

Institute of Technology Blanchardstown

Internal Audit Review of Risk Management Framework

Ref: 2016/S01

Date: 31 August 2016

Report Distribution

*Audit Committee
Top Management Group*

Executive Summary

An audit of the Risk Management Framework that is in place in the Institute of Technology Blanchardstown (ITB) was agreed as part of the 2016 Internal Audit plan. The objective of the audit was to perform an assessment of the design and operating effectiveness of key controls and processes in place over Risk Management within ITB.

Based on our work we identified some **good practices** with respect to Risk Management in ITB. Most notable of these were:

- An awareness of the importance of Risk and Risk Management amongst all Managers interviewed. Risk Management is a central part of the strategic management of ITB that supports the development and implementation of ITB's strategy; and,
- While the majority of the administration work in updating the risk register rests with the Secretary Financial Controller, it is acknowledged by the Top Management Group that Risk Management is their responsibility, as part of their day to day operational activities.

We identified five findings as part of our review, which are rated as follows:

Rating	Significance	No. of findings
Grade 1	Critical	-
Grade 2	Substantial	3
Grade 3	Moderate	2

The grade 2 findings relate to:

- Enhancements required with respect to the current risk governance structure in ITB;
- Improvements identified for the risk identification and assessment process; and,
- No formal process is in place for regular risk monitoring and reporting.



Use of this Report

This report is intended for the information and use of Institute of Technology Blanchardstown and is not intended to be relied upon by anyone other than ITB. We accept no duty of care and deny all liability to any third party that places reliance on our report.

We have provided no opinion, attestation or other forms of assurance with respect to our services or the information upon which our services are based. We did not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in our Terms of Reference (Appendix A).

Our work was performed in accordance with the PwC's Internal Audit Methodology which is consistent with the Chartered Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing. As agreed, the review did not constitute an examination in accordance with full scope generally accepted auditing standards.

Acknowledgement

We would like to thank all personnel who assisted and facilitated us in carrying out this review.

PricewaterhouseCoopers
August 2016



Audit Overview

Background

As part of the Internal Audit plan for 2016 an internal audit of the Risk Management Framework that is in place in ITB was agreed.

Objective

The objective of the internal audit was to perform a detailed review of the design and operating effectiveness of the Risk Management Framework, structure processes and controls that are in place in ITB.

Scope & Approach

Our scope and approach is based on the key elements of the PwC's Enterprise Risk Management Lifecycle which is set out below.

As part of the audit we gained an understanding and review the key elements in the risk lifecycle including the risk identification and assessment processes, risk register reporting and monitoring.

Our approach comprised a desktop review of key risk documentation review including the risk register, risk management framework, policy and procedures that are in place. We conducted a number of interviews with key stakeholders including members of the Top Management Group (TMG).

We also assessed ITB's Risk Management Framework to see if it is in line with the compliance requirements of the Code of Governance for the Institutes of Technology.



Summary of Findings

Finding	Rating
1. Enhancements required for existing risk governance structure	Grade 2
2. Improvements identified for risk identification and assessment process	Grade 2
3. No formal process in place for regular risk monitoring and reporting	Grade 2
4. Risk Management Policy requires updating and risk appetite not formally defined	Grade 3
5. No regular risk management training given to staff	Grade 3

Detailed Findings & Recommendations

1. Enhancements required for existing risk governance structure (Grade 2)

Risk Governance is about the structures, culture and processes that support good business decision making. Effective risk governance should provide the operating model and decision-making framework needed to identify and respond to risks. To be effective, all the pieces of the framework need to be in place and operating, including roles and responsibilities - starting with Governing Body and the Top Management Group.

Current Practice

The roles and responsibilities of Governing Body and Management team are formally documented in the Risk Management Policy. These include the role of Governing Body to set the tone and influence the culture of the risk management process and determine the risk appetite. The role of the Top Management Group, functional areas and Heads of Department includes implementation of the process and policies on risk management and internal controls including the identification and assessment of risks within their areas of control. The Audit Committee's role "to keep under review and advise on the operation and effectiveness of the Institute's risk management systems" is clearly set out in its Terms of Reference.

A risk register has been documented for ITB and all risks recorded on the Risk Register are assigned an owner (either an individual or a group) across the Institute. There is a clear link between the principal risks identified by Internal Audit in its audit scoping and planning documents.

