



Investors in
Risk Management

Sample Company
Risk Management Maturity Report
30 September 2015

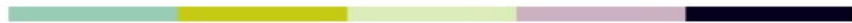


TABLE OF CONTENTS

1. INTRODUCTION

- 1.1 Background to the Assessment
- 1.2 Assessment Methodology
- 1.3 Desk-Based Review of Documentation
- 1.4 Overview of the Risk Management Maturity Model (“RMMM”)

2. RISK MANAGEMENT MATURITY OF SAMPLE COMPANY

- 2.1 Assessment Results
- 2.2 Risk Management Maturity – Summary Observations by Core Areas
- 2.3 Risk Management Maturity – Recommendations by Core Areas
- 2.4 Certificate of Accreditation

1. INTRODUCTION

1.1 Background to the Assessment

Sample Company is a leading UK construction company. Sample Company has selected IIRM to carry out an external review of its risk management maturity on an annual basis. This is the third such assessment.

1.2 Assessment Methodology

The approach adopted in assessing risk management maturity involved:

1. Use of IIRM Risk Management Maturity Model (RMMM) to support the assessment.
2. Desk-based review of Sample Company's risk strategy, risk policy, risk registers and other documents relevant to the risk management.
3. Meetings with Sample Company management and staff involved in risk management across the organisation.
4. Assessment of eight core areas with each category having an individual assessment that is then aggregated to provide an overall risk maturity rating for the organisation.

1.3 Desk-Based Review of Documentation

A large number of documents were reviewed by IIRM in support of the assessment. The desk-based review of documentation helped IIRM to gain insights into the practical operations of risk management in the college. Initial observations on maturity were identified and these observations were discussed as part of the management and staff meetings to support the maturity assessment.

1.4 Overview of the Risk Management Maturity Model (“RMMM”)

In evaluating the effectiveness of the risk management frameworks, the IIRM Risk Management Maturity Model (“RMMM”) forms the cornerstone of our risk management maturity assessment methodology.

Core Areas

RMMM covers the following eight core areas with each category having an individual assessment that is then aggregated to provide an overall maturity level:

1. Risk context
2. Risk culture
3. Risk identification
4. Risk assessment
5. Risk treatment
6. Communication and reporting
7. Review
8. Risk management systems

Risk Maturity Levels

To rate the level of risk maturity, all eight core areas were examined through a desk-based review and meetings with relevant management and staff. The RMMM describes an improvement path from a very basic and immature Risk Management function to a mature and advanced function focused on continuous improvements. The Model consists of the following five risk management maturity levels to gauge risk maturity:

Level	Level Name	Description
1	Very Basic	Minimal or no awareness and understanding / No process in place / Unsatisfactory
2	Basic	Applied inconsistently / Some formal processes in place / Satisfactory
3	Emerging	Implemented consistently across the organisation/ Not all the processes implemented fully / Good
4	Mature	Consistently and fully implemented. / Processes are reviewed for improvements / Very Good
5	Advanced	Risk management is considered a value driver / Advanced processes are used / Excellent

Overall assessment Levels / Rating

Levels	Score %	Descriptor
1. Very Basic	1-20	The organisation has minimal or no awareness and understanding of risk management. Risk management is performed on an ad hoc basis by individuals. No processes in place.
2. Basic	21-40	Risk management applied inconsistently with limited standardisation. Some formal processes in place.
3. Emerging	41-60	A risk management framework exists with defined and documented risk management principles. Risk management applied consistently throughout the organisation. Not all processes have been fully implemented.
4. Mature	61-80	The organisation is proactive in risk management. Risk management is consistently and fully implemented across the organisation. Key risk indicators are used for major risks. Risk management processes are monitored and reviewed for continuous improvements.
5. Advanced	81-100	Risk management is considered a value driver and is proactively used for day-to-day decision-making and pursuit of opportunities. KRIs and predictive risk analytics are proactively used to identify and monitor risks. Advanced and sophisticated risk management processes are used.

