ANNEX 4A

RISK POLICY

UPDATED 2016

Confidential

Everyone at ICAEW has a responsibility for risk management

RISK | MANAGEMENT AND REPORTING

Introduction

1. Managing risk is a part of everyone's everyday responsibilities. It enables us to make decisions about what we do and how we do things – both strategically and in day to day tasks.

2. We expect everyone to consider risk when planning and managing activities from strategic planning, operational planning through to contract management, project planning and the implementation of these plans.

3. Risk management does not just mean avoiding risks. We need to balance the risks we take with the achievement of our strategic goals – if we take no risks at all we will never achieve these goals.

4. This policy and guidance sets out when you need to report risks including when to discuss risk with senior management, the Board and the Council. It clarifies when a risk is significant enough to be reported to senior management and when it can be managed within a department or team. It is important that only significant risks are escalated. As a general rule, though, if you are not sure – ask. Contacts are below.

5. This document contains:
    - Definition of risk;
    - Our risk appetite;
    - Guidance on how to identify risks;
    - Clarification on how to set the priority of risks;
    - Guidance on how to report risks and who to report them to; and
    - Roles and responsibilities.

Who can I ask about risk?

1. **My line manager**
2. **My departmental business manager**
3. **The Manager, Strategy and Risk (in the Executive Office)**

Version	February 2016
Author	Ben Everitt, Manager, Strategy and Risk
Next review	December 2016

Definition of risk

6. We define risk as **an uncertain event, which will affect the achievement of objectives, if it occurs**[1].

7. A risk needs to be described as what might occur and what effect this might have.

8. A good example of a risk is:

   "There is a risk that breach of system security **leading to** unauthorised access to ICAEW systems and data **resulting in** disruption to operations and reputational damage"

The uncertain event is:	breach of system security
The effect, if it occurs, is:	unauthorised access to ICAEW systems and data
The possible consequence for us:	disruption to operations and reputational damage

Things that are not risks

9. Issues are not risks. An issue is something that is happening now or has already happened. A risk is the potential for an issue to arise.

10. A situation arising through inactivity is not a risk because we can predict that it will happen – it is within our control. This would be an issue.

11. Someone not doing their job properly is not a risk. It is within our control and would be a management issue.

12. Worries are not risks. A worry is something that might happen but the likelihood is so remote that we cannot take any preventative or avoidance actions. It could also be something insignificant, with little impact. This doesn't mean you shouldn't think about worries, or that the things you worry about might not develop into risks if things change – which they often do. If you need help, ask.

13. "Widespread disruption from whatever cause" is too broad to assess for impact on ICAEW and it is not a well-defined risk.

14. Again, if you are not sure what is a risk, ask.

Relationship with project risks

15. Project risks are managed as part of the project management process. They should not be reported as part of the corporate or departmental risk management process.

16. The process for managing project risks is clearly detailed in the Project Management Toolkit[2]. The toolkit and user guide are available on the W Drive:

    Computer > W Drive > Project Management > ICAEW Project Toolkit

17. Project risk registers and benefits registers should be assessed as part of the project closure procedure. Any remaining risks and (dis)benefits that are identified as relevant should be inserted into the appropriate departmental or corporate risk register and dealt with in the normal way.

---

[1] This is taken from the definition of risk of the Office of Government Commerce in their publication: *Management of Risk: Guidance for Practitioners* (*TSO 2007)*

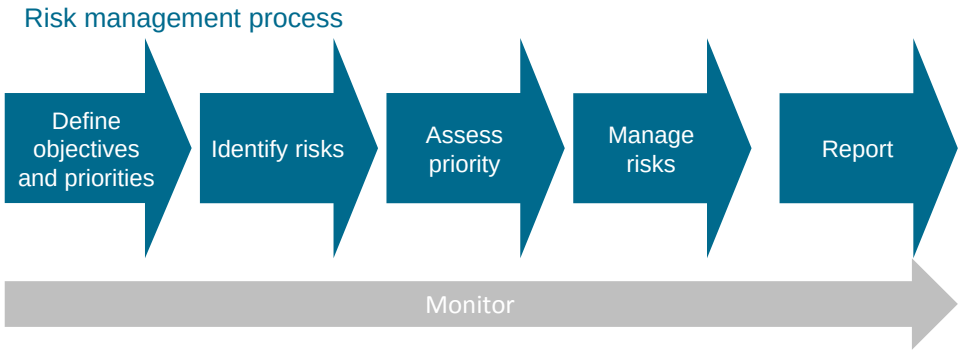
[2] http://icaew.idlive.co.uk/How-to/Manage-projects

