applied to any type of risk domain, whatever its nature, whether considering positive or negative consequences.

The standard covers each of the 3 main components [and the relationships between them] of a comprehensive, mature risk management system. As shown in **Exhibit 1A** they are:-

- the **principles** for managing risk, { 22 questions }
- the **framework** in which it occurs { 79 questions }
- the risk management **process** { 164 questions }

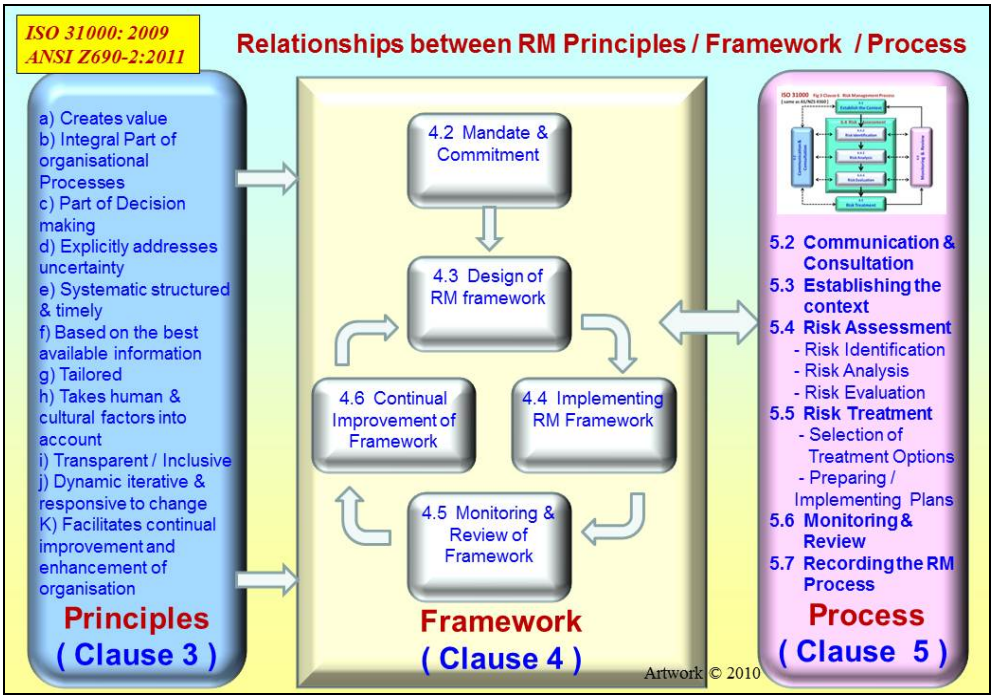


Exhibit 1A RM Standard – adapted from Fig 1 - ISO 31000 – ANSI Z690.2

The Process of risk management is detailed in Clause 5 Fig 3 of the Standard and is shown graphically in **Exhibit 1B.**

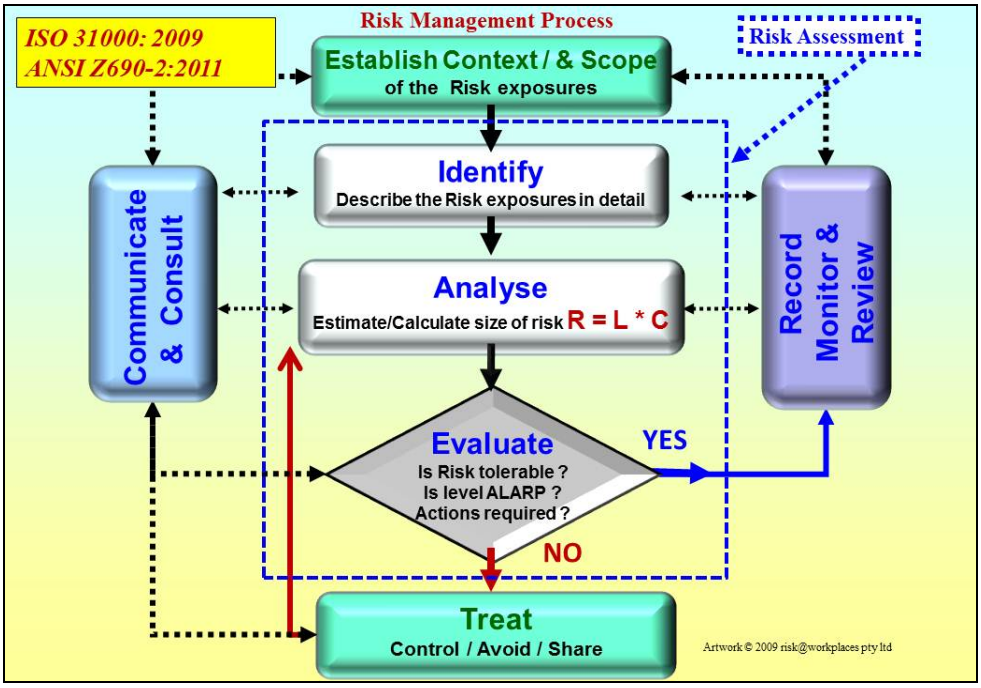


Exhibit 1B RM Process – adapted from Clause 5 : Fig 3 - ISO 31000 – ANSI Z690.2

Part 2 Risk Management "Maturity" and "Adequacy"

What is risk maturity ? The Institute of Internal Auditors IIA defines risk maturity as:

"The extent to which a robust risk management approach has been developed and applied, as planned, by management across that organization to identify, assess, decide on response to and report on opportunities and threats that affect the achievement of the organization's objectives." Note the emphasis on positive opportunities as well as the traditional focus of RM on negative consequences or "threats."