Findings	Recommendations	Management Action Plan
<ul style="list-style-type: none"> Each Head of Department and TMG member are responsible for identifying and managing their own risks. However as the collation and updating of the risk register (as part of the risk management process) rests primarily with the Secretary / Financial Controller, it is updated on an ad-hoc basis. There is no separate formal risk forum or individual who is formally responsible for maintaining the Risk Register on a regular basis, overseeing progress of remedial actions and formally reporting to Governing Body or the Audit Committee. Governing Body is required to annually review the Institute's approach to risk management. This has not been formally completed for a number of years. 	<ul style="list-style-type: none"> Formally nominate a person at senior level with overall responsibility for the risk management framework and process within ITB. Nominate Risk Champions for each Business Unit in the Institute. Establish a formal risk governance and reporting structure for ITB and ensure this is clearly documented in the updated Risk Management Policy. Define and agree the level of risk reporting required at TMG, Audit Committee and Governing Body levels and implement accordingly. See Appendix D for an example Risk Governance Structure. Ensure that Governing Body or the Audit Committee conducts a formal annual review of the effectiveness of the risk management framework. 	<ol style="list-style-type: none"> One member of the ITB Senior Management (TMG) group will be nominated as the person with overall risk management responsibility for the Institute. (Target date: 30 September 2016) The current risk management practices will be documented, updated to take account of audit and internal audit recommendations, and included in a revised risk Management Policy to be adopted. (31 October 2016) The Policy document will include a proposed Risk Governance Structure with reporting processes outlined. (31 October 2016) Management will propose to Governing Body, through Audit Committee, an

<ul style="list-style-type: none"> While the Audit Committee and Governing Body have responsibility for risk, through discussions and a review of a sample of Governing Body meeting agendas, risk is not a standing agenda item for meetings. 	<ul style="list-style-type: none"> Include Risk as a standing agenda item at Audit Committee and / or Governing Body meetings. 	<p><i>appropriate annual review mechanism. (31 October 2016)</i></p> <p>5. <i>Accepted as recommendation to Audit Committee (AC). Management suggest that Governing Body deal with Risk through AC reports with a facility to add risk to any other agenda if deemed necessary. (31 October 2016)</i></p> <p>Responsible Party</p> <p><i>Secretary / Financial Controller</i></p>
---	---	--

2. Improvements identified for risk identification and assessment process (Grade 2)

Risk identification and assessment are fundamental elements of a Risk Management Framework. They comprise the process of determining, assessing and quantifying risks that could potentially impact on the achievement of business objectives.

Current Practice

A formal Risk Register is in place for ITB which identifies a mix of risks under the defined headings of Strategic, Operational, Financial, Reputational & Compliance and IT. The risk register was drafted in February 2016 and includes headings for information on impact, likelihood, overall score, risk rating, controls, risk owner, rating of current controls, actions required and specified timeline.

The current risk register comprises 49 risks and includes a documented scoring schedule which includes definitions for Impact, Likelihood, Overall Risk Rating and Control Effectiveness. Impact criteria are based on ratings from Insignificant (1) to Catastrophic (5). Likelihood criteria are rated from Rare (1) to Very Likely (5). The product of these two gives an overall risk rating (high, medium and low).

Findings	Recommendations	Management Action Plan
<ul style="list-style-type: none"> There is no defined, regular risk identification and assessment process in place to identify risks at Business Unit or Institute-wide levels. The current Risk Register was last updated in February 2016 and is in draft format. Although 49 risks are documented, some are documented at a very high level (e.g. 'Risk of fraud' or 'risk that students will not be retained') and are not very clear or specific; as such it is difficult to pinpoint the actual risk being identified. Risk definitions should be concise, self-explanatory and should deal with one risk only. The risk register is not comprehensive or complete in all cases. Some members of management indicated that not all risks were captured on the register. In addition while the register has columns for key information on each risk, however not all fields are populated (e.g. the risk score or action is not included for all risks). 	<ul style="list-style-type: none"> Conduct a risk identification and assessment exercise amongst all Business Units. To this end consider scheduling a formal risk identification and assessment workshop session with the management teams and relevant stakeholders. This should facilitate a group discussion around risk and ensure all risks are identified. Leverage the existing risk register as an input into this workshop and use this as an opportunity to reword and revise the way risks are currently worded. Review the wording of risks to ensure the risk identified is concise and clearly defined. As part of the risk workshop formally assess risks with clear pre-defined criteria for impact and likelihood assessment. An output from this workshop should be a revised and updated risk register which should include risk owners for each risk. This should form the basis for regular risk reporting and monitoring as part of the risk governance framework. Develop a more comprehensive set of impact criteria (e.g. financial, reputation, operational) and 	<p><i>The Draft update of the Risk Register prepared in February 2016 will be finalised by scheduling a risk identification & assessment workshop with the management groups.</i></p> <p><i>As part of the workshop we will:</i></p> <ul style="list-style-type: none"> <i>Review and refine risks, where appropriate, to give greater clarity to the actual risk being identified;</i> <i>Identify and record additional risks;</i> <i>Assess risks identified using a clear pre-defined criteria for impact and likelihood assessment; and,</i> <i>Assign risk owners for all risks.</i> <p><i>Once this initial risk identification and assessment exercise is complete we will ask risk owners to consider and identify the existing controls that are in place to mitigate or reduce the risk score / rating.</i></p> <p><i>They will also be asked to identify any further actions which may need to be taken to address each risk or to improve the effectiveness of the existing control.</i></p>

