

ORM

Operational Risk Management



ORM

The following slides outline an approach to meeting ORM requirements across diverse groups and then being able to track and mitigate risk.



ORM

There is a sequence of 10 simple steps and principles to follow which can also roll into an easily managed Risk Knowledge Base.

The following slides outline the key steps and solutions.



ORM

1. Business Operations

1.1. Describe the Business

1.2. Identify the elements of, and phases in, the business and its operations.

Operations are commonly associated with events/outcomes/processes.



ORM

2. Key Business Operations

2.1. List the KEY (most important) operations.

2.2. The key operations are commonly associated with critical/crucial events, processes or outcomes.



ORM

3. Initial Threat Assessment

3.1. Ask yourself, “Are there any threats/events that could harm these key operations?”

(If you don't know, find out).

3.2. Ask yourself, “Are the key operations vulnerable to these threats/events?”

(If you don't know, find out).



ORM

4.

Initial Risk Assessment

Threat and Vulnerability

4.1. Assess the evidence regarding the threat.

4.2. Assess the evidence of the vulnerability.



ORM

4. Initial Risk Assessment Risk

Risk is a combination of threat and vulnerability plus the likely impact according to the value/importance of the thing that is threatened.

High threat and invulnerable equates to no risk. No threat and vulnerable equates to no risk.

Some threat and some vulnerability to a thing which is unimportant is a low risk.

High threat, low vulnerability to an important “thing” is a HIGH RISK.

Act to mitigate the High Risk!



ORM

5. Risk Controls

5.1. Risk Controls/Processes are the tools, processes and devices put in place to reduce, and MONITOR, risk.

5.2. Design the tools and controls and the measures, metrics and other demonstrable outcomes that prove effective operation of the control.

NOTE: Tools might be situation specific



ORM

6. Initial Control Assessment

6.1. Assess, perhaps externally, the appropriateness of the Controls

6.2. Assess the appropriateness of the measures, metrics and other demonstrable outcomes the tools/controls produce.

If failing, modify the control or the tools.



ORM

7. Control Management Processes

7.1. Describe the Control Management Processes

7.2. Explain how the processes maintain the tools/controls and demonstrable outcomes.



ORM

8. Secondary Control Assessment

8.1. Assess, perhaps externally, the appropriateness of the Control Management Processes in terms of creating and supporting tools and controls.

8.2. Assess the appropriateness of the processes for creating and supporting measures, metrics and other demonstrable outcomes the tools/controls produce.

If failing, modify the control maintenance processes.



ORM

9. Quality Assessment

9.1. Quality assure Control Processes.

9.2. Remediate and/or improve QA processes for
Tools and Controls.

DOCUMENT IN QA BEST PRACTICE FASHION



ORM

10. Final Risk Assessment

10.1. Assess the level of risk based on the level of threat and vulnerability that now exists given that the tools and controls ought reduce vulnerability to a given threat or reduce the likelihood of harm or the level of harm that may result.

10.2. Remember, the importance of the operational component that is being protected has not changed. What has changed is the vulnerability to a threat or the likelihood that the threat will be enacted.



ORM

In summary

..... identify what is important, assess the risk, design the controls, test the effectiveness of controls, accompany with sound processes, test again, enact and QA the risk processes.

For more information on programs and associated services,
please email leigh@kinematic.com.au
Or telephone (+ 61 3) 5222 7578