What is "adequacy"? Is the organization's RM system capable, suitable, appropriate, sufficient, ample, and competent to allow the organization to meet the definition above? It is worth remembering that each organization can have unique risks associated business objectives and risk criteria. Hence measures of maturity and adequacy need to take that uniqueness into account. There is no "one size fits all." Maturity assessments can be absolute within an organization's own individual character and relative with respect to other organizations similar in size, business activity, industry, locality etc.

How can the risk maturity of an organization be assessed? Even though the concept of risk maturity is not new, the working concept used in this paper is that a maturation process is a growing , developing, evolving process towards an achievable sustainable level of management of risks required by an organization's needs and objectives. The maturation process will need to follow phases of development from *Intentions* to *Maintenance* as in **Exhibit 2** :-

Exhibit 2 Evolutionary Stages in the Maturation Process

Maturation as a change process is rarely revolutionary; rather it is mostly evolutionary in character. Quick, large changes are usually unachievable and often not desirable. Degrees of maturity can be assessed by examining how well the maturation process has progressed through these phases by reference to a number of indicative attributes. For a "broad brush" preliminary review of RM maturity, 5 levels for degrees of maturity are usually chosen. The 5 levels and their commonly used verbal descriptors are shown in **Exhibit 3 and Table 1.** The 6 indicative attributes chosen in this paper for reference to assess how far the organization has matured at a given time of assessment are shown in **Table 2.** A version with guidelines for each Level and Attribute is given in **Appendix 1.**

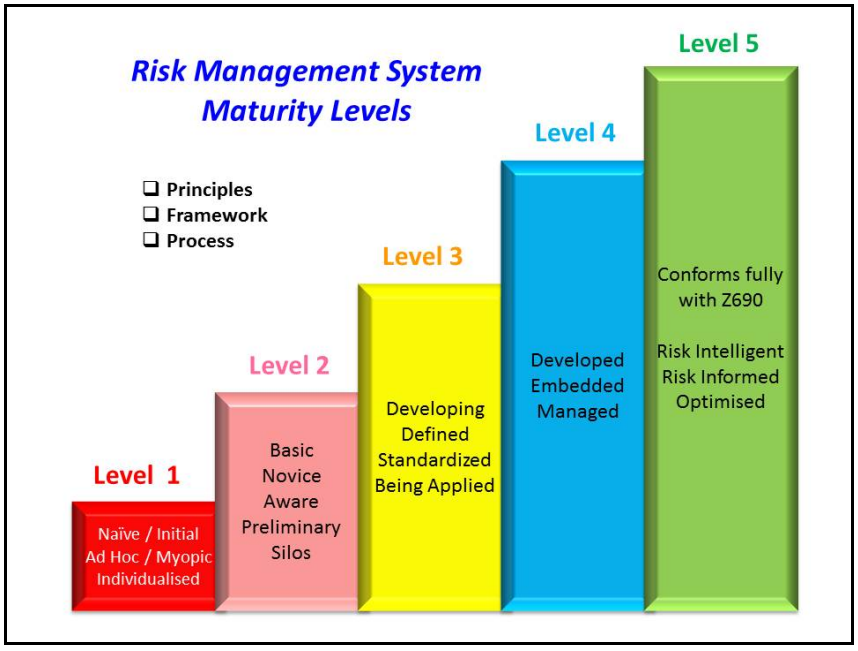


Exhibit 3 A 5 level maturity scale with commonly-used descriptors

The 6 indicative attributes chosen in this broad-brush assessment tool are:-

- **Management Commitment & Resourcing**
- **Risk Management Processes**
- **Knowledge & Skills** & **Experience**
- **Positive Risk Culture**
- **Behaviours & Applications**
- **Responsibilities and Accountabilities**

Using the achievement guidelines for each of the Attributes in **Table 2**, an assessor can give a "broad-brush" estimate of a maturity level achieved. No one of any of the maturity levels for each of the 6 attributes is given more weight than any other. The usual conservative approach is to record each of the 6 levels and also an aggregate level of maturity based on the lowest of the 6 assessments.

5 Maturity Levels	
#	**Verbal Descriptors commonly used**
5	• Conforms fully with ISO31000 • Risk Intelligent • Optimized

	• Risk Informed
4	• Developed • Embedded • Managed
3	• Developing • Defined • Standardized • Being Applied
2	• Basic / Novice • Aware • Preliminary • Silos
1	• Naïve / Initial • Ad Hoc • Myopic • Individualized • Non-existent

Table 1 A 5 level maturity scale with commonly-used descriptors.

6 Indicative Attributes to Evaluate Maturity
Management Commitment & Resourcing
Risk Management processes
Knowledge & Skills & Experience
Positive Risk Culture
Behaviours & Applications
Responsibilities & Accountabilities

Table 2 A Maturity Review Tool using 5 Levels & 6 Attributes
[details for each level of each attribute are given in Appendix 1.]

The results from applying the tool of **Tables 1, 2,** and **Appendix 1** for 2 different assessments for the same organization to show one year's progress are represented in **Exhibits 4 (A) and (B)**.