<ul style="list-style-type: none"> ▪ The risk scoring criteria definitions are not clearly understood by all stakeholders interviewed. The impact and likelihood criteria are not supported with clear descriptions of financial, qualitative or timelines which would aid in measuring the actual impact or likelihood for each risk. 	<p>likelihood (e.g. percentage chance of occurring and timescales to occurrence) criteria to support consistency of the risk assessment.</p> <ul style="list-style-type: none"> ▪ Once ITB has completed an updated formal risk identification and assessment exercise, consider introducing the concept of net or residual risk assessment by considering the effectiveness of existing controls. 	<p>Target Date</p> <p><i>31 January 2017</i></p> <p>Responsible Party</p> <p><i>The member of the TMG nominated in finding 1 above.</i></p>
---	---	---

3. No formal process in place for regular risk monitoring and reporting (Grade 2)

Risk mitigation, monitoring and reporting: Risk mitigation centres on the actions taken to reduce or eliminate the impact or likelihood of occurrence of an identified risk. Risk monitoring and reporting forms a critical part of a Risk Management Framework which should be a planned part of the risk management process.

Current Practice

The Risk Management Policy states: “*Comprehensive and regular reporting is designed to monitor key risks and their controls*”. The Risk Register contains columns for details of controls, control ratings, actions required and specified timelines for each risk. Control effectiveness ratings are defined as effective, partially effective or ineffective. Additional ratings for IT controls are included in a numerical format in the risk register.

Findings	Recommendations	Management Action Plans
<ul style="list-style-type: none"> There is no formal process in place for monitoring and reporting risk to Governing Body, the Audit Committee, TMG or Croí. There is also no formal process for monitoring and reporting significant changes to the risk environment and agreeing on remediation plans. 	<ul style="list-style-type: none"> Agree on a risk reporting template and content which can be used at TMG, Audit Committee and Governing Body meetings. Consider developing a risk heat map or summary risk report which can be used on a regular basis for Audit Committee / Governing Body highlighting the top and fastest moving risks. Complete a formal quarterly review at TMG to update the Risk Register for changes in the risk profile and environment. 	<ul style="list-style-type: none"> Develop appropriate reporting templates based on best-practice examples in use Recommendation accepted for quarterly review – probably adopting a rolling review method ensuring critical risks are reviewed quarterly and all risks reviewed at least annually. <p>Target Date</p> <p>31 January 2017</p> <p>Responsible Party</p> <p>The member of the TMG nominated in finding 1 above.</p>

4. Risk Management Policy requires updating and risk appetite not formally defined (Grade 3)

Risk Strategy & Policy: A Risk strategy and policy defines the way in which an organisation undertakes risk management. It demonstrates how the management of risk, risk appetite and tolerance enables an organisation to reach its business objectives. The balance of risk and reward that the organisation is willing to accept is known as its risk appetite.

Current Practice

A Risk Management Policy has been formally documented for ITB (dated 2 August 2009, version 01). The Policy forms part of ITB's internal control and corporate governance arrangements. It sets out the Institute's key principles for the risk management process and defines roles and responsibilities of Governing Body, and the management team with respect to risk and its management. The business and operating environment is well understood by the Top Management Group. There is an appreciation and awareness of risk and the risk management as part of day-to-day operations within the Institute.