RMMM Levels and their distinguishing features

Very Basic (Level 1)	Basic (Level 2)	Emerging (Level 3)	Mature (Level 4)	Advanced (Level 5)
<ul style="list-style-type: none"> • Emphasis on protecting assets • Focus on physical and financial assets • Risks managed within functional silos • Inconsistent approaches • No formal risk management processes • Not being able to distinguish between positive and negative risk • No systematic attention to risk management • No formal risk management policy 	<ul style="list-style-type: none"> • Understand that risks require formal management • Establishes basic risk management processes • Narrow scope of risk management, generally restricted to addressing critical and pure risks • Identifying regular risks and establishing insurance as the unique strategy • Tends to be influenced less by formal risk management processes than by the repetition of activities and practices that have worked out for the organisation before • Demonstrate an isolation of the risk management function • Uses the same measures or risk responses that were used the period before • Policies would not be reviewed nor would the treated risks be evaluated • Risk would be considered a static phenomenon instead of a dynamic one 	<ul style="list-style-type: none"> • Define and implement a formal risk management process. • Define policies and procedures that could guide risk management • Seek to formalise the risk management function within the organisation • Identify risks in a systematic manner • Analyse risks considering their probability and impacts • Insurance is not the only response to risks • Internal and operational risks are identified and included in the risk management policy • Consider reputational risks as well as risks related to the damage inflicted on a third party • Would mention explicitly which responses they have taken for each specific analysed risk • Establish a clear objective for the risk management policy • Determine a procedure for reviewing and evaluating the risk management program • Establish responsibilities and roles 	<ul style="list-style-type: none"> • Facilitate the implementation of the risk management perspective • Look for the application of the wider perspective of risk management • Extend risk management processes throughout the organisational hierarchy and across all functional boundaries • Implement a monitoring process to have a clear view of the effectiveness of the risk management program • Participation of top management in defining risk policy and reports • Review of risk management process • Setting up goals, strategies and practices of the best practices of risk management • May have difficulties adapting to the challenges that the context imposes on them 	<ul style="list-style-type: none"> • Board/executive support of risk management • Clear accountabilities • Appropriate risk oversight structures • Dedicated risk management coordinator • Explicit consideration of both operational and strategic risks • Risk management integrated with operational and general management processes • Clear accountabilities and timeframes for treatment of risks • Differentiated risk reporting tailored to specific stakeholders • Regular reviews of risk and risk management processes • Risk management is considered a value driver and proactively used for day-to-day decision-making and pursuit of opportunities. • KRIs and predictive risk analytics are proactively used to identify and monitor risks. • Advanced and sophisticated risk management processes are used.

Features of Maturity by core areas

1	Context	Key characteristics
1.1		The board and executives have expressed their support for a risk management programme.
1.2		The organisation has identified a person who will be responsible for implementing and controlling risk management.
1.3		The risk manager (or equivalent) has reasonable access to staff and management personnel across the organisation.
1.4		The organisation has identified its internal and external stakeholders.
1.5		The organisation has a documented ERM Strategy.
1.6		The risk process is integrated with other organisational planning processes - for example, risks are considered during the strategic planning, budgeting and audit planning processes.
1.7		The risk committee (or equivalent) and the board have approved the risk strategy.
1.8		The organisation has agreed what types and levels of risks are acceptable (Risk appetite/tolerance).
1.9		There is a clear organisational strategy (or objectives) articulated for the organisation.
1.10		A risk policy has been defined.
1.11		The risk committee (or equivalent) and the board have approved the risk policy.
1.12		The organisation has defined risk management roles and responsibilities.
1.13		The job descriptions for the organisation include responsibilities for risk management.
1.14		The organisation has an existing risk profile/ risk register.
1.15		The current approach to risk recording and reporting is meeting organisational needs.
1.16		The organisation has defined categories of risk relevant to the organisation and industry.
1.17		The risk categories reflect all strategic and operational risk areas of the business.
1.18		The organisation has defined and agreed a likelihood scale to assess the potential for risks to occur throughout the organisation.
1.19		The organisation has defined and agreed a consequence scale to help assess risk impacts across the organisation.
1.20		The organisation's consequence scale describes both financial and non-financial impacts.
1.21		The risk management framework considers the effectiveness of controls or risk treatments.
1.22		There is an agreed template or format for recording risks and risk treatment information (a risk register).
1.23		A mechanism is in place to identify, assess, treat and review risks on projects.
1.24		There is an agreed format/template for reporting on risk.
1.25		There is a process and/or template where new risks can be recorded.

