International Actuarial Association

Risk Oversight Task Force

Report to Audit & Finance Committee

28 August 2015

Contents

Glossary

Abbreviation	Meaning
A&F	Audit and Finance Committee of IAA
IAA	International Actuarial Association
RAS	Risk Appetite Statement
RMF	Risk Management Framework
ROTF	Risk Oversight Task Force
ToR	Terms of Reference

1 Executive summary

1.1 Overview

The Risk Oversight Force (ROTF) was established by the Audit and Finance Committee (A&F) of the International Actuarial Association (IAA). Its Terms of Reference were established following the September 2014 IAA meeting and formally approved by the A&F on 19 May 2015. The ROTF is focused on risks to the IAA. These risks are not necessarily the same as risks to the profession, or Member Associations or individual actuaries, which may have different risk profiles.

The effective management of risk in any organisation is a challenging and ongoing task. The IAA is no different. From a governance perspective the IAA should have adequate and appropriate risk management policies and processes in place.

The IAA is also a professional association and so from a professional perspective, particularly as actuaries provide professional guidance to their clients on risk management, the IAA should also have, and be seen to have, adequate and appropriate risk management policies and processes in place.

The ROTF has accomplished a number of things. These include:

- Outlining a Risk Management Framework (RMF) that provides a basis for establishing, monitoring and managing risk. This is a specific application of the actuarial control cycle.
- Providing a high level risk taxonomy for governance purposes
- Proposing a Risk Appetite Statement (RAS) for the IAA
- Conducting a survey of members to obtain views on risks to the IAA
- Completing an initial assessment of key residual risks facing the IAA
- Summarising a Likelihood-Consequence–Impact approach to risk management
- Identifying an initial set of consequences to support the assessment of potential risk events and so support their management
- Linking the IAA's risk management approach to its activities as given by its strategies
- Clarifying the roles and responsibilities for risk management activities
- Providing recommendations to the A&F, and so ultimately to Council, regarding how the IAA's risk management should continue to be developed.

There remains further work to be done, particularly to ensure successful implementation. This is beyond the scope of the current ROTF. It is also reality that risk management is an evolving process and so it should be expected that things will not remain static. It should be expected that ongoing improvements will be made and the risk management process is a 'living process' that reflects and responds to experience.

The challenge facing the IAA, as all organisations, is to effectively implement its risk management strategy, processes and behaviours. Central to this is to have the top-down, global, organisational perspective on aggregate risks faced by the organisation merge

effectively with the bottom-up, local, project specific perspective on particular risks being addressed by those leading and carrying out individual projects. The contribution of the IAA Secretariat will be a critical component of success.

Recommendations, summarised in section 1.3, are provided to guide future IAA work.

This report completes the work of the ROTF.

1.2 Audience

The primary intended audiences of this report are IAA's A&F Committee, the IAA Council, the IAA Executive Committee and the IAA Secretariat.

This report is for the exclusive use of the IAA.

1.3 Summary of recommendations

This report makes the following recommendations:

Section	Recommendation
2.4	1 RMF: The risk management framework (RMF) outlined in this report be adopted by the IAA.
3.5	2 RAS: The Audit and Finance Committee adopt the proposed Risk Appetite Statement (RAS) and this then be put forward to Council for its approval. This implicitly means the Risk Likelihood, Risk Consequence and Risk Impact Tables are also agreed. The RAS should then be published on the IAA website.
3.6	3 BCP: A Business Continuity Plan (BCP), as outlined in this report, be prepared by the Secretariat for approval by the Audit and Finance Committee. This plan then should be implemented.
4.2	4 Risk identification: The IAA, through the Executive Committee, maintain a non-exhaustive listing of possible risks that IAA projects may face. This list will be built on the prototype that emerged from the ROTF risk survey of 2015 (as presented in Annex 9 of this report).
5.2	5 Risk management function: The IAA, through the Audit and Finance Committee, should ensure that all relevant components of a risk management function are explicitly reflected in appropriate job descriptions and/or terms of reference. This includes risk management activities and reporting as well as the processes and controls to support those activities.
5.3	6 Risk management – key responsibilities: The risk management responsibilities for Council, Executive Committee and Audit and Finance Committee as outlined in this report be adopted by the IAA.
5.3	7 Risk management – Committees and Sections: The risk management responsibilities for IAA Committees, sub-committees, Working groups, Task forces and Sections as outlined in this report be adopted by the IAA and

Section	Recommendation
	operationalised by the Secretariat.
5.3	8 Risk management - Secretariat: The risk management responsibilities for the Secretariat as outlined in this report be adopted by the IAA and operationalised as soon as practicable.
6	9 Internal processes and controls: The Secretariat be tasked with collecting into a single accessible place information regarding current risk mitigation steps (including insurance coverages), processes and controls that are relevant from a risk management perspective.
7.1	10 Risk reporting: The detail and construction of Risk Report, reflecting their various purposes and audience needs, be progressed by the IAA. This, coupled with the establishment of a Risk Register, is a necessary and critical component of the effective implementation of risk management.
7.2	11 Risk map: The development of a risk map, with the capacity for ongoing enhancement, be progressed by the IAA. This, coupled with the establishment of a Risk Register, is a necessary and critical component of the effective implementation of risk management.
7.3	12 Risk assessment process: The risk assessment process proposed in this report be adopted by the Secretariat and IAA.
8	13 Risk register: The IAA implement a risk register. This is to provide a central, dynamic source through which risk management activities are recorded, monitored and reported. Regular reports based on the Risk Register should be made to Audit and Finance Committee, Executive Committee and Council.
9	14 Monitor and audit: The Audit and Finance Committee establish a program to ensure that the IAA risk management policies and procedures, both their design and their implementation, are monitored and audited (as appropriate) for their acceptance, efficiency and effectiveness.
9	15 External compliance: The Audit and Finance Committee ensure that all relevant external compliance requirements are documented and provided to the Executive Committee so that the risk of breach of any specific requirements can be monitored and addressed prior to such a breach occurring.
10	16 Review: The Audit and Finance Committee establish a program for continuing development work on the IAA risk management policies and procedures, and also establish a regular review cycle for the review of these policies and procedures.
11	17 Dissemination: The IAA consider the timing and extent, if any, the approach, processes and outcomes established in this report should be shared with IAA members and more widely.

2 Background and scope

2.1 Need for risk management

At a basic level there is no disputing the need for risk management. As it is commonly said, the world is a risky place. Experience and common sense indicate that when a course of action is planned, steps to mitigate undesirable outcomes should be taken. It may also be that a decision to take no action will also have undesirable or unintended outcomes.