Our risk appetite

> At its simplest, risk appetite can be defined as the amount of risk, on a broad level, that an organisation is willing to take in pursuit of value. Or, in other words, the total impact if risk an organisation is prepared to accept in the pursuit of its strategic objectives.
>
> *KPMG – Understanding and Articulating Risk Appetite, 2008*[3]

18. We are a risk-conscious organisation. We understand, explore and manage risk in order to deliver our strategy. Our risk appetite varies across our organisation. What remains the same is that we recognise that every activity that we engage in must uphold and promote our reputation. Our reputation is our ultimate commodity.
19. Our risk reviews (process detailed below) should clearly state the appetite to risk for each reporting department.

Risk management and risk reporting



Define objectives and priorities

20. This is completed as part of the strategic and operational planning processes

Identify risks

21. A risk is normally directly related to a core activity of the organisation and/or a business objective.
22. It's easiest to think about and identify risks when operational activities and objectives are being defined and agreed, i.e., during the operational planning process or when setting out the objectives for a project. Risks can, and should, be identified and acted upon at any time.
23. Identifying risk begins with a clear understanding of the ICAEW strategic activities and objectives, and department objectives. For each activity and objective, we can then consider what might prevent us from achieving our goals. These are the risks.
24. In most cases, this is an intuitive process and part of planning and management of any activity. For risk reporting, these risks need to be formally recorded so that they can be reported and monitored.

---

3 https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/documents/Risk-appetite-O-200806.pdf

25. Risks could come from many sources. We have grouped some risk sources under the AIMS, but these are not the only sources of risk:

ACCESS – Risks that affect our portfolio of qualifications and services, their fitness for purpose, their international reputation and our ability to explore and tap into new markets. Our core business involves attracting students; they train for the ACA and become members for the long term.

INFLUENCE – These include risks to building our reputation, including building key relationships, which allow us to influence the future of the profession in the public interest. Factors could include, but are not limited to:

- The regulatory environment: risks that affect our ability to influence and respond to UK, European and global agendas.
- The economic environment: risks that affect our ability to promote the work of ICAEW, members, firms and businesses.

MEMBERS – The work of our members lies at the heart of our reputation. Factors could include, but are not limited to:

- Risks that affect our ability to grow our membership base, increase awareness of the benefits of membership and evolve our brand.
- Risks that affect our ability to build relationships with our members.

STANDARDS – Our professional standards work is fundamentally about keeping the badge shiny and protecting consumers. We uphold the public interest, maintain standards and the reputation of the profession.

26. Keep the focus of the risk assessment at the right level. If you try to cover too much detail you will be swamped with risks and unable to deal with them.

Assess priority

27. Each risk is assessed for its impact and likelihood. This will enable us to determine whether it is a priority risk or not. The matrix used to assess the risk is shown on the next page.
28. We then consider the possibility of occurrence despite mitigating actions and the likely impact if it did occur.
29. Again, this would normally be an intuitive process – you would know immediately if a risk was high priority, but for risk reporting we need to be able to assess priority on a scale that can be compared between departments and between activities.
30. Even with this guidance, risk priority cannot be easily quantified. A significant amount of judgement is necessary. It is important that staff and management work together to ensure all the relevant risks are identified and prioritised as consistently as possible.
31. If you are not sure, then it is better to escalate the potential risk so that staff and management can work together to ensure all the relevant risks are identified and prioritised as consistently as possible.

32. The overall assessment, or priority, is based upon the combination of the impact and likelihood:

Impact

Likelihood	1	2	3	4
5	Medium	High	High	High
4	Low	Medium	High	High
3	Low	Medium	Medium	High
2	Low	Low	Medium	Medium
1	Low	Low	Low	Medium

Impact

33. The following guidance is there to assist in assigning an impact rating to the risk. The impact banding is set in terms of the impact on ICAEW as a whole and we are focusing on the more significant risks.