Risk management is viewed as part of the Institute's system of internal control and the approach for the annual review of effectiveness of internal controls. The key risks facing the Institute are considered and form part of the development of ITB's overall business plans and strategy. TMG and the Department Heads are responsible for the risks under their control and within their functional area.

Findings	Recommendations	Management Action Plan
<ul style="list-style-type: none"> The Risk Management Policy is in draft (dated 2009) and has not been updated or reviewed since. In addition it has not been formally approved by Governing Body. Based on the current Risk Management Policy, Governing Body should “determine the appropriate risk appetite”. While the risk appetite is understood to be low within ITB, it is not formally defined or documented. Given the nature of its operations the Learning and Innovation Centre (LINC) may have a different risk appetite. A number of gaps were identified with respect to the draft Risk Management Policy; specifically it does not include key risk definitions, risk categories and what the detailed risk management process is within ITB. This should specifically set out the risk identification and assessment processes including the risk scoring criteria to be used. 	<ul style="list-style-type: none"> Review and update the Risk Management Policy to include the items mentioned above. As part of this process agree on the risk management process (i.e. risk identification, risk assessment and scoring criteria) to be followed in ITB. An example Risk Management Policy is set out in Appendix C for reference. Consider defining and documenting a formal statement of risk appetite. At the outset explore with the TMG and articulate a draft statement of risk appetite which can then be reviewed and refined over time with the Audit Committee and Governing Body. Ensure the Policy is formally approved by Governing Body and communicated across the Institute as required. Ensure it is reviewed at least annually, or as necessary in response to changes in the business or risk profile of the Institute. 	<ul style="list-style-type: none"> Update the existing Risk Management Policy based on appropriate best-practice guidelines and incorporating the issues raised in Items 1-3 above (Target date: 31 October 2016) Develop a formal statement of risk appetite for presentation to Audit Committee and Governing Body (Target date: 31 October 2016) Recommendation accepted (31 October 2016) <p>Responsible Party</p> <p>The member of the TMG nominated in finding 1.</p>

5. No regular risk management training given to staff (Grade 3)

Risk Culture is the system of values and behaviours present that help shape risk decisions i.e. the risk and compliance implications of the organisation's culture, expressed perhaps as "the way we do things around here". The culture reinforces the principle of 'doing the right thing' and is typically supported with training.

Current Practice

There is a positive culture in the Institute around improving the management of risk and there is a good awareness of risk, risk management and the importance of actively managing risk as part of day-to-day operations. The Secretary / Financial Controller has taken on responsibility for driving the updating of the risk registers in ITB.

Findings	Recommendations	Management Action Plan
<ul style="list-style-type: none"> Although the Secretary Financial Controller has taken on responsibility for driving the updating of the risk register, the absence of a formally nominated individual with responsibility for the risk management process may result in a lower profile across the Institute and less awareness of the importance of risk. There is no regular risk / risk management training provided to staff within the Institute. 	<ul style="list-style-type: none"> As indicated earlier, formally nominate a person at senior level with overall responsibility for the risk management process. Once the Policy and risk management process is agreed and updated, provide risk training as appropriate to staff throughout the Institute. Ensure that a risk training briefing session is provided on at least an annual basis, either on its own or as part of other regular staff updates or briefings. 	<ul style="list-style-type: none"> One member of the ITB Senior Management (TMG) group will be nominated as the person with overall risk management responsibility for the Institute. (Target date: 30 September 2016) Recommendation accepted (31 January 2017) <p>Responsible Party</p> <p>The member of the TMG nominated in finding 1 above.</p>