Organisations necessarily take risk in undertaking actions to achieve their strategic objectives. Normally checks and processes are in place to mitigate outcomes that do not achieve the planned objectives. Not all the outcomes to be mitigated can be prospectively anticipated (except in a perfect world … or in a model). It is also often the case that mitigation actions are taken in silos, by individual project or by focus and construction. While this may be adequate for individual projects it may not be adequate or efficient for the organisation as whole.

The discipline of risk management seeks to address these issues in a way that supports the organisation achieving its objectives. It makes explicit and brings together in a structured and holistic way many things which are typically already done by organisations (but sometimes either implicitly or piecemeal). It provides both a top-down perspective on the aggregate levels of risk an organisation is managing and a bottom-up approach on the particular risks a specific project may be addressing. A challenge is to get these different perspectives to meet and merge.

Risk management is a tool that is one of the means used to achieve the ends of realising the strategic objectives. It should also support actions taken when unplanned outcomes, particularly adverse ones, occur. It recognises that risk events will occur and supports the management of those events and their consequences after they occur. It is important to acknowledge that risk events will occur. The purpose of risk management is not to achieve a guarantee that such unplanned outcomes will not occur (that is risk avoidance), but to reduce the impact of risk events when they occur in a proportionate and supportive manner.

This may be read as suggesting that risk management is a process which can be developed and then automated. It is the case that a necessary condition for effective risk management is to have in place appropriate controls and processes. However, recognising the multi-faceted and evolving nature of the risks organisations face (a current example might be the rapidly increasing awareness of the impacts of cyber-attacks) it is widely acknowledged that the key to sufficient conditions for effective risk management is an appropriate organisational culture with clear and supportive leadership.

Risk management is challenging and the real test of an organisation's risk management is its capacity to effectively respond to the stress of a major risk event when it occurs while still being able to carry out its mission. A risk management program may be exemplary, but if it adds so much overhead that the organisation is stifled, it is of no use.

Finally, it is important to note that the action of taking no action may be the riskiest of all.

Having established the need for risk management, the purpose of this report is to outline an RMF and place it in an IAA context.

2.2 IAA context

As an organisation the IAA, and its member actuarial associations and their member actuaries, tend to be conservative and risk averse. This culture may have served us well in the past but may not be sufficient in the future. Hence the ROTF is starting a process to put IAA Risk management on a firmer and more explicit footing. This will formalise IAA risk management for the purposes of both internal governance and demonstration to stakeholders. This is consistent with the professional and reputational perspective of the IAA and actuaries in general of demonstrating to IAA stakeholders evidence that 'we practice what we preach'.

This is not to say that there is no risk awareness or management taking place in the IAA, rather that it may be more implicit than explicit, informal rather than formal, and fragmented in being bottom-up rather than more comprehensive and top-down. While outcomes to date seem to have been acceptable since the IAA is fully operational, there is a need for better governance and more complete policies processes, management and monitoring. Actuaries have been at the forefront of the development of many risk management tools and techniques, particularly regarding financially related risks and Enterprise Risk Management. This knowledge and skill set can also be applied to improve the risk management of the IAA.

The IAA is a registered not for profit organisation incorporated in Switzerland. It is located in Canada and so needs to meet the Canadian tax requirements to be exempt from tax. At a summary level any revenue received by the organisation need to be used for the benefit of its members to support its mission and activities. There is an important compliance requirement that an excess surplus is not accumulated to ensure that this beneficial status is retained.

The IAA is also a professional organisation. At a summary level, it seeks to further the actuarial profession at a global level. This therefore includes a focus on education (initial and continuing), professionalism (including developing guidance), and influencing (promoting the profession with potential users of actuarial skills and services). The underlying 'public interest' commitments of the IAA are also noted.

Apart from a small salaried Secretariat, the IAA is also a volunteer organisation. It is relevant to note that the volunteer base makes the IAA a much larger organisation than a head count of the Secretariat might initially suggest. Also, the volunteer status of most participants in IAA activities implies that activity management needs to recognise this status.

These characteristics and their implications should be recognised in the IAA's risk management.

These points also all indicate that the awareness and reputation of the IAA are of great importance. Hence Reputation risk has been identified as a particular risk in its own right to be addressed.

The effort and requirements of risk management should be proportionate to the capacity of the organisation and the risks being managed. A key contribution effective risk management makes to an organisation is that it empowers the organisation to achieve its objectives, not inhibit it from doing so. There is therefore a balance and tension to be maintained between completeness, complexity and precision on the one hand and adequacy, simplicity and insight on the other. Risk management necessarily involves judgement and appropriate

leadership and behaviours supported by processes and reporting structures. Risk management is an evolving and ongoing challenge and its inherent complexity in a changing environment should be acknowledged.

Some guidance might be taken from the following quote attributed from Albert Einstein:

> *In every field of inquiry, it is true that all things should be made as simple as possible – but no simpler. And for every problem that is muddled by over-complexity, a dozen are muddled by over-simplifying.*

More guidance might also be taken from a paraphrase of a quote from H L Mencken:

> *For every complex problem there is an answer that is clear, simple, and wrong.*

2.3 Perspectives

There are various perspectives from which risk and risk management can be viewed.

From a top-down governance perspective an organisation needs to manage a portfolio of risks. This portfolio is made up of different types of risk and, within each type of risk, there are also a variety of specific risks to manage. To the extent it is practical, and without unnecessarily inhibiting the organisation achieving its objectives, the more explicit and integrated risk management is in the activities of the organisation the better. This includes both activities and attitude, that is what is done, how it is done, and why it is done.

From a bottom-up project perspective each project owner needs to specify and execute that project to the best of their ability. In contrast to the organisational governance perspective, a project focus is quite specific and local, not broad and global. The risks involved with a particular project contribute to the overall portfolio of risk managed by the organisation, but the behaviours of the specific project risks and the portfolio may differ. Successful projects are key to an organisation's success as, in the end, they are where all the work gets done.

A core challenge of risk management is to effectively link these two differing perspectives. Risk management needs to be embedded in the operational processes, not viewed as a subsequent and additional 'bolt on' to them from the outside. This then requires effective processes to be in place so that the needs of both projects and the organisation are addressed. The process chain that joins projects to the organisation's governing body is only as strong as its weakest link. A RMF specifies the links in this chain and the quality of its implementation specifies the strength of the links.

Examples of these differences in perspective include the need to link organisational risk appetites with specific project level risk tolerances and limits, the need for adequate reporting of risk from projects so that an aggregate organisational view of cumulative risk taken can be made, the need for project managers to be aware of risk management processes and mitigants the organisation has in place (for example insurance coverages … or the lack of them), and the need to manage risk events when they occur.

