The Institution of Engineering and Technology

Paper Number
T(20)48

26 May 2020

PAPER CLASSIFICATION: OPEN

Board of Trustees

RISK STRATEGY AND APPETITE

(Paper by Emily Meek, Compliance and Risk Management Officer, and Dom Pickersgill, General Counsel. If you have any questions on this paper before the meeting please contact Emily Meek on 01438 765674 or by email emilymeek@theiet.org)

1. Issue

The Risk Strategy requires an annual review and approval by the Board of Trustees.

2. Timing

Board of Trustees meeting, 5 June 2020.

3. For Recommendation

3.1. The Board of Trustees is invited to review and approve:

3.1.1. the updated Risk Strategy document set out in Appendix A;

3.1.2. the proposal for further information on risk appetite to be included within the Risk section within Board and Committee papers as set out in Appendix B.

4. Background

4.1. The Risk Strategy is a standing item on the Board of Trustees agenda for its June meeting.

4.2. The Board of Trustees first approved an IET Risk Strategy in October 2016 and reviewed and approved minor amendments in November 2018 and June 2019.

4.3. It was requested by the Board of Trustees during the approval process in November 2018 that the risk appetite statement is reviewed, and a more detailed version is considered.

4.4. Following an initial risk appetite survey of Trustees, a Risk Appetite Working Party was established. Minute 12.3 of T(19)M4 refers: “It was agreed to set up a Risk Appetite Working Party to conduct a review of the current risk appetite, examine the results of the recent survey, and make recommendations to the Board of Trustees on the next steps to achieve a more satisfactory risk appetite statement.”

4.5. A Working Party was set up and one virtual meeting was held. The results of the survey were deemed inconclusive and the current risk appetite was discussed. Unfortunately, due to the lack of external best practice, insufficient progress was made on creating a workable solution and therefore no recommendations were made to the Board of Trustees from the Working Party.

4.6. Following the appointment of Crowe as the new internal audit co-sourced partner, it became possible to access their expertise on reviewing risk management processes. Through discussions of the IET requirements, a concept, definitions and approach was created, which is described within this paper, to help consider risk appetite during decision making.

5. Key Points

5.1. There are small amendments proposed to the Risk Strategy. The amended version is shown in Appendix A.

5.2. The concept, definitions and approach for operationalising risk appetite is included in Appendix B.

5.2.1. The recommendation is to expand the risk section within Board and Committee papers to clarify what the risk appetite is for that item – Risk Averse, Risk Balanced and Risk Seeking. Appendix B includes an overarching definition of these, as well as more detailed definitions for the following four areas – Financial, Activities, Regulatory and Reputational.

5.3. If the overarching concept and approach is agreed, it is proposed that the Audit and Risk Process Committee is delegated with the authority to approve the more detailed operational process of how this will be approved within the Risk Management Manual and timescales for implementation.

6. Risk

If our risk appetite is not clearly defined we risk both exposing ourselves to more risk than we can control, and also missing opportunities in areas we wish to pursue.

7. Resources

No additional resource is required.

The Institution of Engineering and Technology

IET Risk Strategy

1. Background

Any organisation faces risks in its activities. Responsibility for the IET's activities, and the risks that go with them, ultimately sits with the Board of Trustees (BoT).

The IET Risk Strategy outlines the IET's approach to managing risk, which we define as:

"The opportunities and uncertainties which may impact on the IET's ability to deliver its Vision, Mission and Strategy or which may jeopardise the IET's compliance with legal, contractual and regulatory requirements."

The Risk Strategy outlines the way in which the BoT leads, directs and oversees the IET's risk management which helps underpin the delivery of the IET's overall strategy and supports the IET's reputation and performance.

Risks must be understood and an effective and integrated system of risk identification, assessment and management must be implemented throughout the IET. The risk of missing opportunities must be considered as well as risks that are more commonly recognised, such as financial and reputational risk, which may impact on the IET.

The IET Risk Strategy is supplemented by the IET Risk Management Manual setting out the practical details of how risk will be identified, assessed, recorded and managed by the Executive and staff.

The IET Risk Strategy will clarify the IET's approach to risk; the Risk Management Manual sets out how risks are identified and managed.

2. The IET's integrated approach

Risks occur at every level of the IET and therefore the understanding of and management of risk must also exist throughout the Institution. The focus is on the risks themselves and the management of them and it is the culture of the organisation which will determine the success of achieving an integrated and effective approach, where considering risk is part of business as usual for all levels of staff and management. Integration is consistent with the IET values of Integrity, Excellence and Teamwork. The systems used for identifying and recording risk, for example the Strategic Risk Register, are tools to assist in and record risk; but merely using the tools does not manage risk.