Appendices

Appendix A – Assigning Ratings for Findings

Appendix B – List of Personnel Interviewed

Appendix C – Example Risk Management Policy

Appendix D – Example Risk Governance Structure

Appendix A – Assigning Ratings for Findings

Rating	Basis of our classification
Grade 1	<p>A critical weakness which could compromise internal controls potentially resulting in significant loss to the Institute or which could be interpreted as a critical weakness in the governance oversight function of the Institute and which should be addressed as a matter of urgency.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Critical impact on operational performance e.g. resulting in major disruption to Institute or inability to provide a quality service to students for more than 3 days, or leading to a loss of the majority of students; <i>or</i> • Critical monetary or financial statement impact; <i>or</i> • Critical breach in laws and regulations e.g. resulting in material fines, penalties being levied on the Institute or funding being withheld; <i>or</i> • Critical impact on the Institute's reputation or brand e.g. resulting in sustained adverse national and/ or international media coverage and political reaction
Grade 2	<p>A control weakness which could undermine the system of internal controls and / or operational efficiency and should be addressed within three months.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Substantial impact on operational performance e.g. resulting in disruption to the Institute or inability to provide a quality service to students for up to 3 days, or leading to a loss of a significant number of students <i>or</i> • Substantial monetary or financial statement impact; <i>or</i> • Substantial breach in laws and regulations e.g. resulting in substantial fines and consequences; <i>or</i> • Substantial impact on the Institute's reputation or brand e.g. resulting in unfavourable national, or local media coverage, or a significant number of student complaints
Grade 3	<p>A weakness which does not seriously detract from the system of internal controls and / or operational efficiency but which should nevertheless be addressed by management within six to 12 months.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Moderate impact on operational performance e.g. resulting in limited disruption to Institute or inability to provide a quality service to students for up to 4 hours, or limited impact on students; <i>or</i> • Moderate monetary or financial statement impact; <i>or</i> • Moderate breach in laws and regulations with no fine, and no regulatory investigation; <i>or</i> • Moderate impact on the Institute's reputation or brand e.g. resulting in limited media coverage, or some student complaints
Observation	<p>A finding that does not detract from the system of internal controls and / or operational efficiency but which should be addressed by management within 12 to 18 months. Findings in this category can be raised to highlight areas of inefficiencies or suggested good practice.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Minor impact on operational performance e.g. resulting in disruption of non-core activities for up to 2 hours; <i>or</i> • Minor monetary or financial statement impact; <i>or</i> • Minor breach in laws and regulations; <i>or</i> • Minor impact on the Institute's reputation e.g. resulting in no media coverage and no student complaints.

Appendix B – List of Personnel Interviewed

We met with, or obtained information from, the following people throughout the course of our review.

Name	Title
Mr. Richard Gallery	Registrar
Mr. Denis Murphy	Secretary Financial Controller
Dr. Brian Nolan	Head of School of Informatics & Engineering
Ms. Assumpta Harvey	LINC Manager
Mr. Dave Curran	IT Manager

Appendix C – Example Risk Management Policy

1. Purpose of this document

- 1.1 The policy forms part of the XXX's internal control and governance arrangements.
- 1.2 The policy defines XXX's policy on the way that risks are identified and dealt with within XXX's. It explains XXX's underlying approach to risk management and the processes adopted to manage risk. In addition it articulates XXX's risk appetite including the level and nature of acceptable risk and provides a common risk language including risk definitions and categories. It also sets out the key roles and responsibilities for risk management and identifies the main reporting procedures.

2. What is Risk Management?

- 2.1 Risk Management is a formal process which involves:
 - identifying the various risks which affect an organisation;
 - assessing the risks in terms of impact and likelihood;
 - identifying actions to mitigate or reduce risk to a level which is acceptable to the organisation and within the overall risk appetite; and,
 - monitoring and periodic reporting on the status of risk.

3. Risk Definitions

- 3.1 **Risk** is defined as:

“... the chance of something happening that will have an impact upon the achievement of objectives. It is measured in terms of impact and likelihood. . .”

- 3.2 Risks can be considered under the following headings:

- **Hazards:** - the possibility of bad things happening with adverse consequence for the organisation e.g. natural disaster such as fire or flooding, criminal or terrorist attack, or the failure of a system or process.
- **Uncertainties:** - possible variations from expectations which could arise as a result of internal or external factors affecting the performance of the organisation. Examples could include problems recruiting new staff, economic downturn or competitive forces.
- **Opportunities:** - ways in which performance can be improved e.g. continued investment in upgrading technology.

- 3.3 Risks, by their very nature, may or may not occur and fall into a variety of categories. The organisation categorises its risks under 4 main categories:

- **Strategic Risks:** - the inability to achieve the organisation's strategic and operational objectives as set out in the Strategic Plan and also, not availing of opportunities when they arise;
- **Operational Risks:-** the inability to prevent a loss resulting from inadequate internal processes and systems;
- **Financial Risks:-** exposure to losses arising as a result of the need to improve the management of the organisation's financial assets;
- **Reputational Risks:** - exposure to losses arising as a result of bad press, negative public image and the need to improve stakeholder relationship management.