In larger organisations it is common practice to have a dedicated risk management function in place which is tasked with supporting and co-ordinating the organisation's risk management activities. This risk management function may be a separate area with employees dedicated to it, or it may be a specified component of one or more employees'

overall roles. The risk management function provides a co-ordinating 'head' for the risk management 'body' of processes and activities of the organisation.

2.4 Risk management framework

A risk management framework (RMF) includes the totality of strategies, systems, structures, policies, processes and people within the organisation that identify, assess, mitigate, monitor, report and manage all risks (internally or externally generated) that could have a material impact (financial or non-financial) on an organisation's operations.

It is important to consider both known (well defined and quantifiable) and unknown (either or both of ill-defined or not quantifiable a priori) risks. It is also necessary to have in place processes to identify, manage and resolve risk events when they occur since it is not realistic to presume that all risks can be identified at a point in time and, even if they could be, that their occurrence can be guaranteed not to take place at some time in the future.

Risk management is thus inherently complex and evolving. However, risk management activities need to enhance an organisation's capacity to achieve its objectives and should be commensurate with the size, objectives and complexity of organisation.

A RMF provides a high level 'language' that supports the discussion of risk management matters. A RMF can comprise a number of elements.

- Construction:
    - Identification of material risks
    - Risk appetite and tolerances
    - Risk management strategies
- Implementation:
    - Internal process and controls, including Roles and Responsibilities
    - Risk reporting and risk maps
    - Risk register
    - Monitoring and audit
    - Review and update

These elements are described in some more detail in Annex 1.

These elements provide the basis for the structure of this Report.

Recommendation 1: RMF: The risk management framework (RMF) outlined in this report be adopted by the IAA.

2.5 Application of Control Cycle

The application of actuarial control cycle paradigm is a core actuarial skill. At its core is the Analytic cycle which has three components of 'Specify – Solve – Monitor'. This problem solving cycle entrenches continual review. This cycle can be recast in a governance and risk management context as a 'Policy - Implement - Monitor' cycle.

Tasks and responsibilities can then be assigned within each of these components.

Problems arise and are solved in a wider context and environment. The analytic cycle is embedded within a Professional cycle to put the problem solving into this wider context. This cycle has four components as follows. These, reflecting a governance and risk management focus, include amongst other things:

- Governance. Including strategy and risk management
- Application. Including project management and communication
- Behaviour. Including culture and professionalism
- Environment. Including public interest (including stakeholders) and awareness.

In the context of risk management the Analytic cycle provides a problem solving process and the Professional cycle provides context. The Application component of the professional cycle is of particular importance since effective implementation of risk management is necessary for the long term survival of any organisation. The Risk Governance risk in the IAA high level risk definitions attests to this.

Annex 2 contains some more discussion of the actuarial control cycle and its application to risk management.

2.6 ROTF Scope

The Terms of Reference (ToR) of the ROTF, as approved by the A&F, are given in Annex 3.

A comparison of the RMF and the ROTF scope shows that the scope of the ROTF is limited.

The ToR of the ROTF includes review of existing IAA processes and providing recommendations for change. They do not extend to the implementation of such recommendations. The importance of implementation can be put into context by observing that it is common that the 'engine' for risk management activities is often an organisation's Risk Register. This provides a central location in which information about risks and risk events is accumulated, risk management activities are recorded and reporting is done from. The IAA does not have a formal Risk Register.

As indicated by the recommendations made, further work is needed to complete the work of developing and implementing an adequate and appropriate risk management framework for the IAA.

In this context it is perhaps worthwhile remembering that a key reason why some new Risk Management Frameworks do not live up to expectations is because the risks of inadequate follow-through of the design and poor implementation are not properly addressed at the outset. (See 'implementation risk' as noted under Risk Governance in Annex 5.)

3 Risk appetite

3.1 Risk

A definition of risk is that it is the possibility of not meeting objectives. Hence key to managing risk is the need to have clear objectives so that an assessment can be made of whether they were met. Then the consequences of not meeting objectives can be assessed and managed.

The risk appetite of an organisation characterises the extent to which it will tolerate not meeting its objectives.

A key set of objectives against which IAA risk and risk management are assessed are those provided by its strategies and the specific project undertaken to pursue those strategies. From an organisational perspective, these strategies are outward looking. The current IAA strategies and associated projects are given in Annex 4.

To effectively implement these strategies, there needs to be adequate supporting infrastructure in place. This necessary infrastructure is provided by the IAA Secretariat and the policies and procedures of the IAA. Consequently there are also objectives in place to provide that infrastructure.

3.2 Key risks

A set of high level risks has been identified. These were used in the Survey conducted by the ROTF. Definitions are provided in Annex 5. In summary they are:

- Strategic risk
- Reputational risk
- Operational risk
- Finance risk
- Risk governance
- Other risk (ideally this category should not be used).

It is noted that there are many risks generally identified, with more emerging on a regular basis. The ROTF suggests that while being more specific about risks may aid discussion and resolution, it is also appropriate to include them in the proposed taxonomy which should be used in a hierarchical manner with increased refinement with each level of the hierarchy. Annex 5 provides the top level of the hierarchy with some guidance with regard to the next level in the commentary.

3.3 Impact of risks

The impact of a risk on an organisation can be assessed in terms of its likelihood and consequence (given that it occurs). This standard approach was used on the survey conducted by the ROTF. It is described, with Tables, in more detail in Annex 6.

3.4 Risk culture

It is well established that the risk culture of an organisation is a key factor in its success or failure in introducing effective risk management.

Consideration of the status of the risk culture of the IAA is outside the scope of the ROTF.

The nature and objectives of the IAA and the typically conservative and risk averse nature of actuaries in general suggest that it might be anticipated that the risk culture of the IAA is likely to support risk management in IAA activities.

3.5 IAA risk appetite

Risk appetite applies to residual risks which are the inherent risks assessed after mitigating actions have been applied. An acceptable risk is one which meets the criteria of the risk appetite and/or associated risk tolerances.

Risk appetite can be summarised as being the amount and type of risk that an organisation is willing to accept in the pursuit of its objectives, before action is deemed necessary to reduce it. That is, the total impact from a type of risk the organisation is willing to accept. Risk appetites may be specified either qualitatively or quantitatively.

Risk tolerance can be summarised as the specific maximum risk that an organisation is willing to take regarding each relevant risk.

Risk appetite is thus pitched at a higher, aggregate, organisational level, while risk tolerance is pitched at a more granular, individual risk, level. Risk tolerances need to translate risk appetites into operational measures and so need to be as quantifiable and measurable as possible.