	1 Minor	2 Significant	3 Major	4 Critical
ACCESS	Damage to qualifications in specialist area or geographic region with limited take up.	Significant impact on qualifications affecting specialist area or geographic region or degradation to qualifications affecting all students.	Major damage to qualifications that affects the majority of students.	Critical impact on qualifications leading to significant loss of students.
INFLUENCE	Negative impact on our reputation and influence in a country outside of the UK or a contained area within the UK.	Significant negative impact on our reputation and ability to influence in another region outside the UK.	Major damage to UK reputation and influence. Negative national media, regulator or government attention for several days.	Critical damage to global reputation and influence. Sustained, negative media, regulator or government attention.
MEMBERS	Minor damage to our brand, or the reputation of the profession, or more significant damage in a localised area. Damage to the member experience for a small group of members or students, or a minor degradation for all members.	Significant damage to our brand, or the reputation of the profession, in a region outside of the UK. Significant impact on member services affecting some members or significant degradation for majority of members	Major damage to our brand, or the reputation of the profession, the UK or an equivalent region. Major impact on member services that negatively affects a large number of members.	Critical damage to our brand, or the reputation of the profession. Critical impact on member services in the long term leading to loss of major member firms or significant number of members.
STANDARDS	Ability to deliver our role in maintaining standards in the profession is affected.	Significant reduction in our ability to deliver our role in maintaining standards in the profession, such as the loss of some regulatory responsibilities.	Major reduction in our ability to deliver our role in maintaining standards in the profession, such as the loss of key regulatory responsibilities.	Critical impact on ability to maintain standards in the long term leading to loss of major member firms or significant number of members.

Likelihood

34. The likelihood of a risk occurring is defined as follows:

5 Almost certain	The event will occur in all but exceptional circumstances. 80% probability or more.
4 Probable	The event is expected to occur in most circumstances. 50% to 80% probability.
3 Possible	The event should occur at some time. 20% to 50% probability.
2 Unlikely	The event may occur at some time. 5% to 20% probability.
1 Rare	The event may occur at some time, but it would be exceptional. Up to 5% probability

Risk approach

35. When reporting a risk we also need to determine whether the risk is being managed to an acceptable level or not. This is an assessment of whether the risk remaining, with all the controls and other risk management activity in place, is acceptable.

36. In some cases we are seeking to limit or eliminate risk. In other cases we are taking on a risk in order to achieve a goal that has a significant benefit. Risk management is not about avoiding risk, it's about being conscious of what you are doing.

37. Management must judge if a risk is acceptable. This will depend on the description of the risk, its priority and the management activity in place.

    - If a risk is defined as high priority it is unlikely to be acceptable. Exceptionally a high priority risk can be acceptable if there are no possible additional remedial actions available to reduce the risk further. In this case a contingency plan may be necessary to manage the risk if it occurs.
    - Medium priority risks may or may not be within tolerance – this depends on whether the risk requires immediate remedial action or not, or whether the risk is outweighed by the benefits
    - If the risk is defined as low priority it will normally be acceptable.

Manage risks

38. Risks can be managed in many different ways. This activity can include specific controls, insurance, contingency planning, etc. but it's just as likely to be managed by what you consider to be normal activities.
39. When reporting a risk, it's important to describe this activity so that the reader understands what you do.
40. Current management activity means activity that is already in place. This may be on-going activity, e.g., a monthly reconciliation, or something you do on a reactive basis, e.g., implement a contingency plan.
41. If the risk is not within acceptable levels, you must provide details of the additional management activity necessary to reduce the risk further. This must be accompanied by a responsibility and due date (like an action plan).
42. As part of the process of embedding of risk, departments should review their departmental risk register at every departmental team meeting. They should notify the Executive Office of any new principal risks and any changes to corporate or departmental risks which have made them principal risks, for report to Management Team and the Board.

Net Risk Reporting

43. Net risk is the residual level of risk once the risk management activity has taken place. This demonstrates the effect of the activity taken, to mitigate the likelihood and/or impact of the priority risk.
44. Net risk rating provides a clear understanding of how the current risk management activity impacts the priority level of risk and to what degree. Net risk also puts forward the question whether the priority risk can be mitigated further.
45. Some risks, however, can't be mitigated even with feasible actions taken (such as a global recession) because it is out of our immediate control. This will result in net risk equalling priority risk level.