2	Culture	Key characteristics
2.1	The mission, vision, and purpose of the organisation promote a culture of risk-awareness.	
2.2	Risks are managed on a day-to-day basis as part of the application of organisational values.	
2.3	Risk management systems and processes enable effective and efficient risk management.	
2.4	The process for managing risk has been/is integrated with day-to-day processes.	
2.5	The structure enables risk-based decision-making without bureaucracy, making jobs easier and facilitating better outcomes.	
2.6	Leadership skills and attributes around risk management are fostered, rewarded and implemented across the business.	
2.7	Poor behaviours or practices around risk management are not tolerated by leaders.	
2.8	Jobs have been designed to reflect risk management and risk policies.	
2.9	Various job definitions include the performance expectations around risk management.	
2.10	The accountabilities with regard to risk and risk management have been clearly articulated.	
2.11	There is a clearly articulated consensus around desired behaviours across the business.	
2.12	Desired behaviours are modelled by leaders and workers are responsive to these behaviours.	

3	Risk Identification	Key characteristics
3.1	The executive and board have considered risks relating to the achievement of key organisational goals and objectives.	
3.2	Research has been performed to understand common industry-specific risks.	
3.3	A risk brainstorming workshop (or workshops) has been conducted.	
3.4	Information has been gathered from different sources to identify risks.	
3.5	The organisation has applied a set of risk identification tools and techniques.	
3.6	The organisation has used risk categories for comprehensiveness.	
3.7	People with appropriate knowledge have been involved in identifying possible risks.	
3.8	The organisation has documented all identified risks.	
3.9	The organisation has documented the risk identification process.	
3.10	The organisation has assessed the effectiveness of the risk identification process.	
3.11	The organisation has identified the risk drivers for identified risks.	

4	Risk Assessment	Key characteristics
4.1	The organisation has considered the history of events and incidents in the organisation during the risk assessment process.	
4.2	Existing controls have been identified and evaluated for risks during the risk assessment process.	
4.3	The perceived effectiveness of controls has been assessed by a person who understands the risk and the controls in place.	
4.4	The risk register is updated throughout the year to reflect changes in risks.	
4.5	The organisation has determined the risk likelihood for the identified risks.	
4.6	The organisation has determined the risk impacts for the identified risks.	
4.7	The organisation has ranked the risks based on the outcome of the risk assessment process.	
4.8	The organisation has developed a list of priority risks.	
4.9	The organisation has considered the overall risk profile.	
4.10	The Key Risk Indicators (KRIs) have been defined and agreed for key risks/ risk areas.	
4.11	The organisation has documented the risk assessment process.	

5	Risk Treatment	Key characteristics
5.1	It is clearly specified who is accountable for every identified risk (the 'risk owner').	
5.2	It is clearly specified who is accountable for each control and action to treat the risks.	
5.3	The organisation has identified possible actions/treatment plans that could help to reduce the risk level.	
5.4	The benefits of a treatment approach have been compared to the potential cost of the risk to determine the appropriateness of the treatment strategy.	
5.5	Risk treatment plans or action plans have been documented and approved for important risks.	
5.6	Due dates/completion dates have been agreed for risk treatment actions and plans.	
5.7	The organisation's physical assets are appropriately insured.	
5.8	A Business Continuity Plan (BCP) is in place for critical organisational functions/processes.	