A risk appetite can be constructed in terms of specifying acceptable levels of risk impact. Visually, it can be thought of as specifying an ‘acceptable’ region for each risk considered in a Risk Impact Table. Visually, risk mitigation steps can be thought of as steps which move a specific risk to the left and/or down on the Risk Impact Table as they transit from being inherent risks to residual risks.

In terms of managing to a risk appetite, the actions required as a consequence of placing an inherent risk in a Risk Impact Table are:

- Extreme: Requires immediate action as the potential risk exposure could be devastating to the organisation.
- Very High: Requires action very soon (within 3 months), as it has the potential to be damaging to the organisation.
- High: Requires treatment with routine or specific procedures.
- Medium: Continue to monitor and re-evaluate the risk, ideally treat with routine procedures.
- Low: Continue to monitor and re-evaluate the risk

The RAS is determined in terms of future expectations regarding future risk events. Current risk events may be being addressed and may impact or generate a review of the RAS. The levels of Low and Medium impacts accept that risk events may occur but presume that their

impacts are manageable within standard processes. In this context the set of levels used to manage a risk appetite have the following choices added:

- Very Low: This means that it is accepted that a risk event may occur occasionally, but that all reasonable arrangements will be put in place to prevent its occurrence and if it does occur corrective action will be promptly undertaken
- Nil: This means that there is no acceptance of risk events and should such risk events occur there will be a severe and immediate response.

Having a risk appetite that is Low (or more conservative) does not automatically imply that risk with higher (inherent) ranking may not be taken on. Rather it implies that the risk management around such a risk needs to be strong enough to bring the residual risk down to acceptable level as indicated by the risk appetite.

Further, it does not imply that the occurrence of a major risk event, in of itself, is an indication that the risk management policies or processes failed. This may be the case, however the possibility that a low risk event has actually occurred (unfortunately) should be accepted. In this case the statistical likelihood of occurrence may be low, but the issue is the impact in the case where such an event occurs.

A Risk Appetite for the IAA is given in Annex 7.

Recommendation 2: RAS: The Audit and Finance Committee adopt the proposed Risk Appetite Statement (RAS) and this then be put forward to Council for its approval. This implicitly means the Risk Likelihood, Risk Consequence and Risk Impact Tables are also agreed. The RAS should then be published on the IAA website.

3.6 IAA Business Continuity Plan

The IAA Secretariat is critical to the successful functioning of the IAA and the implementation of its strategies. Consequently its continuing functioning under the stresses of business interruptions is also critical.

The IAA does not currently have a comprehensive Business Continuity Plan. A secretariat project, under the auspices of the A&F, is currently in progress with regard to IT in this regard.

Further high level comments with regard to BCPs are provided in Annex 8.

Recommendation 3: BCP: A Business Continuity Plan (BCP), as outlined in this report, be prepared by the Secretariat for approval by the Audit and Finance Committee. This plan then should be implemented.

4 Risk identification

4.1 Survey

In the first quarter of 2015, the ROTF conducted a voluntary survey of IAA members and committees et al to solicit input on risk facing the IAA. 32 usable responses were received with 119 specific comments. 16 member associations, 7 IAA committees (et al), 4 Secretariat staff, 3 individuals and 2 other organisations responded. Respondents were asked to list up to 5 key risks they saw the IAA facing. Responses were not requested in any order of priority. The specific comments are summarised in Annex 9.

In August 2015 a short 'thank you' report was provided to participants summarising the responses (as summarised in Annex 9). No analysis of commentary on the results was included.

It is worth noting that the focus of the respondents to the survey come from different organisations and so may have differing perspectives, and that the IAA perspective is probably also different, reflecting its different purpose(s) compared to those of national associations.

The topics identified by the survey provide a useful starting point for identifying possible risks to IAA work and so topics to be considered when assessing the risk profile of projects and activities supporting achieving the IAA's strategic objectives. The list of topics from the survey is not complete, but it does serve to start a risk assessment process for a project.

Perhaps as might be expected the largest group is the combination of the Strategic and Reputation risks with operational risks following. As might also be expected, there are few 'Other' risks.

4.2 Further ROTF Analysis

The ROTF has not undertaken identifying further possible risks since it is potentially inappropriate to provide checklists as that may create the risk of encouraging selection from such lists and may not encourage specific thought and analysis of the particular risks a specific project may face. However the balancing perspective is that it is inefficient to expect project managers to continually 'reinvent the wheel' when undertaking risk assessments and there is clearly value in having reference lists to provide prompts which may help avoid risk being overlooked.

Recommendation 4: Risk identification: The IAA, through the Executive Committee, maintain a non-exhaustive listing of possible risks that IAA projects may face. This list will be built on the prototype that emerged from the ROTF risk survey of 2015 (as presented in Annex 9 of this report). This list is to serve as a prompter for further risk analysis and not to be used as a definitive or complete list to only be checked against.

5 Risk management strategies

5.1 Risk management approaches

There are a number of standard approaches that can be taken when seeking to mitigate the prospective impact of risk events. These include:

- Avoid. Do not take on a course of action that allows a risk of this nature to arise.
- Mitigate. Reduce impact by reducing either or both of likelihood and consequence.
- Transfer. Transfer the impact of the risk event to a third party which can deal with the risk (insurance).
- Accept. Accept the risk and the consequences of any risk events that might arise.
- Hedge. Determine offsetting risk events so that on a portfolio basis aggregate events are managed.

In the IAA context the Hedge approach is unlikely to be used.

It is beyond the scope of this report to make a detailed review of the current set of risks being managed by one or more of the above approaches and the appropriateness of the approaches being used.

Such an assessment should be considered when the IAA risk mapping exercise is completed as it is central to the assessment of the transition from inherent to residual risks.

5.2 Risk management function

As suggested in section 2.3, a risk management function provides a co-ordinating 'head' for the risk management 'body' of processes and activities of the organisation.

The IAA currently does not have a designated risk management function. In practice the Secretariat is too small for it to be appropriate to designate a full person to this role. This practical outcome heightens the need for vigilance by both the Secretariat and the governance processes to ensure that independent and impartial risk assessments and management are made and seen to be made.

Recommendation 5: Risk management function: The IAA, through the Audit and Finance Committee, should ensure that all relevant components of a risk management function are explicitly reflected in appropriate job descriptions and/or terms of reference. This includes risk management activities and reporting as well as the processes and controls to support those activities.

5.3 Key responsibilities

The key responsibilities of:

- Council
- Executive Committee
- Audit and Finance Committee
- Committees, sub-committees, Working groups, Task forces and Sections
- Secretariat

are listed in Annex 10.

