


2/7/2010



# ISO 27005 vs. AS/NZS 4360

*A Comparison of Risk Management Standards*



Pivot Point Security – Mosi K. Platt, CISA

# ISO 27005 vs. AS/NZS 4360

## *A Comparison of Risk Management Standards*

The purpose of this document is to identify the similarities and differences between ISO 27005:2008 and AS/NZS 4360:2004. An important note is that ISO 27005 is an information security risk management framework – *not* a generic risk management framework.

<b>Risk Management Activities</b>	<b>ISO 27005 Actions/Outputs</b>	<b>AS/NZS 4360 Guidelines</b>	<b>Differences</b>
Context establishment	Define scope and boundaries Specification of basic criteria <ul style="list-style-type: none"> <li>• Risk evaluation criteria</li> <li>• Impact criteria</li> <li>• Risk acceptance criteria</li> </ul> Establish organization for the information security risk management process	Establish the external context Establish the internal context Establish the risk management context Develop risk criteria Define the structure for the rest of the process	No significant differences
Risk assessment	Risk analysis <ul style="list-style-type: none"> <li>• Risk identification               <ul style="list-style-type: none"> <li>○ Identification of assets</li> <li>○ Identification of threats</li> <li>○ Identification of existing controls</li> <li>○ Identification of vulnerabilities</li> <li>○ Identification of existing controls</li> </ul> </li> <li>• Risk estimation               <ul style="list-style-type: none"> <li>○ Risk estimation methodologies</li> <li>○ Assessment of consequences</li> <li>○ Assessment of likelihood</li> <li>○ Level of risk estimation</li> </ul> </li> <li>• Risk evaluation</li> </ul>	Risk identification <ul style="list-style-type: none"> <li>• What can happen, where &amp; when</li> <li>• Why &amp; how can it happen</li> <li>• Tools &amp; techniques</li> </ul> Risk analysis <ul style="list-style-type: none"> <li>• Evaluate existing controls</li> <li>• Consequences &amp; likelihood</li> <li>• Types of analysis</li> <li>• Sensitivity analysis</li> </ul> Risk evaluation	No significant differences

<b>Risk Management Activities</b>	<b>ISO 27005 Actions/Outputs</b>	<b>AS/NZS 4360 Guidelines</b>	<b>Differences</b>
Risk treatment	Define risk treatment plan Risk reduction Risk avoidance Risk transfer	Identify options for the treatment of risks with positive outcomes  Identify options for treating risks with negative outcomes  Assess risk treatment options  Preparing and implementing treatment plans	No significant differences
Risk acceptance	The decision to accept the risks and responsibilities for the decision should be made and formally recorded	The level of risk retained may depend on risk criteria	AS/NZS 4360 does not provide very detailed guidelines for risk acceptance (aka retention)
Risk communication	Information about risk should be exchanged and/or shared between the decision-maker and other stakeholders	Communicate and consult.  The concept of 'risk communication' is generally defined as an interactive process of exchange of information and opinion, involving multiple messages about the nature of risk and risk management  Consultation can be described as a process of informed communication between organization and its stakeholders on an issue prior to making a decision or determining a direction on a particular issue.	No significant differences

<b>Risk Management Activities</b>	<b>ISO 27005 Actions/Outputs</b>	<b>AS/NZS 4360 Guidelines</b>	<b>Differences</b>
Risk monitoring and review	Monitoring and review of risk factors Risk management monitoring, reviewing and improving	Manage changes in context and risks Risk management assurance and monitoring <ul style="list-style-type: none"> <li>• Continuous monitoring</li> <li>• Line management review</li> <li>• Third party audit</li> </ul> Risk management performance measurement Post-event analysis	No significant differences