Within the IET everyone should understand how they are required to contribute to managing risk through a culture of speaking up; openly discussing and identifying risks; and being able to challenge, regardless of role or position. Staff must think about issues which may be barriers or facilitators to success in their work. The Risk Strategy and Risk Management Manual enhance understanding of risk and provide a consistent approach.

A culture of openness will lead to risk management being integrated into business as usual. Focus should be on the quality of discussions about risk, not the tool used to record them.

3. The Purpose of Risk Management

The IET undertakes coherent risk management practices to give consistency and sustainability to the delivery of the Vision, Mission and Strategy, to support the Institution's values and to ensure compliance with legal, contractual and regulatory requirements. Effective risk management facilitates well-considered risk taking in the context of an agreed strategy and in the development of strategic opportunities.

Effective risk management enables a better approach to taking opportunities.

4. Roles and Responsibilities for Risk

The Board of Trustees

The BoT has overall accountability for risk management, and delegates responsibility for managing risk to the Executive Committee and staff. A fundamental aspect of risk management is assurance that appropriate systems of controls and actions are in place, along with a robust and transparent reporting mechanism for strategic risk. The Board achieves this by having effective oversight procedures in place. In addition to the identification of strategic risk, which is a joint responsibility with the Executive Team, the BoT will receive an overview of strategic risk on a quarterly basis for their consideration, with a particular focus on any emerging risks to the current IET strategy or objectives or on strategic risks that are above the level of tolerance.

The Audit and Risk Process Committee

The Audit and Risk Process Committee is an integral part of risk oversight and assurance for the BoT. The Committee reviews the Strategic Risks and also determines work to be undertaken by Internal Audit.

The Finance and Investment Committee

The Finance and Investment Committee takes responsibility for the oversight of the financial performance of the Institution and proposes options for timely actions to mitigate risks to satisfactory financial performance.

Internal Audit

The Internal Audit function supports the BoT in providing assurance, evaluation and improvements to the effectiveness of the IET's risk management, control, and governance processes. Internal Audit reports directly to the Audit and Risk Process Committee.

Main Boards

The main boards (Knowledge Services and Solutions Board, Membership and Professional Development Board and the Volunteer Engagement Board) which report to the BoT have oversight of the activities of the IET's Directorates and work with the BoT and Executive to manage strategic risk and with the Executive to manage operational risk.

Council

The IET Council is separate from the BoT and has within its remit the role of monitoring governance.

The Executive Team

The day-to-day oversight and management of risk is dealt with by the Executive, who lead and encourage good, sound risk management practices.

All Staff

All members of staff have an important role to play in identifying, assessing and managing risk. To support staff in this, and consistent with its values of Integrity, Excellence and Teamwork, the IET nurtures a fair, open, consistent and non-judgemental culture reflecting a willingness to be open and honest and to report any situation where things have, or could go wrong. All members are able either to speak to their manager(s) or, they may consult the Legal and Compliance Team who will help them assess the risk and consider appropriate steps.

The IET Project Office

The Project Office provides support to all of the IET's projects. It provides a framework for recognising and managing risk across all projects.

Everyone has a role in the IET's risk management.

5. Risk Management Operations

The IET has established a risk management function as part of the Legal and Compliance Team, which reports into the Director of Governance and External Engagement.
Support for the identification and management of Strategic Risks is also provided by the Strategic Planning Manager.

The IET's governance framework includes an Audit and Risk Process Committee whose terms of reference include: '*to review management's and the internal auditor's reports on the effectiveness of systems for internal financial control, financial reporting and risk management*."

Risk management is a standing item on the agenda for Board of Trustees meetings through the Chief Executive's Report on Risks, and at the Audit and Risk Process Committee
The IET maintains a Risk Management Manual which outlines in detail the systems maintained and roles in place to manage risk.

The risk management operations are designed to ensure good governance and monitoring of risk. However, everyone has a role in the *management* of risk.

6. Risk appetite and tolerances

Active management of our risk appetite (the risk that the IET is willing to take on) and risk tolerance (the level of risk which is acceptable in our activities) is the technique used to control how much risk our organisation is willing to accept. Where the current level of risk exceeds the risk appetite, the relevant activity will need to be reviewed and consideration given to mitigating the risk further or taking other action such as stopping the activity.