6	Communication and Reporting	Key characteristics
6.1	The organisation has established a stakeholders' communication plan.	
6.2	The organisation has developed key messages and identified their purpose.	
6.3	The organisation has identified communication owners and senders.	
6.4	The organisation has identified appropriate communication channels.	
6.5	The organisation has determined the timing of communication.	
6.6	The organisation has determined the frequency of communication.	
6.7	Staff members know to whom they should report/escalate risks.	
6.8	Managers or supervisors know that they are responsible for managing risk in their area/s of responsibility.	
6.9	The executive and the board have provided guidance on what information they would like to see in risk reports,	
6.10	There is agreement on when and how often risk reports will be produced.	
6.11	The recipients of risk reports have been identified and agreed.	
6.12	Different risk reports can be produced to meet different needs of stakeholder groups.	
6.13	Responsibility for managing/treating specific risks has been assigned and communicated to those who are responsible.	
6.14	Staff members are encouraged and motivated to report risk or suggest risk reduction strategies.	
6.15	Reports contain current and updated quality information.	
6.16	Reports are easily understandable.	
6.17	Reports contain the right level of detail and are supported by detailed underlying risk information, where appropriate.	

7	Review	Key characteristics
7.1	The organisation has established a monitoring and review cycle.	
7.2	The organisation measures risk management performance.	
7.3	The organisation reviews current risk management context to ensure it remains aligned to the strategic intent of the organisation.	
7.4	The risk process follows the steps described in the risk management framework.	
7.5	An internal audit function/process is in place.	
7.6	The internal audit function or equivalent reviews risk management processes.	
7.7	Internal auditors focus their time and efforts on the most critical risks recorded in the risk register.	
7.8	The organisation tracks the changes in risk levels over time, in order to understand trends/changes in risk levels.	
7.9	The risk policy has been reviewed within the last year.	
7.10	The risk committee (or equivalent) and the board have reviewed the risk strategy.	
7.11	The organisation detects changes in external and internal context, including changes to the risk itself which may require revision of risk treatments and priorities.	
7.12	The organisation ensures that all risk control and treatment measures are effective in both design and operation.	

8	Risk Management Systems	Key characteristics
8.1	The current risk register is easy to use and update.	
8.2	The organisation is sufficiently large and complex to warrant the use of risk management software.	
8.3	The organisation has agreed a budget for risk management systems.	
8.4	Risk rating scales (likelihood, consequence) can be customised by the user.	
8.5	Risk categories can be defined by the user and sub-categories are allowed.	
8.6	The organisational structure can be reflected in the risk assessment hierarchy.	
8.7	Risks can be linked to specific business processes.	
8.8	Risks can be linked to one or more business objectives or strategies.	
8.9	The system allows multiple access levels (view, modify, add etc.)	

8.10	The system maintains an audit trail of changes to risk information over time, notably previous risk assessment scores.
8.11	The system allows multiple users to access the data.
8.12	The system can be accessed via the web or intranet.
8.13	Multiple risk drivers (causes) can be linked to one or more risks.
8.14	Multiple impacts can be linked to each risk.
8.15	A risk can be linked to more than one area of the business.
8.16	A single risk can be rated by more than one person.
8.17	Risks can be assessed at both an inherent and residual level.
8.18	'Near-miss' information is recorded by the system.
8.19	The system supports the comparison of alternative mitigation strategies.
8.20	The system allows the user to define thresholds or rules for escalating risks.
8.21	Multiple risk treatments or action plans can be linked to a risk or risks.
8.22	More than one person can be allocated responsibility for a specific risk or risk treatment.
8.23	Risk events or incident costs can be associated with a specific risk or risks.
8.24	Dates for action plans/risk reviews etc. can be captured and reported on.
8.25	The system allows for KRIs to be defined and linked to specific risks.
8.26	The user can easily define or customise risk reports.
8.27	The system contains an appropriate range of pre-defined risk reports.
8.28	The system supports graphical reporting (heat maps, matrices, graphs).
8.29	Risks can be reported by business units.
8.30	Risks can be reported by responsible persons.
8.31	Risks can be reported by severity (likelihood and consequence).
8.32	Risk trends can be reported on based on historical or previous risk assessments.
8.33	The system allows the progress of risk treatment plans to be tracked and reported on.
8.34	Reminders can be sent to those responsible for risk treatments, for example via email.
8.35	Data can be exported from or exported to other applications.