Report

46. Medium and high priority risks must be documented as part of the following processes:

- **Operational planning:** When completing their operational plan, departments must consider risks that will affect their ability to achieve the key priorities for their department.

  The response to these risks will be embedded in their operational activities, key priorities and budgets, but we also need the risks to be clearly specified to enable us to report them. With the operational plan guidelines, departments are provided with two templates to record these risks:

  - The first contains the key risks to ICAEW as identified by the senior management team and departments must describe how they contribute to the management of these risks.
  - The second template is for the department to record the risks that they consider to be of significant priority to them.

- **Strategic priority reporting:** Following the approval of the operational plan, a quarterly update is provided in the strategic priorities report. This details progress made in achieving these key strategic objectives.

  As part of the reporting, departments must include reference to risks. If there is any deviation from target, a specific comment on how you are going to achieve

the overall target for the rest of the year is required. This is a form of early warning report.

- **Project approvals:** Within the standard template for approval of any projects by the Board, there is a section on risk. This includes all kinds of risk to the project and not just financial risks. This section must be completed for all project proposals that go to the Board for approval.

  Once the project has been approved by the Board, the relevant director is responsible for updating their risk register as necessary.

- **Other:** Risk should also be considered as part of any other activity. Specifically, reports to the Board such as the quarterly reforecast and the monthly Executive Director reports should include significant changes in risk.

The risk register

47. The Executive Office will collate the risks reported in the above into a single risk register. The details required for each risk are:

- A description of the risk;
- The inherent likelihood and impact of the risk (i.e. before any mitigating action is taken);
- Current management activity. This can include:
    - Activity to change the likelihood of it occurring, including outsourcing to a third party who can provide more resilience;
    - Activity to change the impact when it does occur, including taking out insurance; and,
    - Acceptance of the risk as it is (i.e., no action).
- Any additional future management activity planned, along with a target date for implementation (an action plan);
- The owner of the risk;
- The owner of the actions to mitigate the risk ('responsibility'), with description of the timescale for reviewing the risk within the context of the current and planned actions; and,
- Net assessment of the risk (i.e. our actual exposure to the risk after the mitigation actions are taken into account).

48. An example of a risk in the risk register is included as an appendix to this document.

49. At least twice a year, the senior management team will review all of the risks on the register and, using the priorities assigned to each of these risks, identify those risks that are of priority to ICAEW is a whole (e.g., principle risks). This will include any risks where the residual risk is not within tolerance and risks that combine to create a significant risk to ICAEW.

50. The Executive Office will produce reports for the Board and Audit Committee on key risks to ICAEW.

Escalation procedures

51. When risks are defined as high priority they are highlighted and reported to the Board and Audit Committee. In addition, any risks identified as not within tolerance are reported to the Board and Audit Committee.

52. This will occur routinely twice a year – once following the operational plan update and then again mid-year – or more frequently should circumstances demand.