Recommendation 6: Risk management – key responsibilities: The risk management responsibilities for Council, Executive Committee and Audit and Finance Committee as outlined in this report be adopted by the IAA.

A review by the Secretariat of all IAA Committees, Sections et al determined that only two ToRs referred to risk management explicitly (A&F and ROTF). There is a need to have a process by which risk management matters are addressed by Committees, Section et al.

It was clarified that the ToR structure for IAA Committees, Sections et al has two parts: mandate and operations. It is recommended that reference to risk management be included in the operational section for all Committees, Sections et al. This then automatically requires each Committee, Section et al to report on risk management matters on at least an annual basis. This approach also has the advantage of being standardised. The Secretariat has been tasked with ensuring that Committees, Sections et al include appropriate risk management considerations in the operational component of their ToRs. All material projects commenced in the future by the IAA are to have risk management considerations included in their ToRs.

It is noted that embedding and operationalising risk management considerations into Committee, Section et al ToRs and practices may require some care. The perception that such considerations are a 'nuisance' needs to be avoided and, instead, they should be seen as supportive and value adding. The Secretariat, A&F and the Executive Committees may need to consider in advance appropriate responses in case there may be resistance to embedding and reporting on risk management activities in Committee, Section et al work so that an effective portfolio management of aggregate risks against the IAA risk Appetites can be done.

Recommendation 7: Risk management – Committees and Sections: The risk management responsibilities for IAA Committees, sub-committees, Working groups, Task forces and Sections as outlined in this report be adopted by the IAA and operationalised by the Secretariat.

Recommendation 8: Risk management - Secretariat: The risk management responsibilities for the Secretariat as outlined in this report be adopted by the IAA and operationalised as soon as practicable.

6 Internal process and controls

The IAA, and the Secretariat in particular, already have in place a number of internal processes and controls to support the conduct of business. These include topics which are relevant to risk management, such as:

- IAA Authorities Matrix. This is being reviewed and updated by the Secretariat as part of a separate project for the A&F. The ROTF role, from a risk management perspective, with regard to this project is limited to noting the issues and receiving assurance that it is being addressed.
- Escalation and delegation processes to and from the A&F and Executive Committees. The ROTF was informed that these need review, clarification and updating. This is to be addressed by the Secretariat.

Other aspects of risk management are available from a variety of current processes and controls within the Secretariat. An immediate example is the extent of insurance coverages held by the IAA. However these references, from a risk management perspective are somewhat scattered, are not well co-ordinated, and in some cases are not well known by Committees, Sections et al which should know about them.

An example is the insurance coverages held to cover IAA and IAA volunteer activities. The IAA has directors and officers and professional liability insurance which covers the IAA volunteers in their work for the IAA. These would cover a volunteer working on the actuarial standards committee from liability with respect to his/her work on the ISAPs. However, they do not cover Actuaries Without Borders volunteers who are 'working in the field'; the latter must sign a waiver releasing the IAA from any liability and advising them to obtain appropriate insurance coverage.

A key value of establishing clear and consistent internal processes and controls is that this supports a common understanding and approach to risk management matters. Their links to wider management issues, business planning, management and governance is also of value.

Recommendation 9: Internal processes and controls: The Secretariat be tasked with collecting into a single accessible place information regarding current risk mitigation steps (including insurance coverages), processes and controls that are relevant from a risk management perspective. This source is to be maintained and kept current on an ongoing basis. Access to this information by Committees, Sections et al is to be encouraged.

The ROTF has been informed that this recommendation is in the process of being actioned by the Secretariat.

7 Risk reporting and risk maps

7.1 Risk reporting

The ROTF has been informed that the IAA does not have a standardised and regular process for reporting the status of the risk faced by its projects. This should be rectified and reporting on risk matters better integrated into management processes.

In order to report on risks they need to be assessed in a structured manner.

The essential interaction between risk management and business activities can be captured in a matrix form. This recognises that the 'footprint' of a particular risk can reach across multiple business activities, and that business activities can reach across multiple risks. On an ongoing basis it also allows for the practical reality that risk profiles of activities may change over time, both for prospective risk management and mitigation and for risk events.

Each cell would contain an assessment of whether or not that cell is considered to be within the IAA's risk appetite. A 'traffic light' approach would be visually appealing. This has three states, positive (green), at risk (amber) and negative (Red). More insight might be provided by also providing an indication of movement in time of the statuses.

The level of detail held in such a matrix depends on audience and purpose.

At the highest management level reporting on the risk status of each Strategic objective against each of the major risk categories may be sufficient and appropriate. The strategic objectives published by the IAA (see Annex 4), which are externally focussed, should be augmented by some high level Operational objectives which are necessary to ensure the development and maintenance of the required internal infrastructure to support the achievement of the stated IAA Strategic objectives. The Operational objectives support the adequacy of the IAA internal processes, people, systems, controls, and reporting.

This would lead to a matrix with, say, 8 reporting columns, one for each Strategic Objective and allowing two more columns for Operational Objectives, and 6 reporting rows, one for each high level risk.

It is the case that each cell in such a matrix is a summary over multiple items. There will likely be multiple activities from the business perspective in a given column and multiple risks from the risk management perspective in each row. The detail of how such aggregate outcomes may best be obtained will depend on purpose. For example, it may be based on the expert judgement of one or more people, perhaps on a consensus basis. It may also reflect a more automated approach. A straightforward approach would be to take the worst outcome over all the outcomes being considered. This may be seen as being too pessimistic, so perhaps some form of averaging over the outcomes may be preferred (a risk of this is that the 'tyranny of the average' appears, and extreme or adverse outcomes may be obscured). In a financial context more sophisticated aggregations may need to be considered.

In general, the key concern is to have a process which is robust and relatively straightforward to apply. The purpose of the reporting is not, in of itself, to make decisions, but provide useful and constructive input to support a better informed decision making process.

When more detailed information is required, additional granularity can be included in rows and or columns, noting that then not all the major rows and columns may be needed.

In practice, strategic objectives are achieved through various projects, and projects are carried out by either Committees (Sections et al) or the Secretariat. It may be useful to have reporting by Committee (Sections et al) and by their projects with the strategic objectives they support then being subsidiary information. Alternatively, it may be useful to have reports that focus on specific risks and reflecting their footprint across multiple projects and/or objectives.

The flexibility of reporting will depend on the flexibility (and extent of currency) of the system that contains the risk related information. This system will likely be the Risk Register.

Recommendation 10: Risk reporting: The detail and construction of Risk Report, reflecting their various purposes and audience needs, be progressed by the IAA. This, coupled with the establishment of a Risk Register, is a necessary and critical component of the effective implementation of risk management.