2. Risk Management Maturity of Sample Company

2. RISK MANAGEMENT MATURITY OF SAMPLE COMPANY

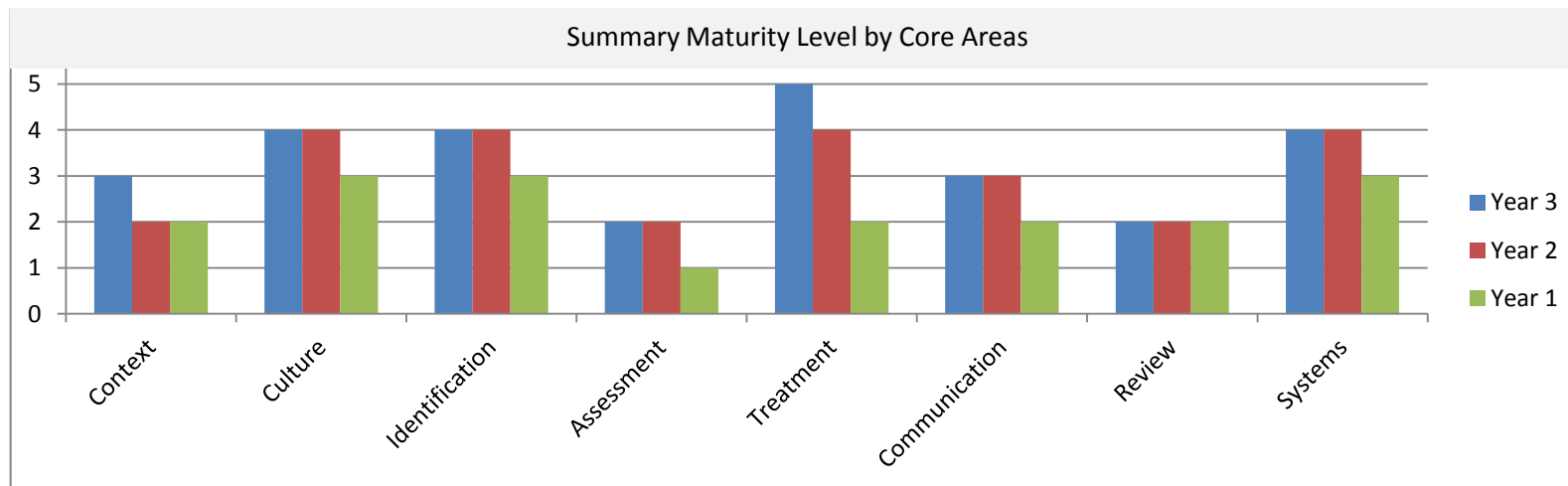
2.1 Assessment Results

Overall we found that the formal risk management framework within Sample Company operates effectively given the risk profile of the organisation, the length of time that formal risk management has been in place and the resources available to support and manage the processes.

We found that Sample Company compares favourably to other organisations of a similar scale and profile in terms of the maturity and effectiveness of its risk management framework. Through the course of the review we identified elements of good practice and areas for improvement, and these are reported in detail in the Summary Observations and Recommendations sections. Summary observations of risk maturity by each core area are presented in section 2.2 and recommendations for improvement to a higher level of maturity are made in section 2.3

Please note that the risk management maturity assessment was not an audit and we have not reported in detail against each core area. Rather, we have attempted to assess the risk management maturity through a desk-based review of documents and meetings with management and staff.

The following graph illustrates the level of maturity against each core area within the Sample Company:



The Risk Maturity Matrix Score based on the desk-based review of documentations and meetings with management and staff in relation to each core area is as follows:

Sample Company Risk Maturity Matrix						
Core Areas	Current Year	Previous Year	Current Year		Previous Year	
	Score %	Score %	Level		Level	
Risk Context	60	40	Emerging	3	Basic	2
Risk Culture	80	72	Mature	4	Mature	4
Risk Identification	72	70	Mature	4	Mature	4
Risk Assessment	40	35	Basic	2	Basic	2
Risk Treatment	92	80	Advanced	5	Mature	4
Communication & Reporting	52	45	Emerging	3	Emerging	3
Review	36	29	Basic	2	Basic	2
Systems	76	64	Mature	4	Mature	4
Overall Score and Level	64	55	Mature	4	Emerging	3

The overall Risk Maturity Matrix Score for the Sample Company is 64. This score translates into an overall risk maturity level of 4 (Mature).