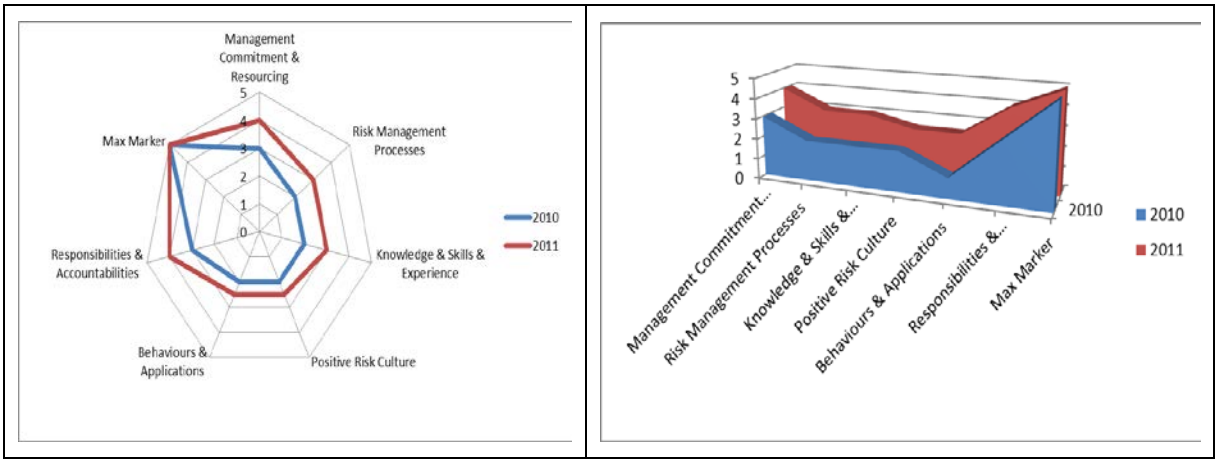


Exhibit 4 (A) (B) **Using the Broad 6 Attribute method - Sample Results**

Part 3 Conformity with Z690.2 as a measure of maturity

In contrast to the common "broad brush" approach of Part 2, this paper describes how Z690.2 Principles and Guidelines represent a more extensive, detailed, thorough set of attributes - way beyond the 6 attributes of the broad brush approach of Part 3. With each one of its "should" statements, Z690.2 provides a basis for framing Questions / Criteria to assess Conformance more objectively and completely and hence with more confidence and assurance.

The Z690.2 based Conformity Assessment Tool that has been developed consists of a series of questions related to each requirement of the Standard. **Table 3** shows a few examples of the 164 questions to be asked by the assessor for each of the requirements of Process of a RM System - Clause 5 of the Standard**.**

Conformity Assessment using ANSI Z690.2 criteria

Clause 3 - Principles	**{ 22 questions }**
Clause 4 - Framework	**{ 79 questions }**
Clause 5 - Process	**{ 164 questions }**

5.5.3 Preparing & Implementing Risk Treatment Plans.	None 0	Very Little 1	Some 2	Good 3	Complete 4
a) How well are risk treatment plans being prepared and implemented ?					
b) What is the level of detail in the plans on how the chosen treatment options will be implemented ?					
c) To what extent, does the information provided in treatment plans include the reasons for selection of treatment options, including expected benefits?					
Sample of 164 Questions for Clause 5					

Table 3 **Examples of Questions in the Assessment Tool based on ISO31000**

According to the information obtained / provided in responses to each Question in the Conformity Assessment Tool, a rating of 0 → 4 is allocated according to evolutionary levels of **Intent** / **Planning / Application Progress / Achievement / Sustainability** as described in **Table 4**.

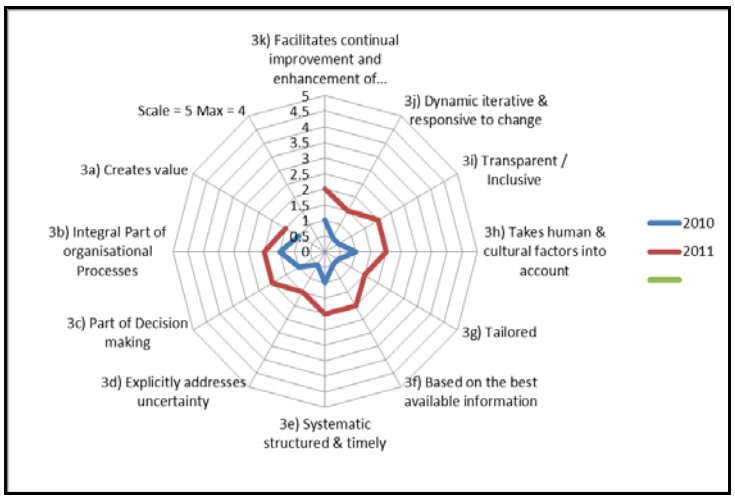
Degrees of Conformity for each Assessment Question		
#	Descriptor	Criteria / Guidelines
4	Complete	Complete Sustainable Achievement of conformance Is consistently effective & professional with confirmation by formal monitoring
3	Good	Good intent / planning / achievement to conform AND significant but incomplete progress / achievement
2	Some	Some but limited intent / planning / achievement to conform AND some progress / achievement
1	Very Little	Very little intent and immature planning to conform with requirements AND little progress / achievement
0	None	No intent / planning and achievement of conformance with requirements beyond some Ad Hoc / individual heroics