The IET is a charity and it is important that the IET safeguards its position in the longer term to deliver against its charitable purpose. We therefore have a very limited appetite for risks in respect of our reputation but a higher risk appetite for developing products and services which respond to the changing needs of society, and the engineering and technology community. The Board of Trustees is therefore keen that the IET is able, where appropriate,

to take advantage of opportunities to increase its positive impact while managing risk proactively.

When thinking about appetite itself, for simplicity purposes, the following three overarching categories can be considered:

Category	Overarching definition
Risk Averse	Avoidance of risk and uncertainty is a key organisational objective
Risk Balanced	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
Risk Seeking	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)

Then, when the risk appetite of different decisions and actions is considered, these are then applied across four core areas (financial, activity, regulatory and reputational), with the criteria applied based on the nature of the activity.

In view of the breadth of operations within the IET, there will inevitably be a variation in appetites and tolerances to risk across the different areas within the IET and the risks facing the organisation. For example, our appetite for taking strategic risks could vary considerably depending on whether it relates to compliance, finance, people, innovation (which could fall into two categories, one relating to our charitable purpose, and the other to our non-primary purpose activities, usually falling within our trading subsidiaries), or reputation.

The IET's risk appetite and tolerance in these and any other areas should be considered by the BoT when considering Strategic Risks.

The risk appetite and tolerance will vary according to the area of risk and there is no overall level across the IET. Risks will be considered individually and contextually to identify the level of appetite. The IET should be able to take advantage of opportunities to increase its positive impact while managing risk effectively.

7. Types of Risk

Risks are managed within three different categories: Strategic, Project and Operational.

Strategic Risks are those which may impact on the ability of the IET to deliver the Vision, Mission and Values and the IET Strategic Priorities. A strategic risk may occur from an external source and at a macro level, for example, the introduction of new legislation which impacts on the IET's ability to deliver key functions or operate in a particular jurisdiction; or a change in policy by the Engineering Council.

Alternatively, a strategic risk could relate specifically to the IET, for instance significant reputational damage could prevent the IET from fulfilling its influencing or thought leadership functions. Strategic risks often arise from external factors. The oversight of strategic risk rests with the BoT.

Project Risks are those that may impact on the ability of the IET to deliver a successful project.

Operational Risks are those which may impact the delivery of particular operations or services, such as poor staff retention or revenue from a particular product or service. Operational risks can still raise challenges for the IET's delivery of its strategy, but they are

unlikely to do so in isolation. Operational risks are managed within the Directorates of the IET.

Project and operational risks may escalate or crystallise individually or cumulatively to become strategic risks if they impact the IET's ability to deliver the Vision, Mission and Values and the IET Strategic Priorities.

The IET categorises risk as Strategic, Project and Operational. Risks evolve and should be regularly reviewed to check they are categorised correctly.

8. Identifying Risks

Identifying Strategic Risks

The Risk Management Manual outlines the methods used to identify strategic risks. A key element in the IET's integrated approach to risk is that risk will be considered and debated by both the BoT and the Executive. New risks can occur at any time and therefore strategic risks will be considered and reviewed on an ad hoc basis, as relevant, but existing risks will be reviewed at least annually.

Identifying Project Risks

Project risks should be identified and discussed during the project planning process and as they arise during the course of project implementation. Once a project has been completed, any remaining risks will be passed to the relevant department as operational (or strategic) risks.

Identifying Operational Risks

Responsibility for the identification and management of operational risks rests with the staff team, under the oversight and direction of the Executive and the Extended Leadership Team. The Risk Management Manual outlines the tools available to support risk identification but establishing a culture where staff are encouraged to discuss risk and speak out is the most important factor in identifying and managing operational risk.

Risk identification will take place throughout the IET in a continuous process and is <u>not</u> a once a year event.

9. Assessing Risk

Where a risk is identified, it will be assessed and consideration given to the likelihood of something happening and the impact it would have if it did. The appetite and tolerances for the risk will then be considered: is it a risk which the IET is willing to accept at its current level or is it one where steps should be taken to further control, mitigate or avoid the risk?
Controls should be considered to bring the risk to an acceptable level, by reducing the likelihood of an event or by mitigating its impact. "Impact" may be measured in financial terms or non-financial terms such as reputation loss or reduced standards of service. The risk should be re-assessed on a regular basis to ensure the effectiveness of control measures in place. If an identified risk comes to pass, the controls must be reviewed to see what measures can be implemented to prevent or better mitigate any recurrence.

The risk must be assessed for likelihood of occurrence and the potential impact on the Institution and its members and appropriate controls considered and implemented to enable the IET to take advantage of opportunities to increase its positive impact.