Sample Company Risk Management Maturity Matrix by Core Areas

Core Areas	Sample Company Risk Management Maturity Matrix by Core Areas																				Score	Level								
	Very Basic (level 1)					Basic (Level 2)					Emerging (Level 3)					Mature (Level 4)						Advanced (Level 5)								
Context																60											60	Emerging	3	
Culture																					80						80	Mature	4	
Identification																					72						72	Mature	4	
Assessment																					40						40	Basic	2	
Treatment																											92	92	Advanced	5
Communication																					52						52	Emerging	3	
Review																					36						36	Basic	2	
Systems																					76						76	Mature	4	
Overall Level																					64						64	Mature	4	
Scale: %	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100					

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to the Risk Management Context

Risk Management Context		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Emerging (3)	60
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • Executives have expressed their support for a risk management programme • The organisation has identified its internal and external stakeholders. • A risk policy has been defined. • The organisation has defined risk management roles and responsibilities • The job descriptions for the organisation include responsibilities for risk management • A mechanism is in place to identify, assess, treat and review risks on projects 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Risk Management Culture

Risk Management Culture		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Mature (4)	80
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • The mission, vision, and purpose of the organisation promote a culture of risk-awareness. • Risk management systems and processes enable effective and efficient risk management. • Jobs have been designed to reflect risk management and risk policies. • Desired behaviours are modelled by leaders and workers are responsive to these behaviours. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Risk Identification

Risk Identification		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Mature (4)	72
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • Research has been performed to understand common industry-specific risks. • Information has been gathered from different sources to identify risks. • The organisation has applied a set of risk identification tools and techniques. • The organisation has documented all identified risks. • The organisation has identified the risk drivers for identified risks. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Risk Assessment

Risk Assessment		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Basic (2)	40
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • The organisation has considered the history of events and incidents in the organisation during the risk assessment process. • Existing controls have been identified and evaluated for risks during the risk assessment process. • The organisation has determined the risk likelihood for the identified risks. • The risk register is updated throughout the year to reflect changes in risks. • The organisation has developed a list of priority risks. • The organisation has documented the risk assessment process. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Risk Treatment

Risk Treatment		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Advanced (5)	92
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • It is clearly specified who is accountable for every identified risk • It is clearly specified who is accountable for each control and action to treat the risks. • The organisation has identified possible actions/treatment plans that could help to reduce the risk level. • Risk treatment plans or action plans have been documented and approved for important risks. • The organisation's physical assets are appropriately insured. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Communication and Reporting

Communication and Reporting		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Emerging (3)	52
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • The organisation has established a stakeholder’s communication plan. • The organisation has developed key messages and identified their purpose. • The organisation has identified appropriate communication channels. • The organisation has determined the frequency of communication. • The recipients of risk reports have been identified and agreed. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Review

Review		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Basic (2)	36
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • The organisation has established a monitoring and review cycle. • The organisation measures risk management performance. • The internal audit function or equivalent reviews risk management processes. • The risk policy has been reviewed within the last year. 		

2.2 Risk Management Maturity – Summary Observations by Core Areas

The following table provides a summary of observations relating to Risk Management Systems

Risk Management Systems		
Maturity Assessment Date	Maturity Level	Maturity Score
05/11/2015	Mature (4)	76
Summary Observations		
<p>Based on desk based review performed and meetings carried out;</p> <ul style="list-style-type: none"> • The current risk register is easy to use and update • The organisation has agreed a budget for risk management systems. • Risk categories can be defined by the user and sub-categories are allowed. • Risks can be linked to specific business processes. • Risks can be linked to one or more business objectives or strategies. • Multiple impacts can be linked to each risk. 		

2.3 Risk Management Maturity – Recommendations by Core Areas

Risk Context – Assessment Rating: Emerging (Level 3)

- The job descriptions for the organisation should include responsibilities for risk management.
- The risk categories should reflect all strategic and operational risk areas of the business.
- The organisation's consequence scale should describe both financial and non-financial impacts.