4. *Underlying approach to Risk Management*

4.1 The following key principles outline the XXX's approach to risk management and internal control:

- the Board has overall responsibility for overseeing risk management within the organisation as a whole
- an open and receptive approach to solving risk problems is adopted by the Board, Audit and Management Committees
- staff support, advise and implements policies approved by the Board/Audit Committee
- all staff are responsible for encouraging good risk management practice within their areas of work
- key risks will be identified by the Board/Committee/key employees and closely monitored on a regular basis.

5. *Risk Management Process*

[Outline each aspect of the Risk Assessment Process (i.e. risk identification, risk assessment including scoring criteria etc.) in more detail below]

6. *Risk Appetite*

- 6.1 Risk appetite describes the balance between the willingness to live with a risk and the expected cost of reducing it given the likelihood and forecast impact. Viewed another way risk appetite is the organisation's tolerance for risk.
- 6.2 The approach to risk taking is conservative except in the areas of research and strategy. Risks scoring up to X may be tolerated in these areas. Risks scoring above X in other areas should not be tolerated and steps should be taken to reduce the risk to acceptable levels. Risks being carried above the appetite level should be brought to the attention of the Board immediately they are identified.

7. *Role & Responsibilities*

[In this section outline the responsibilities of key parties including the Board, the Audit Committee, the Risk Management Committee as well as the role of staff.]

- 7.1 **The Board:** - Overall responsibility for the management of risk within the organisation lies with the Board. The Board will approve the organisation's Risk Management Policy, will satisfy itself through its Audit Committee (& Management's Risk Management Forum) that an adequate Risk Management Framework is in place in the organisation and that key risks are being managed appropriately. Its role is to:

- a. Set the tone and influence the culture of risk management within the organisation. This includes:
 - communicating the organisation's approach to risk
 - determining what types of risk are acceptable and which are not
 - setting the standards and expectations of staff with respect to conduct and probity.
- b. Determine the appropriate risk appetite or level of exposure for the organisation.
- c. Approve major decisions affecting the organisation's risk profile or exposure
- d. Annually review the organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

7.2 Audit Committee: - The role of the Audit Committee is to assure the Board that an adequate Risk Management Framework is in place in the organisation. In providing the required level of assurance, the Audit Committee will:

- a. Keep under review, and advise on, the operation and effectiveness of the organisation's Risk Management Framework;
- b. Ensure that assurance provided by management and external/internal auditors is appropriate; and,
- c. Monitor the effectiveness of Risk Management in relation to risks identified as key to the success or failure of the organisation's strategic objectives.

7.3 Risk Management Forum : - The Risk Management Forum is responsible for:

- a. Ensuring the communication of the key elements of the organisation's Risk Management Framework;
- b. Maintaining the organisational Risk Register, including its review and up-date on a regular basis;
- c. Supporting the embedding of risk management and the development of a risk-aware culture; and,
- d. Reporting to the Audit Committee/Board on the organisation's risk register and the implementation of the Risk Management Framework.

7.4 Internal Audit: - Internal Audit is responsible for the review of internal controls within the organisation. In developing its Annual Internal Audit Plan cognisance will be taken of the Risk Register. The internal audit reviews will include an assessment of the Business Unit's effectiveness of their respective risk management processes and will provide independent assurance to the Board, through its Audit Committee, that risks are being managed appropriately.

8. Annual Review of Effectiveness

8.1 The Board/Committee is responsible for reviewing the effectiveness of internal control of the organisation, based on information provided by the senior employees. Its approach is outlined below.

8.2 For each fundamental risk identified, the board will:

- review the previous year and examine the organisation's track record on risk management and internal control
- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