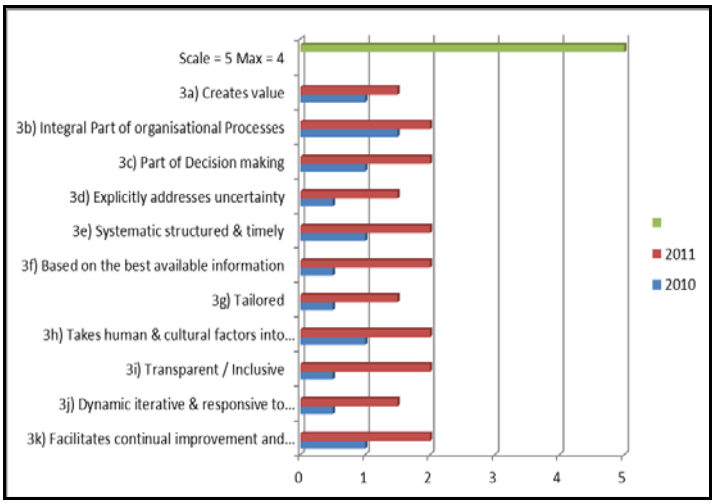
Table 4 Criteria for assessing degrees of conformity for each requirement of Z690.2

The questions provided in the Z690.2 Conformity Assessment Tool are constructed carefully to be as "open" and revealing as possible.

The onus on answering the questions, to provide information / evidence to the assessor to make each estimate of level of conformity 0 → 4, lies squarely on the organization and its relevant personnel. Whether the assessor is internal or external, is not relevant to the nature and conduct of the information gathering process. The context of the conformity assessment needs to be positive with the organization recognizing that it has the opportunity to demonstrate its progress and maturity for internal and external communication purposes. The tone of any conformity assessment has to be a positive revelation of progress and gap analysis for continuous improvement rather than any negative punitive outcome for individuals whose responsibilities and accountabilities were not clear and agreed.

Exhibit 5 (A) (B) and (C) show sample results indicating 1 year's progress towards maturity achieved by 1 organization. As such it provides a useful indicator of continuous improvement and even an appropriate addition to KPI measurements for associated personnel. Similar Charts exist for Clause 4 Framework and Clause 5 Process.





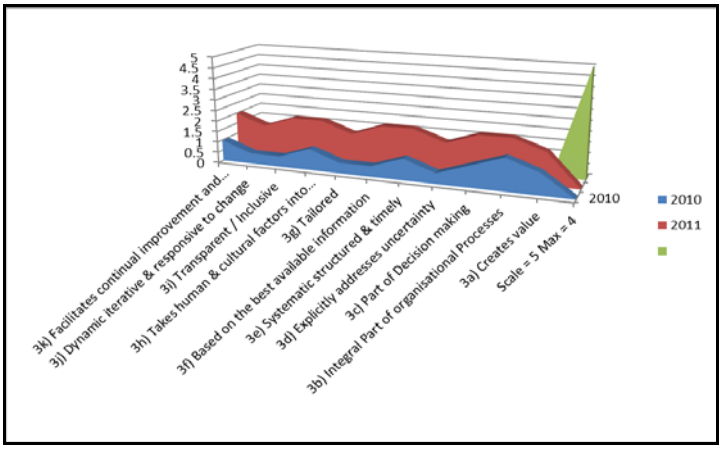
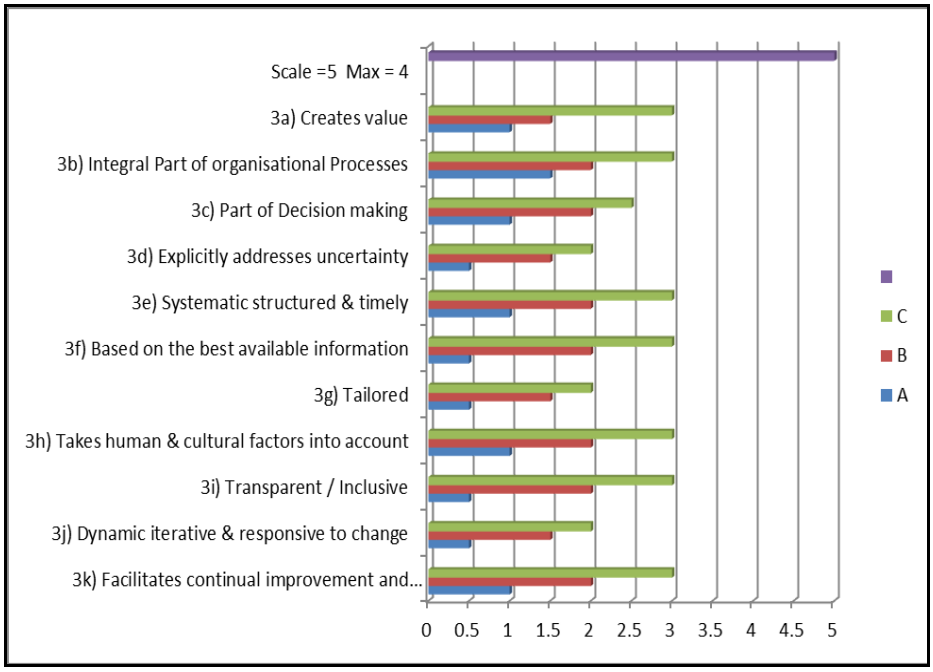
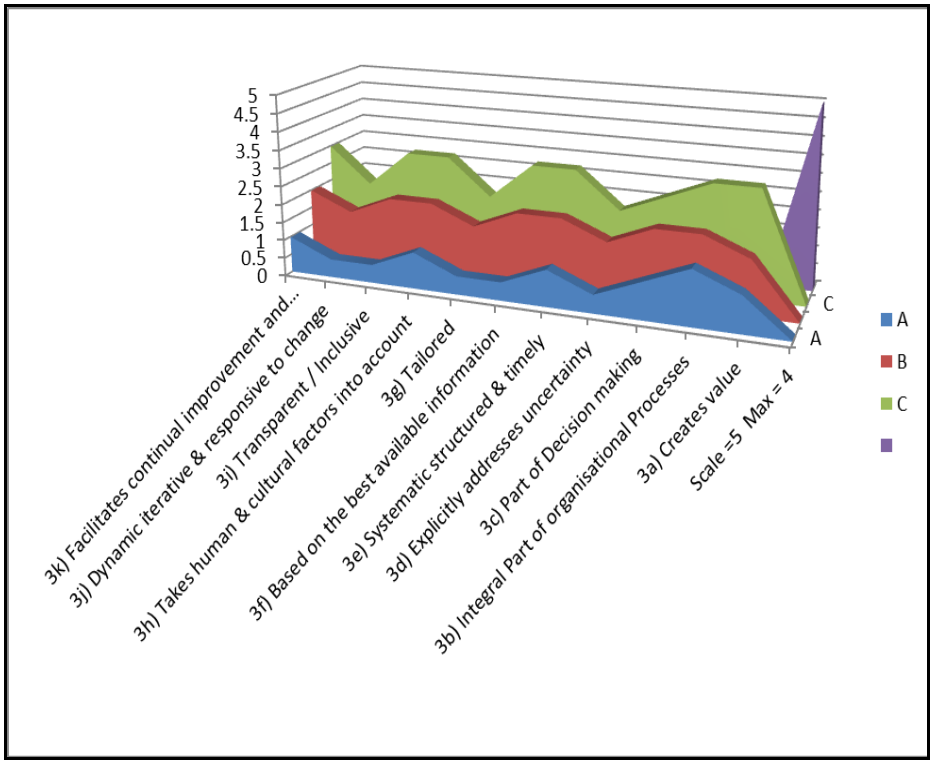


