rightstrategy

PO Box 1152 Surrey Hills North Victoria Australia ABN 96 054 347 189 Ph: 61 3 9890 1161

Enterprise Risk Management Checklist

The following checklist is meant as a “guide” only and is not an absolute or exhaustive risk management resource.

Always refer to IS0 31000 (the standard) for clarification when implementing enterprise risk management and to ensure appropriateness of the checklist questions to the organisation.

Risk Scope & Application

1. The scope and application of risk management is documented and communicated?
2. The scope of the risk management framework considers internal risk? If so, what is the extent of internal risk scope coverage?
3. The scope of the risk management framework considers external risk? If so, what is the extent of external risk scope coverage?
4. Risk management terminology and definitions used by the organisation are defined and communicated?

Risk Context

5. The organisation has assessed its organisational context and risk perspective?
6. The organisation has documented a current risk context statement?
7. The various risk stakeholders (internal & external) have been formally identified?
8. A stakeholder analysis has been documented from a risk perspective?
9. The stakeholder analysis considers the needs and the degree of risk influence over the organisation?
10. A stakeholder communication plan exists (including any communication constraints)
11. A public relations communications policy has been established regarding risk communications?
12. The legal, statutory and other requirements of the organisation have been formally identified?
13. A process is in place to ensure that the organisation is kept up to date with applicable legal changes?
14. Responsibilities are established for the identification of legal impacts and dissemination of requirements?
15. A process is in place to ensure identified legal changes required are effectively implemented in a timely manner?

Risk Framework & Risk Process

16. A Risk Management Policy has been established, approved by the most senior manager.
17. The Risk Management Policy has been communicated to stakeholders (as appropriate)?
18. Risk management goals and objectives have been formalised, communicated, implemented & are being performance measured?
19. A Risk Management Strategy (What) document has been formalised, approved and communicated?
20. The Risk Management Strategy includes timing and responsibilities for risk implementation throughout the organisation?
21. A Risk Management Plan (How) document has been formalised, approved and communicated?
22. Risk authorities & responsibilities have been defined, documented and effectively communicated?
23. Risk authorities and responsibilities cover the entire risk scope and all levels & functions of the organisation?
24. An appropriate risk governance structure has been established and is effective?
25. A formal charter of operation exists for the various risk governance structure(s) in place?
26. The risk charter is effectively communicated and understood by the governance structure participants?
27. Risk lead and lag indicators have been established and implemented?
28. The risk indicators cover the risk management scope and are effective for managing risk?
29. A process has been established for consultation with the appropriate stakeholders with regards risk identification and assessment?
30. A process has been established for communicating risk related requirements with internal and external stakeholders?
31. Risks are identified, assessed, evaluated and controlled for all areas of the risk scope?
32. A risk assessment methodology is available & suitable for all areas of the organisation and types of risk (scope)?
33. The risk methodology to be used is quantitative?
34. The risk methodology to be used is qualitative?
35. The risk methodology to be used is a combination of quantitative & qualitative?
36. Personnel have been appropriately trained in the organisation's risk assessment methodology and requirements?

37. The likelihood and consequence descriptors are specific and detailed to properly assess risk for all areas of the scope?
38. The risk rating criteria provides adequate coverage for the entire risk scope?
39. Organisational risk culture is considered when establishing risk criteria and risk methodology?
40. The risk criteria and methodology cover critical success factors associated with the organisation and entire scope of risk?
41. Suitable methods are available and used for developing risk identification?
42. Organisational risks are identified and included on a risk register(s) or similar for all areas of risk scope?
43. Risk identification includes the sources of risk for all areas of risk scope?
44. Risk register addresses negative and positive risk impacts (as appropriate)?
45. Risk identification includes cause and consequence for all areas of risk scope?
46. The risk registers are current and documented review periods are defined to assist with ensuring that the risk registers remain current?
47. The risk controls are based on preventive, detective and corrective (as appropriate) for the entire risk scope?
48. The effectiveness of existing controls for all risks are regularly monitored and reported?
49. The risk register considers existing controls as part of the initial risk assessment?
50. The risk register considers existing controls as well as future risk treatments?
51. The various risk treatment options are available, documented and communicated to personnel for input and decision-making purposes?
52. Is a process in place for the development and approval of risk treatment plans for the entire risk scope?
53. Implementation plans exist for new risk treatment actions for the scope of risk?
54. A process and responsibilities are in place for tracking the implementation of new risk treatments for the risk scope?
55. A risk management budget exists either explicit or implicit within functional budgets?
56. The risk management budget is appropriate to the size, context and operation of the organisation?
57. The risk budget allows for input from external risk expertise in line with the risk scope requirements and needs?
58. The risk tolerance of the organisation is identified and communicated as part of the methodology and as appropriate to the scope of risk?
59. The risk appetite of the organisation has been established and is understood, monitored and controlled by the organisation?

60. The risk evaluation process considers risk context, legal requirements, risk tolerance, the organisation’s risk appetite and risk priority?
61. Is the hierarchy of controls effectively used for OH&S and sustainability type risks?
62. Where required by law (e.g. OH&S) are risks reduced to as low as reasonably practical (ALARP)?
63. Is a process and responsibilities in place to accept (sign off) risks that exceed the risk tolerance of the organisation?
64. Do senior management have oversight of key organisation risks in line with organisational context and scope?
65. The risk framework monitoring and review process has been established and implemented?
66. The risk monitoring processes include all areas of risk scope? (List the processes and methods for monitoring all risks)
67. A risk management review process has been established for the risk scope? Detail how you ensure that all areas of risk are reviewed?
68. Processes have been put in place to ensure continuous improvement of the risk framework, process, criteria, methodology & culture?
69. Records of risk management have been identified?
70. Risk management records are version controlled and previous versions saved?
71. Retention periods have been established for risk management records?
72. Responsibility has been assigned for the retention of risk management records?