7.2 Risk mapping

To be able to report on risk related matters on a consistent basis, the risks being considered need to be listed in a coherent way.

A risk map provides this. It is constructed in a hierarchical way, starting from the high level risk categories and then adding granularity (and explanation) into these levels as required. The process needs to be flexible and sustain ongoing change and improvement. It is perhaps useful to note that a key characteristic of developing risk maps is that they provide a consistent way of naming and describing risks to support communication. It is then not so much about the outcomes being 'correct', but more about them being consistent and coherent over time.

The beginnings of a risk map are provided in Annex 9 which reports on the results of the Survey conducted by the ROTF. This risk map clearly needs extension.

The specific risks identified for each Strategic and Operational objective need to be identified and included. These can be expected to change over time.

Recommendation 11: Risk map: The development of a risk map, with the capacity for ongoing enhancement, be progressed by the IAA. This, coupled with the establishment of a Risk Register, is a necessary and critical component of the effective implementation of risk management.

7.3 Risk assessment process

The process is as follows:

- For each project risks are identified. The Risk map is a tool to ensure consistent identification. It also provides a prompter for risks that may be considered or added.
- For each project, and where appropriate, for specific risks within that project, a Project Owner is nominated. This Project Owner is then the person initially responsible for the assessment of the risk and the determination of any risk mitigation steps.
- Each risk is assessed to identify its inherent risk level, that is the inherent impact of the risk is assessed. Annex 6 outlines how this can be done.
- The inherent impact of the risk is assessed against the relevant RAS statements.
- If the RAS is satisfied, no further risk management action is required. The inherent risk is then accepted as the residual risk.
- If the RAS is not satisfied, then risk mitigating steps need to be taken so that, after these steps have been taken, the residual risk is reduced to satisfy the RAS. Where possible the application of established and consistent processes and controls, with the support of the Secretariat, is recommended. Where new mitigating steps are taken it is recommended these be shared with the Secretariat so that they may be integrated into more standard processes and controls for wider application.
- The IAA, through the Secretariat, establishes a process that both supports and reviews the risk assessments and associated risk mitigation steps. This will provide both consistency in approach and a review process.

Recommendation 12: Risk assessment process: The risk assessment process proposed in this report be adopted by the Secretariat and IAA.

8 Risk register

The importance of implementation of risk management processes and controls may be put into context by the observation that it is common that the 'engine' for risk management activities is often an organisation's Risk Register. This provides a central location in which information about risks and risk events is accumulated, risk management activities are recorded and reporting is done from. It is a key tool for the risk management process.

The nature of prospective risk management, which is focused on managing the expected future impact of residual risks, is of a different nature to the management of risk events once they have been detected and are then being managed. Both forms of risk management need to be recorded in the Risk Register.

The IAA does not have a formal Risk Register. This should be addressed.

Recommendation 13: Risk register: The IAA implement a risk register. This is to provide a central, dynamic source through which risk management activities are recorded, monitored and reported. Regular reports based on the Risk Register should be made to Audit and Finance Committee, Executive Committee and Council.

The frequency of these regular reports needs to be clarified. It is suggested that standard reports are provide to the Audit and Finance Committee and Executive Committee on a quarterly basis, and reports to Council regularly provided on half yearly basis.

It is also noted that if material risk events or environmental (internal or external to the IAA) changes arise outside these reporting frequencies that they are to be escalated in written form as soon as possible.

9 Monitoring and audit

This aspect of the RMF is outside the scope of the ROTF.

This step completes the 'Identify-Solve-Monitor cycle of the control cycle.

Recommendation 14: Monitor and audit: The Audit and Finance Committee establish a program to ensure that the IAA risk management policies and procedures, both their design and their implementation, are monitored and audited (as appropriate) for their acceptance, efficiency and effectiveness.

It is noted that there a number of external (to the IAA) regulatory obligations that need to be complied with. These include, for example:

- The IAA retaining its status as a 'not for profit' organisation
- External audit requirements
- Conformance with relevant other regulation and legislation, such as
    - Occupational Health and Safety requirements
    - Privacy laws

Recommendation 15: External compliance: The Audit and Finance Committee ensure that all relevant external compliance requirements are documented and provided to the Executive Committee so that the risk of breach of any specific requirements can be monitored and addressed prior to such a breach occurring.

The ROTF has been made aware of the possibility of such risks arising due to lack of effective internal communications.

10 Review and update

This aspect of the RMF is outside the scope of the ROTF.

Recommendation 16: Review: The Audit and Finance Committee establish a program for continuing development work on the IAA risk management policies and procedures, and also establish a regular review cycle for the review of these policies and procedures.

The ROTF is aware that this report does not complete the task of implementing a RMF for the IAA and further work is required. This work is both in terms of processes and controls and in terms of embedding an appropriate risk management culture into the IAA and its activities. Both remain challenges, with perhaps the risk management culture being the more difficult. An appropriate risk management culture supports the effective implementation of strategic objectives and does not impede or inhibit flexibility.

The ROTF suggest that when the IAA's RMF is fully implemented regular reviews of it, its effectiveness and its completeness be undertaken. However, in the absence of specific reason for review, such reviews should not be overly burdensome or frequent. A periodicity of every five years is suggested.

It is noted that an international standard for risk management exists: ISO 31000 - Risk management (see http://www.iso.org/iso/home/standards/iso31000.htm). The website states, in part:

> *Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.*
>
> *ISO 31000:2009, Risk management – Principles and guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.*

11 Next steps

As noted in previous sections, there remains work to be done to fully implement an IAA RMF.

The completion of this report completes the work to the ROTF. The Audit and Finance Committee will then consider the recommendations made and provide the next steps for the IAA. Many of the recommendations propose actions by the IAA Secretariat and successful implementation of risk management in the IAA will depend heavily on the Secretariat. It would be logical for the immediate next steps to include the IAA Secretariat developing an actionable implementation plan to be agreed by the A&F. The A&F will then also monitor and review the execution of the implementation plan. As the Secretariat develops the implementation plan, and drawing on the advice and guidance of the A&F, further task forces, working groups or other consultative committees or processes may be put in place to participate in the implementation process.

The successful implementation of risk management in the IAA will be an ongoing endeavour for all IAA committees and the Secretariat. Leadership by the senior IAA Committees and the Secretariat will be a critical ingredient of success. In a dynamic environment the RMF will continue to require ongoing and attentive management.