Exhibit 5 (A) (B) and (C) Using the Z690.2 Method - Sample Formats of Results

A comparison between 3 organizations' results using the Z690.2 Method is shown in **Exhibits 6 (A) and(B).** The comparative results shown are for Clause 3 "Principles" only. Similar Charts exist for Clause 4 "Framework" and Clause 5 "Process".





Exhibits 6(A) and (B) Using the Z690.2 Method – Clause 3 Principles
Comparative Results for 3 Organizations A, B and C

Part 4 Information / Evidence Gathering

Gathering / providing the information required to answer the Assessment's Tool's questions is essentially no different to that involved in any other kind of review / audit / assessment.

Information / Observation / Interpretation / "Evidence" has to be gathered by, or provided to, the assessor by finding answers to 265 attribute questions of Z690.2 as the assessment framework. The bases [evidence] to support confidence and assurance needs to be sufficient in scope and weight to support any conclusions regarding the degree of conformance [0 → 4] as in **Table 4.**

The information must be – as far as practicable - :-

- ❑ relevant;
- ❑ reliable;
- ❑ understandable;
- ❑ free from material misstatement;
- ❑ neutral/free from bias;
- ❑ such that another person would reasonably come to the same conclusion.

Not all "evidence" has the same weight in obtaining confidence and assurance. Evidence needs to be weighted according to its :-

- **independence** – affects reliability requiring detailed knowledge of the sources
- **relevance** – to more significant risks is of greater relevance to the overall assurance;

Types of Information Gathering Sources are usually classified as :-

- ❑ Documentary – Desk-Top
- ❑ Field Sampling

Formats include :-

- ❑ Interviews –individuals / workshops;
- ❑ Observations of meetings, office and field based processes and activities;
- ❑ Review of documentation and records;
- ❑ Surveys / Questionnaires.

Information – often qualitative - but nevertheless extremely useful can be obtained from direct actual observation [looking over the shoulders] of the operations and activities, interviewing management, staff and internal / external stakeholders.

Methods include :-

- **Reviewing Records –** files, Risk Assessments and Reviews, logbooks, incident reviews etc. These are indicators of whether the policies and procedures are actually happening as they should AND examining the operational RM culture.
- **Interviews with Stakeholders** – used to gauge feelings and attitudes and explore the experiences of individuals.