10. Risk Mitigation Tools

The IET has in place a number of risk mitigation tools to help both the assessment and monitoring of risk though appropriate levels of monitoring. The key tools are mentioned below.

a. **An open culture** – being able to talk about risk. "Setting the right principals and tone from the top, ensuring staff understand the risk appetite and desired behaviours"

b. **Good governance** – a robust structure of oversight and challenge, led by the Board of Trustees.

c. **The IET Strategic Risk Register** – used to support the identification, review and reporting of strategic risks.

d. **Your Directorate's own Operational Risk Register -** – used to support the identification, review and reporting of your Directorate's operational risks.

e. **The IET Risk Management Manual –** providing practical guidance on how to manage risk at the IET.

A range of tools will be provided to help assess and mitigate risk.

Approved by the Board of Trustees June 2019

Appendix A

Control Sheet

Risk Strategy Policy

Document owner: Dom Pickersgill
Document reviewer: Emily Meek and Dom Pickersgill
Document adopted on: 1 October 2016
Next review date: 1 June 2020

Review/change history

Date of Review/Change	Summary of changes	Version no.
October 2016	First Version – Dom Pickersgill	1.0
October 2018	Draft amends ready for approval by Board of Trustees – Emily Meek	1.1
May 2019	Updated logo and control sheet to fit current policy template style. Other minor amends ready for approval by Board of Trustees – Emily Meek	1.2
May 2020	Draft amends ready for approval by Board of Trustees	1.3

IET Operationalising Risk Appetite

Summary

This paper proposes a new concept, definition and approach to risk appetite which looks at clarifying definitions and including an enhanced Risk section on Board and Committee papers.

1. Background

The Risk Strategy and the Risk Management Manual both contain an outline of the current approach to Risk Appetite (see Appendix).

However, it has been reported that Risk Appetite and Tolerance as a concept has struggled to gain traction within IET. As such, this paper sets out a proposed approach to "operationalise" and embed risk appetite into decision making.

2. Risk Appetite Approach

In determining the approach, and aligning to the existing risk management process, we are proposing the following approach.

2.1 Clarifying Definitions

2.1.1 Target Risk Assessment

Include (as is currently the case) the controlled risk assessment in the Strategic Risk Register but to rebadge this as the "Target Risk Assessment". This will help to inform clarity as to what this metric is, i.e. the impact/ likelihood risk score which is aimed for if the risk is being managed in line with appetite. Use of the terms appetite and tolerance within the Risk Strategy and Risk Management Manual will also be reviewed to provide further clarity.

Particularly given the current operating environment with Covid-19, it will not always be possible to bring a risk to within the stated risk appetite in the short or even medium term and that a tolerance of some risks above the stated risk appetite will be necessary.

This is particularly the case with risks that could have an effect on Business Continuity and therefore the Impact score of the risk is always likely to be high; even with extensive mitigations to bring down the probability (likelihood) of the risk occurring, it may be difficult to bring the risk to within risk appetite while the Impact score remains high.

2.1.2 Financial Assessment

An element of risk appetite recommended is articulated in more financial terms is how much we are prepared to invest in commercial activities and for what return. In such areas it is possible to have a negative return on investment and the level of funds IET is prepared to put at risk (down side) for a possible return (upside) does need to be articulated.

2.2 Approach to defining risk appetite

When thinking about appetite itself, for simplicity purposes, the following three overarching categories are proposed to be assigned to the risks:

Category	Overarching definition
Risk Averse	Avoidance of risk and uncertainty is a key organisational objective
Risk Balanced	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
Risk Seeking	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)

In terms of applying the categories to different decisions and actions, these are then applied across four core areas when determining risk appetite, with the criteria applied based on the nature of the activity.

Area	Risk Averse	Risk Balanced	Risk Seeking
Financial	Avoidance of financial loss is a key objective. IET will only accept minimal financial exposure from the activity, accepting that this will generate a lower financial return. Return on investment will be achieved in the short term. Supplier/ product selection will focus on the lower cost option.	Prepared to accept possibility of some limited financial loss in order to undertake the activity/event/ service. The return on investment may not be realised until the medium term. Costs of supplier/ product selection remains a primary concern but there is a willingness to consider other benefits or constraints.	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk). It is accepted (but control strategies will be established to identify performance and take remedial action) that there is a higher risk of financial loss or of the return on investment not being realised in the short to medium term.
Activities	Defensive approach to completion of activities – the aim to maintain or protect existing value, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision taking authority. General avoidance of emerging technology developments.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary or of low/medium risk. Decision making authority generally held by Board/ Leadership Team. Systems / technology developments limited to improvements to protection of current operations	Innovation pursued - desire to "break the mould" and challenge current working practices. High levels of devolved authority - management by principles rather than direct oversight. New technologies viewed as a key enabler of operational delivery.
Regulatory	Actions taken to minimise risks of regulatory breach. Zero tolerance mindset to	Balanced approach to regulatory compliance.	Given the potential benefits of the activity to the IET it is accepted that there may be a

