Annex A – ISO 31000 Clauses

IL7 will endeavour to ensure that it performs risk assessment assignments aimed at establishing an information security management system, for the organisation or project that provides the basis for meeting the ISO 31001 principles set out below. If IL7 are assessing a single system, its assessment will be compatible with, accommodate and interact with, and promote in the organisation's system these principles.

ISO 31000 clauses:

a) Risk Management creates and protects value.
   If the customer is adopting a new system of risk management, perhaps to replace IS1/2 it must be an integral part of the business, accepted by the Board. It shouldn't be one off for a single project or system but a methodology that is sustainable, consistent and comprehensible throughout the organisation and consistently applied.

b) Risk Management is an integral part of all organisational processes.
   The risk management system should take account of all the businesses drivers and feed into and feed from them as an integral component. It should be structured in such a way as to enable the organisation to take new opportunities, enhance value and mitigate business threats in a controlled manner.

c) Risk Management is part of decision making.
   The risk management system should be utilised in making decisions, enabling informed choices to be made about both 'upside' and 'downside' risks. Opportunities may present themselves for development or expansion of business (or cost saving). If upside risks are not taken the consequences may be worse. A practical risk assessment and management system should allow opportunities to be explored and exploited.

d) Risk Management explicitly addresses uncertainty.
   The customer should be advised to have an arsenal of tools, techniques and measures to treat risks or a systematic process for selecting and applying controls. These activities are described as 'risk treatment' in the ISO Guide 73 as the "process to modify risk".

e) Risk management is systematic, structured and timely.
   The customers system must be consistent and provide an efficient use of resources – avoiding repetitious independent systems and multiple audits.

f) Risk management is based on the best available information.
   The consultants input to the system must be accurate based on evidence expertly gathered from stakeholders. It should reflect the business context and be relevant to both threats and opportunities. Where evidence relates to cyber investigation, threat modelling it should be presented without 'fear, uncertainty or doubt' premises, and be based on proven and extant and applicable vulnerabilities. It must be clear, concise, accurate and pertinent.

g) Risk management is tailored.
   The customer's risk management system must be proportionate and scaled to the business needs and to the business environment it operates in. This would include the need for compliance if applicable.

h) Risk management takes human and cultural factors into account.
   The gathering of evidence, identification of risks and putting threats into context must include human factors such as capabilities, perception and threat IQ. It must include measures such as awareness; training and communication to ensure factors do not work against or hinder the treatment of risks.

i) Risk Management is transparent and inclusive.
All stakeholders need to be included, explained to of their responsibilities and importantly of the salient factors regarding decision making and reasoning behind controls.

j) Risk management is dynamic, iterative and responsive to change.
Whatever, the customer's organisation it is guaranteed that nothing remains constant and the risk management system needs to be extended into configuration change control both for projects and operational systems. The system must also continually reflect and respond to organisational change and the way the organisation operates.

k) Risk management facilitates continual improvement in the organisation.
The management system itself must be subject to review. The review will be based on its consistency with the above and its value to the organisation itself. The review must assess whether all these can be improved and where appropriate these recommendations put to the senior stakeholder for deliberation and action. The review should be regular with a frequency agreed with the senior stakeholder.