One to one interviews can be :-

- **structured**, uses a pre-set list of questions in a standardised way, or
- **unstructured,** uses a list of topics to explore and conduct a fairly free flowing interview
- following up issues as they emerge from the discussion and
- **semi-structured** uses set questions – allowance for discussion & following up on issues

Surveys / Questionnaires need to be well structured, easy to understand and quick to complete. A decision has to be made about how "open" or "closed" the questions and possible answers need to be and also how the data will be analysed. The more closed a question is – the quicker and easier it is to analyse the results, but the less certain you are that the questions and range of answers offered to choose from actually represent what the person really knows or thinks. All surveys should include scope for "Any Other Comments / Information" feedback. One example of a broad survey questionnaire is in **Appendix 4.**

Part 5 Conclusion

While ANSI/ASSE Z690.2 [Risk Management System RMS] was not intended as an auditable Specification Standard such as ISO 9001 [Quality Management System QMS] and/or ISO 14001 [Environment Management System EMS], assessing conformity with its "best practice" requirements does provide confidence and assurance in measuring the maturity and adequacy of the organization's RM System.

The tools described here can be used to perform that Conformity Assessment.

Part 6 Bibliography

AIRMIC / ALARM / IRM, *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*
http://www.theirm.org/ISO31000guide.htm

ANSI/ASSE Z690.**1**-2011 *Vocabulary for Risk Management*
[identical to ISO Guide 73 :2009]

ANSI/ASSE Z690.**2-** 2011 *Risk Management – Principles and Guidelines on Implementation*
[identical to ISO 31000, 2009]
http://www.asse.org/shoponline/products/EZ690-PKG.php

ANSI/ASSE Z690.**3**-2011 *Risk Assessment Techniques*
[identical to ISO 31010, 2009]

CobiT *(Control Objectives for Information and Related Technology), IT Governance Institute, 1996-2007*
http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Comcover, *Risk Management Better Practice Guide*
Department of Finance and Deregulation, Canberra, June 2008
http://www.finance.gov.au/comcover/docs/Better_Practice_Guide.pdf

Comcover, *Risk Management Benchmarking Survey 2010*
Department of Finance and Deregulation, Canberra, 2010aturity Levels
http://www.finance.gov.au/comcover/docs/Comcover-Risk-Management-Benchmarking-2010-Maturity-Statements.pdf

COSO, (2004) – *Committee of Sponsoring Organizations of the Treadway Commission*
Enterprise Risk Management ERM — Integrated Framework – Executive Summary
http://www.coso.org/documents/coso_erm_executivesummary.pdf

Demby, Glenn *What's the Difference Between an OSHA Rule and an ANSI Standard?*
http://www.lomont.com/documents/Dembystandardsarticle3-21-2006.pdf

Griffiths, David *(2006) Risk Based Internal Auditing – Three views on implementation ;*
www.internalaudit.biz

Hall, Elaine M. *(1999) Risk Management Return on Investment – Measure of Success of Risk Management Level 6 Software, 530 Franklyn Avenue, Indialantic, FL 32903*
http://www.theirm.org/events/documents/RiskManagementReturnonInvestment.pdf

Hillson, David A, *(1997) Towards a Risk Maturity Model*
The Intnl Journal of Project & Business Risk Management Vol1 No 1 Spring 1007 Pp 35-45
http://www.risk-doctor.com/pdf-files/rmm-mar97.pdf

HM Treasury, *The Orange Book, Management of Risk – Principles and Concepts, United Kingdom, October 2004.*
http://www.hm-treasury.gov.uk/d/orange_book.pdf

Institute of Risk Management *IRM Guidance Paper Risk Appetite & Tolerance*
http://www.theirm.org/publications/documents/IRMRiskAppetiteFullweb.pdf
International Organization for Standardization, International Standard, Risk Management – Principles and Guidelines on Implementation, ISO 31000, 2009.

ISO *What is conformity assessment?*
http://www.iso.org/iso/casco_2005.pdf and
http://www.iso.org/iso/resources/conformity_assessment/what_is_conformity_assessment.htm

Standards Australia, *Delivering assurance based on AS / ISO 31000:2009 Risk management— Principles and guidelines- HB 158—2010*
http://infostore.saiglobal.com/store/Details.aspx?productid=1396045

CobiT *(Control Objectives for Information and Related Technology), IT Governance Institute, 1996-2007*
http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

RIMS – *Risk Maturity Model*
http://www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx

Software Engineering Institute, Carnegie Mellon University
http://www.sei.cmu.edu

Appendix 1 Details of Table 2 with 5 Levels / 6 Attributes

Maturity Levels		Description of 5 levels of Maturity with 2 of 6 Indicative Attributes	
#	Verbal Descriptors commonly used	Management Commitment & Resourcing	Risk Management Processes
5	• Conforms fully with ISO31000 • Risk Intelligent • Optimized • Risk Informed	• Top down leadership • RM scope fully extended from reactive management of negative consequences to proactive seeking out positive but fully managed risk taking. • KPIs at all levels include RM performance. • RM related committees of Board fully functional visible and responsive.	• RM processes are sophisticated, robust. • Risks are always taken on an informed basis. • RM processes are fundamental to how the organisation is managed. • RM processes and internal control are totally embedded into the business at board, corporate and unit levels. • RM is fully integrated into all risk classes / domains. • Risk Registers / Profiles will be complete and dynamic.
4	• Developed • Embedded • Managed	• Risk tolerability and criteria are clear / completely understood and respected. • ERM focus. Enterprise wide approach to risk management developed and communicated. Includes all risk domains not just Finance and Insurance. • Policies conform with mature Principles	• RM processes broadly developed, measured and controlled. • RM strategies / processes are adopted by all parts of the organization and are integrated into all risk classes. • There are clear metrics to demonstrate ROI return on investment. • Commonality of risk assessment / treatment processes is developed.
3	• Developing • Defined • Standardized • Being Applied	• Risk criteria, attitudes, appetite defined but not yet fully understood and incorporated into decision making. • Common elements of RM are recognized across risk domains including Reputation and Brand. • Meaningful RM roles for Board Committees – Governance / Audit / RM	• RM strategies / processes formalized, and in place as well as widely communicated across the organization. • Top Down Drivers • RM strategy is communicated and accepted across the organization, with clear objectives in line with business strategy. • Quality of RM processes may vary across the organization. • Commonality of RM processes across is developing.
2	• Basic / Novice • Aware • Preliminary • Silos	• RM Policies and Criteria initialised and aware but not believed or used widely and at all levels.	• Uncoordinated silo-based approach to risk management. RM Strategies / Processes are not clearly linked with business strategies. • RM processes highly reactive. • Undisciplined and non-rigorous RM processes. • Absence of a formal RM framework. • Risk Registers will be incomplete or almost non-existent