8.3 In making its decision the Board/Committee will consider the following aspects:

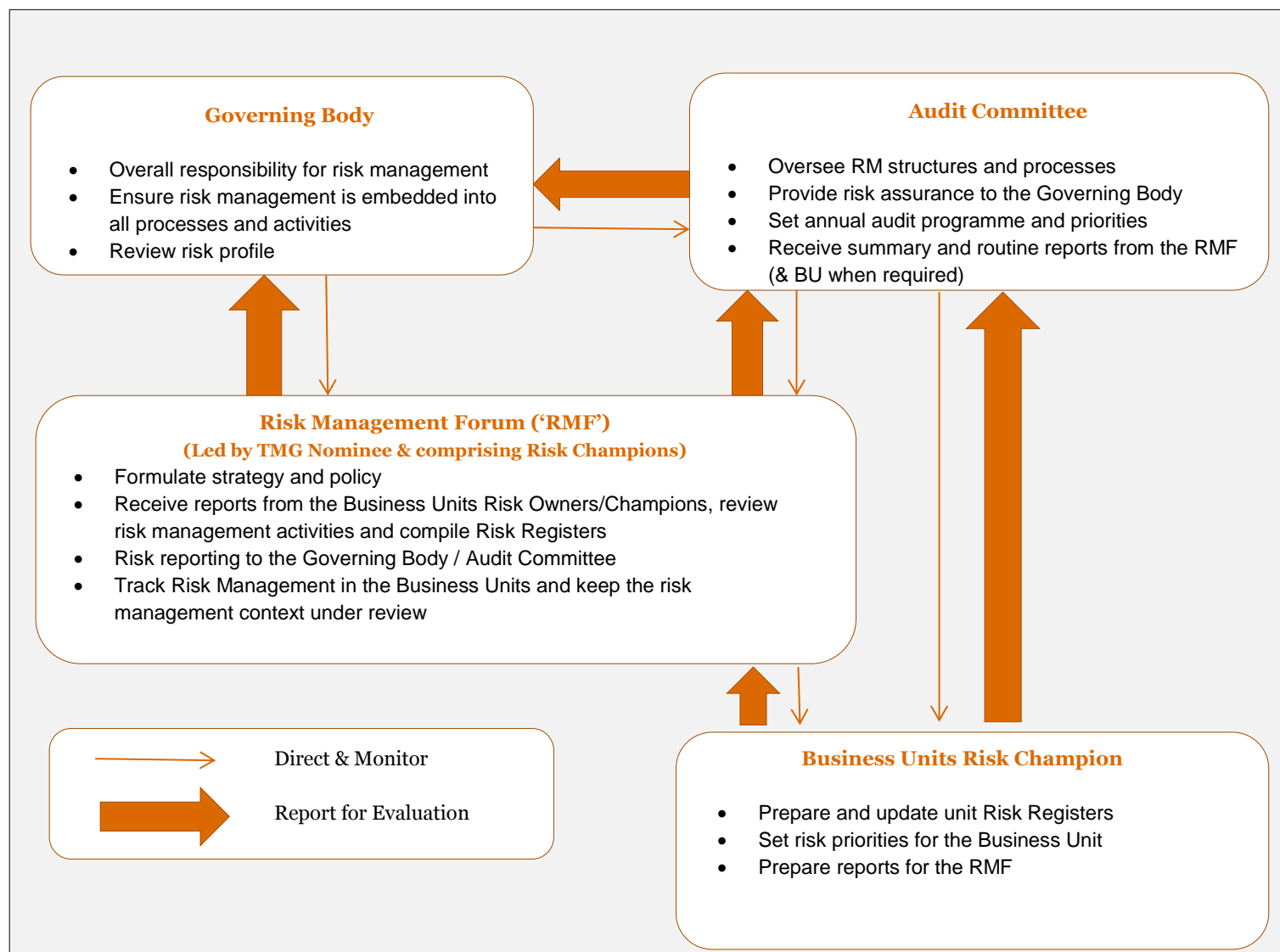
- a. Control environment:
 - the organisation's objectives and its financial and non-financial targets
 - organisational structure and calibre of the staff

- culture, approach, and resources with respect to the management of risk
 - delegation of authority
 - public reporting.
- b. On-going identification and evaluation of fundamental risks:
- timely identification and assessment of fundamental risks
 - prioritisation of risks and the allocation of resources to address areas of high exposure
- c. Information and communication:
- quality and timeliness of information on fundamental risks
 - time it takes for control breakdowns to be recognised or new risks to be identified
- d. Monitoring and corrective action:
- ability of the organisation to learn from its problems
 - commitment and speed with which corrective actions are implemented
- 8.3 The delegated member of staff responsible for risk management will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the Board/Committee.

9. Policy Review

- 9.1 The Policy Owner has been delegated authority from the Board for this Policy. The Policy Owner will review the policy annually in order to ensure that it remains fit for purpose and complies with all relevant requirements. If necessary, the Policy will be updated between annual reviews.
- 9.2 Any amendment to this Policy will require the formal approval of the Board.

Appendix D Example Risk Governance Structure



www.pwc.com

Confidential information for the sole benefit and use of Institute of Technology Blanchardstown.

© 2016 PricewaterhouseCoopers. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

Please see www.pwc.com/structure for further details.