It is suggested that the IAA consider the timing and extent to which it wishes to share its risk management approach and the implications in doing so. Member organisations may be able to benefit from the IAA's work and in some cases may also be willing and able to provide feedback and further sharing in the actuarial community. This should be to the mutual benefit of all. It may also be that the IAA considers it may provide a leadership role, with the application of actuarial skills in risk management being demonstrated, on a wider level.

However it is noted that there remains much implementation work to be completed. Consequently it may be more appropriate, if the IAA does consider wider distribution of this report, to defer until implementation work is underway and any practical issues that may arise from developing more detailed planning and execution are addressed.

Recommendation 17: Dissemination: The IAA consider the timing and extent, if any, the approach, processes and outcomes established in this report should be shared with IAA members and more widely.

12 The Committee

The ROTF membership was as follows:

- Malcolm Campbell
- Tony Coleman
- Jules Gribble (Chair)
- Dave Ingram
- Mike Kilgour
- John Maroney
- Mike McLaughlin
- Godfrey Perrott
- Thierry Poincelin

The support of the IAA secretariat is also gratefully acknowledged.

End of Report

Annex 1 Risk management framework

To fully operationalise a RMF the following topics should be addressed:

1 Construction

- **Identification of material risks.** This includes both actual and perceived risks (for example, conflicts of interest and reputational risks). This should contain sufficient information to permit risks to be assessed and support the development of risk maps.
- **Risk appetite and tolerances.** As approved by the Council of the IAA. In summary, the amount and type of risk the IAA is willing to accept in pursuit of its objectives. Risk appetite statements should be supported, when possible, by risk tolerances which specify the specific maximum risk the IAA is willing to take regarding each relevant risk. All identified material risks are relevant.
- **Risk management strategy.** This describes the strategy(s) to be used to manage risks, including the risk management relationships between the Council and other parts of the IAA

2 Implementation

- **Internal process and controls**. This addresses actions and responsibilities. These are the more detailed processes covering all steps of the risk management processes: identification, mitigation, monitoring, reporting (including escalation requirements and delegated authorities) and responsibilities. Processes and plans to address risk events after they occur, including appropriate contingency arrangements and business recovery plans are included.
- **Risk reporting and risk maps.** This is a critical part of the risk management process. Timely and effective reporting to all stakeholders is necessary for the effective management of risks and risk events.
- **Risk register.** This is a central (up to date) record of risks identified and their assessment. It should contain inherent risk assessments, mitigation steps, and residual risk assessments. It should be the information system that provides the basis for reporting and monitoring of risks. Risk events and their resolutions should be recorded. 'Near misses' should also be recorded.
- **Monitoring and audit**. In the broad sense of the words. This addresses whether the internal processes and controls are effectively carried out. This includes the appropriate level of independent and unbiased assessment and execution of risk management responsibilities.
- **Review and update.** Ongoing/regular. This addressed whether the overall risk management framework approach and implementation is effective, fit for purpose and sufficiently comprehensive.

In general, when risk management is implemented, there is the need for the risk management function to be independent of the business, revenue generating functions and finance and the like. In the context of the IAA, it is considered not to be feasible to require such a separation of roles and powers in a small Secretariat.

Annex 2 Applying the actuarial control cycle paradigm

1 The actuarial control cycle paradigm

As noted in the text, the application of actuarial control cycle paradigm is a core actuarial skill, which entrenches continual, cyclic, review. It has three components:

- Specify (in this context, set policy)
- Solve (in this context implement policy, processes and controls)
- Monitor

Tasks and responsibilities can then be assigned within each of these components. Each component may also have the actuarial control cycle paradigm applied to it. That is, the paradigm can be applied in 'nested' manner.

Problems arise and are solved in a wider context and environment and so problem solving analytic cycle is embedded within a Professional cycle:

This cycle has four components:

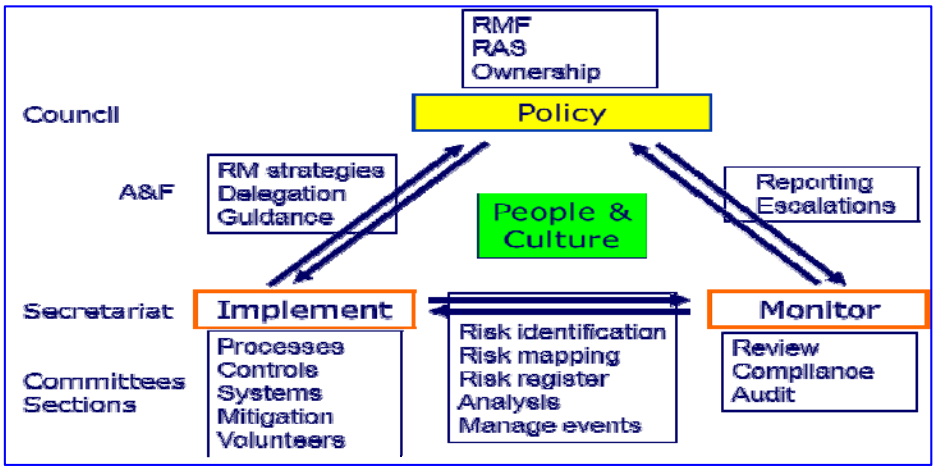
- Governance, including strategy and risk management
- Application, including project management and communication
- Behaviour, including culture and professionalism
- Environment, including public interest (including stakeholders) and awareness

2 Application to risk management

In the context of risk management the Analytic cycle provides a problem solving process and the Professional cycle provides context. The Application component of the professional cycle is of particular importance since effective implementation of risk management is necessary for the long term survival of any organisation. The Risk Governance risk in the IAA high level risk definitions attests to this.

These elements are placed in the context of the actuarial control cycle paradigm in the following sequence of diagrams. Some additional entries are included for context.

Risk management framework in actuarial control cycle paradigm



Annex 3 ROTF Terms of Reference

These ROTF Terms of Reference (ToR) were formally approved by the IAA Audit and Finance Committee 19 May 2015.

1 Context

The current (2011) Terms of Reference of the Audit & Finance Committee Includes:

> *4.2.2.(e) The Audit and Finance Committee shall be responsible for oversight of the IAA's risk management, including (i) identifying key risks to the IAA, (ii) quantifying risk exposures, (iii)assisting Council in defining risk tolerance, (iv) recommending risk management actions, and (v) providing risk information needed to support strategic objectives and decisions. The Audit and Finance Committee shall produce an annual report to Council on its oversight of risk management.*

2 Risks to be considered

Risks to be considered by the ROTF are those that are relevant to the IAA as an organization.

Relevant stakeholders of the IAA will be surveyed to assist the identification of risks relevant to the IAA. The survey will include, but not necessarily be limited to, IAA Council, IAA Sections, IAA member associations, and the IAA Secretariat.