Risk Culture – Assessment Rating: Mature (Level 4)

- Risks should be managed on a day-to-day basis as part of the application of organisational values.
- The structure should enable risk-based decision-making without bureaucracy, making jobs easier and facilitating better outcomes.
- It is advisable that Poor behaviours or practices around risk management should not be tolerated by leaders.
- Jobs should be designed to reflect risk management and risk policies.

2.3 Risk Management Maturity – Recommendations by Core Areas

Risk Identification – Assessment Rating: Mature (Level 4)

- Consider conducting risk brainstorming workshop (or workshops) for managers.
- Consider using risk categories for comprehensiveness.
- Identify the risk drivers for identified risks.

Risk Assessment – Assessment Rating: Basic (Level 2)

- Existing controls should be identified and evaluated for risks during the risk assessment process.
- The risk register should be updated throughout the year to reflect changes in risks.
- Consider the overall risk profile.

2.3 Risk Management Maturity – Recommendations by Core Areas

Risk Treatment – Assessment Rating: Advanced (Level 5)

- The benefits of a treatment approach should be compared to the potential cost of the risk to determine the appropriateness of the treatment strategy.
- Risk treatment plans or action plans should be documented and approved for important risks.
- Due dates/completion dates should be agreed for risk treatment actions and plans.

Communication and Reporting – Assessment Rating: Emerging (Level 3)

- Consider establishing a stakeholder’s communication plan.
- Consider developing key messages and identified their purpose.
- The executive and the board should provide guidance on what information they would like to see in risk reports.

2.3 Risk Management Maturity – Recommendations by Core Areas

Review – Assessment Rating: Basic (Level 2)

- Consider establishing a monitoring and review cycle.
- Board should review the risk policy
- It is advisable to ensure that all risk control and treatment measures are effective in both design and operation.

Risk Management Systems – Assessment Rating: Mature (Level 4)

- System should allow to rate a single risk by more than one person
- Risks should be reported by business units as well.
- Risk trends should be reported on based on historical or previous risk assessments.
- The system should allow tracking the progress of risk treatment plans.

2.4 Certificate of Accreditation

IIRM Risk Management Maturity Model (RMMM) measures the maturity of risk management processes and suggests improvements towards a state where the entity is in an improved condition for the achievement of its strategic and operational objectives.

Maturity levels of RMMM are well-defined evolutionary levels toward achieving a mature process. Each IIRM Risk Management Maturity level provides a layer in the foundation for continuous improvement in a risk management framework.

An output of Risk Management Maturity Assessment is a certificate of accreditation which describes the level of maturity the organisation has achieved. IIRM Risk Management Maturity levels are translated into five IIRM accreditation levels called Platinum, Gold, Silver, Bronze and Standard.

Investors in Risk Management (IIRM) Accreditation Levels		
Maturity Level	Maturity Level Name	IIRM Accreditation Level
1	Very Basic	Standard
2	Basic	Bronze
3	Emerging	Silver
4	Mature	Gold
5	Advanced	Platinum

The overall Risk Maturity Matrix level for the Sample Company is Level 4 (Mature). Sample Company has achieved Investors in Risk Management Gold status accreditation.



CERTIFICATE OF ACCREDITATION

This is to certify that

Sample Company

has achieved Investors in Risk Management

GOLD STATUS

The Chairman

The Chairman
Chairman, Investors in Risk Management UK

Date: 08/10/2015

GOLD



Investors in
Risk Management



Investors in
Risk Management



Investors in
Risk Management

Investors in Risk Management

3 Oswin Road
Leicester, LE3 1HR
United Kingdom

T: 00 (44) 116 3664 011
info@iirmglobal.com
www.iirmglobal.com

This document provides general information. The information contained in this document does not constitute advice and should not be relied upon as such. Professional advice should be sought prior to actions being taken on any of the information.

Investors in Risk Management (IIRM) disclaim all responsibility and liability arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

© 2015 Investors in Risk Management Limited.

Registered Office: Investors in Risk Management Limited, 3 Oswin Road, Leicester, LE3 1HR

www.iirmglobal.com