Area	Risk Averse	Risk Balanced	Risk Seeking
	regulatory failures. Critical focus is upon compliance rather than financial costs.	 Resources to address compliance are balanced with the associated costs.	higher risk of breach of regulatory requirements to achieve the objective. Resources are prioritised to other areas given the potential regulatory sanction/ penalty.
Reputational	No tolerance for any decisions that could lead to scrutiny of, or indeed attention to, the IET. External interest in the organisation is viewed with concern.	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for IET should there be a failure. Mitigations in place for any undue interest.	Willingness to take decisions that are likely to bring scrutiny of the organisation but where potential benefits outweigh the risks. New ideas seen as potentially enhancing reputation of the IET.

3. Decision Making and papers to the Board and Sub-Committees

As a means of embedding risk appetite, it is proposed that papers being presented to the Board and Committees include consideration of risk appetite (or can be marked as N/A). This would include reference to one or more of the factors in tables above.

For example, when a new initiative is being considered, this will include a corresponding assessment of the Risk Appetite. This can help frame the discussion at the relevant Board or committee.

It may be that there is a recurring event that IET has run for a number of years, which generates a steady income stream and numbers in terms of impact/ attendees. In such instances, the risk appetite will likely remain “Risk Averse” in Financial and Activity terms.

However, with an event designed to target a potential new members and audiences this may fall into the “Risk Seeking” category for both Finance and Activities – where it is accepted that the potential upside is such that the IET may also incur a loss if the event is not a success. In the latter category it is also critical to establish monitoring and measures of success – so that if something is not working then decisions can be taken quickly and losses minimised.

The assessment of risk appetite can be different by category – for example, in the example above, an event/ campaign can be Risk Seeking in Financial and Activity terms, but if it includes school children, can also be Risk Averse in terms of regulatory risk, in respect of safeguarding and data risk.

Appendix

Risk appetite and tolerances (taken from the Risk Strategy and Manual)

Active management of our risk appetite (the risk that the IET is willing to take on) and risk tolerance (the level of risk which is acceptable in our activities) is the technique used to control how much risk our organisation is willing to accept. Where the current level of risk exceeds the risk tolerance, the relevant activity will need to be reviewed and consideration given to mitigating the risk further or taking other action such as stopping the activity.

The IET is a charity and it is important that the IET safeguards its position in the longer term to deliver against its charitable purpose. We therefore have a very limited tolerance for risks in respect of our reputation but a higher risk appetite for developing products and services which respond to the changing needs of society, and the engineering and technology community. The Board of Trustees is therefore keen that the IET is able, where appropriate, to take advantage of opportunities to increase its positive impact while managing risk proactively.

In view of the breadth of operations within the IET, there will inevitably be a variation in appetites and tolerances to risk across the different areas within the IET and the risks facing the organisation. For example, our appetite for taking strategic risks could vary considerably depending on whether it relates to compliance, finance, people, innovation (which could fall into two categories, one relating to our charitable purpose, and the other to our non-primary purpose activities, usually falling within our trading subsidiaries), or reputation.

The IET's risk appetite and tolerance in these and any other areas should be considered by the BoT when considering Strategic Risks.

The risk appetite and tolerance will vary according to the area of risk and there is no overall level across the IET. Risks will be considered individually and contextually to identify the level of appetite and tolerance. The IET should be able to take advantage of opportunities to increase its positive impact while managing risk effectively.

The Risk Management Manual also has an appetite and tolerance section and the inclusion of a chart:

'The risk tolerance is assessed when looking at each individual risk and in the chart in section 10.1 is the controlled risk assessment that managing the risk is aiming for.

Chart from 10.1:

	Uncontrolled Risk Assessment	**Current Risk Assessment**	**Controlled Risk Assessment**
Cost			
Probability	Medium High	Medium Low	Low
Impact	Medium High	Medium Low	Low
Risk Profile	Medium Priority (6)	Low Priority (4)	Low (2)