1	• Naïve / Initial • Ad Hoc • Myopic • Individualized • Non-existent	• No formal co-ordinated setting of an enterprise risk management strategy. • Strong need for leadership to promote the establishment of a RM framework. • Relevant Committees of the Board need to initiate an urgent action plan for RM establishment process. • Board and management close to unaware of the value of positive risk management.	• Any RM Process highly dependent on individual competency and efforts. • Any RM Processes are unpredictable, reactive and uncontrolled. • Need for a developed approach for RM & Benefits not yet recognised • Management controls and decision-making not even recognized as informal risk management. • RM processes ad hoc or even chaotic

Appendix 1 [cont'd] Description of 5 levels of Maturity with 4 of 6 Indicative Attributes

#	Knowledge & Skills & Experience	Positive Risk Culture	Behaviours & Applications	Responsibilities & Accountabilities
5	• Everyone knows that they are fully competent to fulfil their RM responsibilities • RM and Change Management are recognized as inter-dependent.	• Self-driven/ Generational • even Evangelical • RM is the way we do business. • Risk language is universal management language. • Focus is fully on the Continuous Improvement of the RM Process.	• Decision making is always based on informed risk assessment • Risk Analysis is as fully quantitative as required. • RM is used as an essential management process. • Mature sophisticated application of ALARP	• All levels of management see RM as the means of providing self-assurance that responsibilities are being fulfilled.
4	• Everyone knows that they are close to full competency in being able to fulfil their RM responsibilities]	• Active proud engagement • Bottom-up as well as Top-down drivers • Innovative confident risk taking • Mostly alignment of everyone's risk perceptions.	• ERM Enterprise wide risk management approach considers risk at highest level but could be further embedded better in lower level decision making	• Risk Ownership fully developed, positive defined and agreed. • The risk makers and the risk takers are the risk managers.
3	• Competence developing widely but not everyone knows if their competence does or does not match their RM responsibilities.	• Still some passive acceptance • Developing understanding of risk tolerability and appetite	• Most decision making involves RM and positive outcome risks are regarded as opportunities. • Projects are conducted according to organization's RM standards.	• Risk Ownership and Risk Registers are developing. • Most managers have compiled Risk Registers
2	• Those who lack RM competence know it but mechanisms for gaining competency unavailable Or inadequate	• Less Sceptical but no real buy-in. • Reliance on form filling	• RM strongly focused exclusively on finance risks and insurance. • HS&E management is not seen nor managed as risk management. • Compliance Focus	• Risk defined and managed differently in separate silos. • Only some managers will have defined their risks.

1	• Most do not even know what RM competencies are required. • Some RM competent people but essentially individual heroics with non-uniform processes.	• Sceptical close to Cynical • Very Risk Ignorant and hence Very Risk Averse • Individuals attempting to introduce formality in risk management • Blame – unfair accounatbility	• Focus is – "down-side" risk only negative consequences • Iindividual "heroes" advocating Change. • Very little or no RM documentation.	• Managers are not being held to account because there are no definitions of RM responsibilities

Appendix 2 Information Gathering

Sources of Conformity Information

A) **Documentary Records / Agenda / Minutes / Follow-Up Reports** of **Meetings / Workshops such as :-**

- ❑ Board Meetings
- ❑ Annual Reports
- ❑ Senior management meetings incl Reviews of Unclosed Actions
- ❑ Insurance Audits
- ❑ Policies and procedures
- ❑ Statement of aims and objectives
- ❑ Staffing structures and deployment of staff
- ❑ Performance indicators or other monitoring statistics or information
- ❑ Results/reports on resident satisfaction surveys
- ❑ Position Descriptions / Performance Measures / KPIs
- ❑ Policy meetings
- ❑ Project Management meetings at all stages of a project Lifecycle
  - *design*
  - *construction*
  - *commissioning*
  - *decommissioning*
  - *disposal*
- ❑ Planning / Scheduling meetings
- ❑ Reviews
- ❑ Incident Investigation Reports – Reviews - Follow-Ups
- ❑ Risk Registers
- ❑ Risk Reviews / Assessments
- ❑ Work Method Developments / Reviews

B) SEARCH Words for each of the "soft" documents

Change / normal / abnormal / new
Risk Exposure
Investment
Risk assessment
Risk levels / scores
Risk Appetite
Accept / Acceptance / Acceptability
Tolerate / Tolerance / Tolerability
Cost benefit analysis

Averse / Tolerant
Priority
Options / Choices
Probability
Impact
Mitigation
Potential
Decision Criteria

Appendix 3 Types of Information / Evidence

- **Direct**
- **Real Documentary**
- **Real Material**
- **Expert**
- **Circumstantial**
- **Hearsay**

- **Direct**
  Evidence of something that has been directly perceived by an observer / witness through one or more of his or her five senses—for example, has been seen, heard, smelled, felt or tasted when physically observing / sampling activities and operations.
  Direct evidence can be obtained by oral interviews and written statements in the field and/or controlled environments. Often strongly influenced by memory of the interviewees.