53. Any low priority risks are not reported outside of the department.

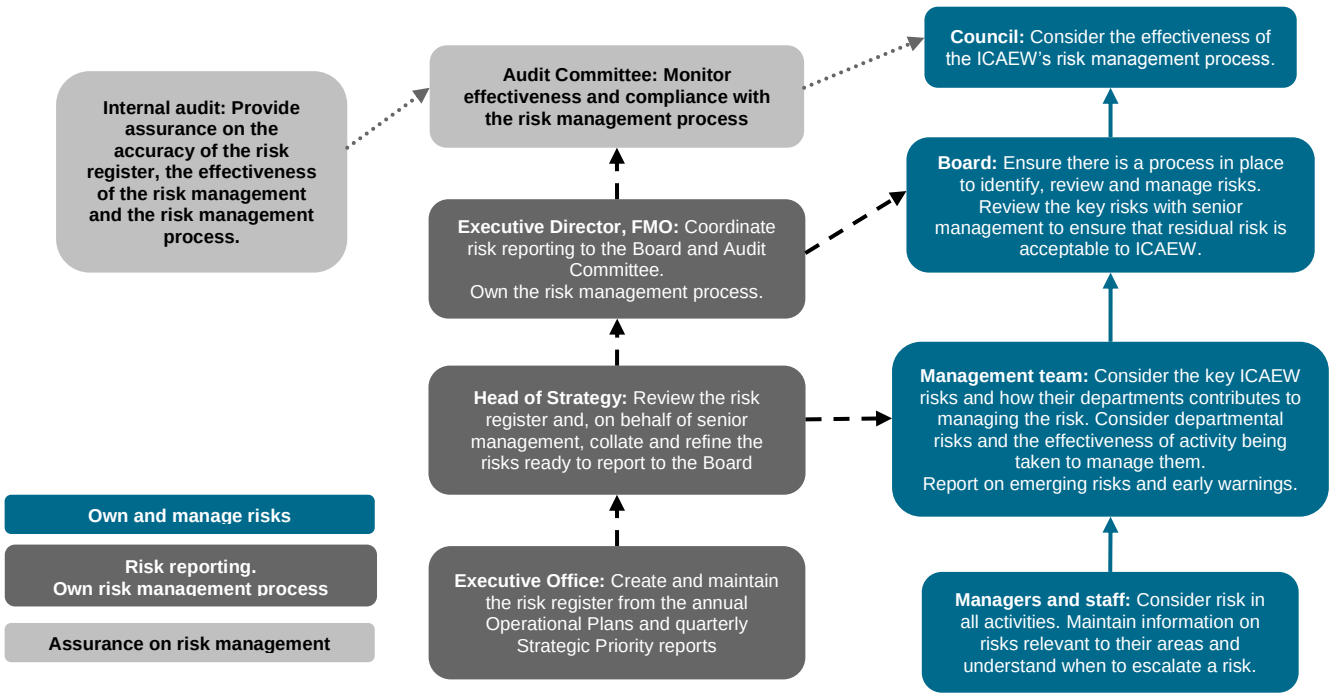
Risk Governance and review

54. **Principal Risks** are owned by Executive Directors and delivery of mitigating actions is built into strategy and operational plan. They are reviewed by the Board at every Board meeting.
55. **Corporate risks** owned by Executive Directors s/Directors (as appropriate) and mitigating actions are either project-based (time-bound) or business as usual, delivered by multiple owners (i.e. person most appropriate regardless of where they are in org).
56. **Departmental risks** are owned by departments and activities (usually) delivered by that department.
57. Risks are reviewed and discussed at departmental management team meetings (usually monthly). Departmental boards should have the opportunity to review all risks and the ability to suggest new risks and suggest alterations to current risks.

Monitoring and quality assurance

58. Internal Audit monitor whether the process is effective through regular reviews of the risk management process and the risk register reports. The results of these audits are reported to the Audit Committee.
59. Internal audit also report on the completeness of the risk register through their regular internal audit programme.
60. Audit Committee conduct regular 'deep dive' exercises into principal and other risks.

Roles and responsibilities



61. Everyone at ICAEW has a responsibility for risk management:
62. Risk reporting is the responsibility of the Executive Office and the Director, Strategy and Governance.

63. The Executive Director, Finance, Operations and Members will present the risk register to the Audit Committee and Board following agreement with the Management Team.
64. The Head of Strategy, with support from the departments, will collate the risks reported in the operational plans, strategic reports and monthly Executive Director reports into a risk register. The risk register will be updated twice a year using these source documents.
65. The Risk Manager will actively support departments to apply this policy. This will include:
    - Providing training and advice.
    - Reviewing the risks reported and challenging them when they do not meet this policy.
    - Considering any gaps in the risk register – looking for “left field” risks or areas of risk that have been omitted or duplicated.

A TEMPLATE RISK REGISTER

Ref	Risk	Objective/ Strategic Priority	Priority	Current risk management activity	Owner	Additional risk management activity planned	Responsibility and target date	Net Risk
	[Description of the risk and its potential effect on ICAEW]	*[The department objective or strategic priority to which this risk relates]*	*[High, medium or low rating based on the risk level pre risk management activity]*	*[Current activity in place to manage the risk.* *May include internal controls, contingency plans, etc.]*	*[Person responsible for managing the risk]*	*[If the risk is not at an acceptable level, what additional risk management activity is planned?]*	*[Responsibility and date to implement additional risk management activity]*	*[High, medium or low rating based on the risk level post risk management activity]*