- **Real Documentary**
  There are two types of documentary evidence available to a conformity assessor:
  - **Primary** documentary evidence is the production of the original document itself.
  - **Secondary** documentary evidence is the production of a copy of the original document—for example, photocopy or certified copy, etc.

- **Real Material**
  Material objects, other than documents, can provide or demonstrate the strengths or weaknesses of a RM System's processes and procedures. They are often the consequences of successes or failures of the RM System. They usually require less interpretation, inference and individual biases.

- **Expert**
  Information Evidence of someone's opinion can be helpful but only if the opinion expressed is in his/her field of expertise. The assessor needs to be convinced that the expert is qualified in the risk dimension being assessed.

- **Circumstantial**
  Usually a collection various items of Information / evidence from which – collectively - a fact may be inferred as a natural or probable conclusion. It is usually made up of a series of facts that collectively indicate the same causal links or conclusion.

- **Hearsay [second hand]**

This is Information which is given by interviewees who do not have direct knowledge of the facts being offered but has been told about them by some other persons. The assessor would normally discount such information unless supported other ways.

Appendix 4 Macro "Risk Maturity / Health" Questionnaire

[often used before applying the Z690.2 conformity assessment tool]

Participant's Information ***(- names are not required)***

A) What is your reporting level in the organisation? Level _____
(For example, if you report to a manager who reports directly to the Board, record number 2)
B) How long have you worked in this organisation? _____ Years
C) What is your age? *(- names are not required)* _____ Years
D) Please indicate your gender by circling FEMALE MALE

Please answer EVERY question by indicating the degree to which you agree or disagree with each statement by placing a "y" in ONLY 1 corresponding box.
Answer as you believe or you can best assess.

	Questionnaire Items: ***(Do you agree / disagree?*** ***Answer as you believe or can best assess)***	**Definitely NO Strongly Disagree**	**Mostly Disagree**	**Mostly Agree**	**Definitely YES Strongly Agree**
1	This organisation spends too much time on **REACTIVE problem / incident management** more than on effective PROACTIVE risk management.				
2	**Key operational risks** are considered fully to obtain a clear understanding of the nature and extent of risk across all the organisation's activities.				
3	Risk Management is seen by the organization **as positive real innovation and exploiting opportunities** not just focussing on negative effects on objectives.				
4	Managers have a good understanding of the **level of awareness of staff** towards defined controlled tolerable risk taking				
5	By means of detailed records of risk information, **Risk Registers**, managers have a good understanding of the **overall risk** faced by the organisation across all our activities..				
6	The **organisational structure** supports the management and communication of risk.				
7	**Sufficient time and resources** are allocated by the board, senior management and the organisation for adequate **internal control** and risk management issues.				
8	Levels of risk **responsibilities, authorities with accountabilities** are clearly specified with regard to **tolerable** levels of risk taking.				
9	The key business, operational and financial risks facing the company are identified in **a timely manner** and the **likelihood** of the risks materialising and the **potential consequences or impacts** on the business are fully considered				
10	Risks at all levels across the organisation are managed with a **consistent and systematic approach**, from the formulation of				

	strategy into programs, projects and the operational environment,				

Questionnaire Items: ***(Do you agree / disagree? Answer as you believe or can best assess)***		**Definitely NO Strongly Disagree**	**Mostly Disagree**	**Mostly Agree**	**Definitely YES Strongly Agree**
11	**Risk Reports** are on the agenda of senior management meetings as a matter of course.				
12	**Historical information / data** show past performances of ours and similar organisations and are used effectively as learnings to **continually improve** the way we will assess and manage risk in the future.				
13	Appropriate **standards of behaviour** and awareness related to the importance of **internal control** are communicated by/to all managers and employees, e.g. through the formalised codes of ethical conduct, policies, procedures, standards of discipline, and performance appraisals relating to risk.				
14	The organisation is committed to providing the required Risk Management **skills and training** to ensure that all our staff are competent to manage risks.				
15	Information relating to risk is **communicated effectively** to all who are involved and exposed - *the risk makers and takers.*				
16	Measuring the ability to manage risk effectively is used as a contributor to rating **performance of staff** and external service providers.				
17	How effectively risk is being managed throughout our **suppliers' / contractors'** systems is being monitored well.				
18	**Contracts and negotiations** with suppliers demonstrate a real and accurate understanding of risk.				
19	**Decision making** is always based on - at least – informal qualitative risk assessments.				
20	Everyone recognises that risk is always created by **CHANGE** of any kind and hence there is recognition that Change Management and Risk Management Policies go hand-in-hand				

Completed!! Thanks for your cooperation and Participation

NB: Return this form IMMEDIATELY on completion to: - ……..

Any Questions / Comments to The Survey Coordinator:

_____

_____

_____

_____

_____