3 Risk management strategy

The ROTF will review existing IAA risk management strategies and how they are promulgated to and from current committees and the Secretariat. It will comment on them and provide recommendations for change.

4 Internal processes and controls

The ROTF will review existing IAA risk management internal processes and controls and how they are promulgated to and from current committees and the Secretariat. It will comment on them and provide recommendations for change.

5 Risk register

The ROTF will review the existing IAA risk register, for both current committees and the Secretariat. It will comment on them and provide recommendations for change. It will update them appropriately and reflect any additional material risks identified.

6 Risk reporting and risk maps

The ROTF will review existing IAA risk reporting and risk maps and how they are promulgated to and from Council and current committees and the Secretariat. It will comment on them and provide recommendations for change. It will update them appropriately and reflect any additional material risks identified.

7 IAA Risk Appetite and Tolerance Statement

The ROTF will draft an initial IAA Risk Appetite and Tolerance Statement for the purposes of this Task Force. This is required to provide a basis against which risks to the IAA may be assessed. See also items 2.2 and 2.3.

8 Constraints and Limitations

Cost: No significant expense outlay or risk modelling is expected to be undertaken.

IAA Risk Appetite and Tolerance Statement: This Statement, ultimately, needs to be adopted and signed off by the Audit and Finance Committee.

9 Term and termination

Term: The ROTF has a limited term and is not intended to have an ongoing role or existence.

Termination: On delivery of the final ROTF report to the Audit and Finance Committee

Annex 4 IAA Strategic Plan (as at May 2013)

Vision Statement

The actuarial profession is recognized worldwide as a major player in the decision-making process within the financial services industry, in the area of social protection and in the management of risk, contributing to the well-being of society as a whole.

Mission Statement

The mission of the IAA, as the worldwide organization of actuarial associations, is:

- to represent the actuarial profession and promote its role, reputation and recognition in the international domain; and
- to promote professionalism, develop education standards and encourage research, with the active involvement of its Member Associations and Sections, in order to address changing needs.

Values Statement

The IAA adheres to the values of integrity, accountability, transparency, and objectivity when dealing with Member Associations, other stakeholders and the public.

Strategic Objectives and Priorities/Action Plans

Strategic Objective 1: Identify, establish, promote and maintain relationships with key supranational audiences and provide them with actuarial input to improve the soundness of decisions being made on important issues with a global impact.

Priorities/Action Plans

1. Identify and prioritize relevant supranational organizations with whom to establish and maintain key relationships.
2. Bring key relationship bodies into contact with the relevant actuarial groups.
3. Build and maintain key relationships.
4. Provide relevant supranational organizations with actuarial input on matters of importance.

Strategic Objective 2: Facilitate the coordination, use and expansion of the scientific knowledge and skills of the actuarial profession, including beyond the traditional areas of actuarial practice, to help enhance the scope, availability, and quality of actuarial services offered by individual members of its member associations.

Priorities/Action Plans

1. Identify and prioritize fields of practice and develop a program to support each area.

2. Create strong links with non-actuarial international organizations in “wider fields”. (links to Strategic Objective 1)

3. Support Full Member Associations in the promotion and development of actuarial practice in Enterprise Risk Management, including the CERA designation.

4. Facilitate the coordination of research among Full Member Associations.

Strategic Objective 3: Establish, maintain and promote common standards of actuarial education and common principles of professional conduct. Promote the development and issuance of actuarial standards in the jurisdictions of all Full Member Associations, and the global convergence of actuarial standards.

Priorities/Action Plans

1. Maintain and promote basic education standards to ensure they remain up to date.

2. Maintain and promote a recommended set of continuing professional development (CPD) guidelines.

3. Maintain and promote a common understanding of the principles of professionalism, including code of conduct and disciplinary procedures.

4. Develop model standards of practice.

5. Periodically monitor activities of Full Member Associations (FMAs) with respect to these action plans.

Strategic Objective 4: Support the development, organization and promotion of the actuarial profession in areas of the world in which it is not present or is not fully developed.

Priorities/Action Plans

1. Help emerging and recently established actuarial associations to develop and assist existing member associations, on request, to continue their development.

2. Facilitate the progress of newly established associations towards becoming Full Member Associations of the IAA.

3. Leverage the volunteer capability of Actuaries Without Borders (AWB) and FMAs to fulfil the objective.

4. Increase awareness and recognition of the profession in new countries.

5. Facilitate interchange of information, experiences and transferable models between countries with a developing actuarial profession and with more developed FMAs.

6. Assist newly established local associations to promote the role of actuaries and to grow the global brand.

Strategic Objective 5: Provide a forum for discussion among actuaries and actuarial associations throughout the world.

Priorities/Action Plans

1. Encourage forums for actuaries to discuss global actuarial issues.

2. Encourage discussions between association Presidents.

3. Encourage not only worldwide, but also regional contact and cooperation among member associations.

Strategic Objective 6: Improve recognition of the actuarial profession among external audiences, including employers, other professionals, academics, business at large, policy makers, regulators, students, and the public.

Priorities/Action Plans

1. Build an actuary brand to increase the breadth of awareness of the skills and training of actuaries in traditional and non-traditional areas of practice;

2. Promote the recognition of the actuary as a professional governed by codes of conduct, professional standards, and a disciplinary process; and

3. Work in conjunction with local member associations to communicate the brand message internally within the IAA, its member associations, and actuaries worldwide.

Annex 5 IAA High level risk definitions

Strategic Risk:

This is the risk that the organisation may not meet its strategy or strategic objectives due to failed, inadequate or incomplete setting, evaluating, monitoring, executing and managing strategic and business planning. A key aspect to strategic risk management is the organisation's identification, development and management of its strategic assets.

Commentary:

- Strategic risks emerge from the strategies the organisation chooses to pursue, hence the importance of the organisation setting clear and well thought out strategies and then managing them effectively. The focus of strategic risks is organisation's long term place in, and relations with, the outside environment. Some strategic risks relate to internal functions but the focus of these is the bearing they have on the organization's situation in relation to its environment.
- Strategic assets may be varied in nature and failure to identify and manage them well is a strategic risk. Vital strategic assets include an organisation's human capital (employees, partners, and contractors) and innovation.
- The primary responsibility for strategic risk management lies with the most senior governing body of the organisation. Addressing this risk reflects the Specify (in the sense of 'set policy') element of the 'Specify-Solve-Monitor' actuarial control cycle.

Reputational Risk:

This is the risk that the organisation may not meet its objectives due to failed, inadequate or incomplete perceptions of its character, integrity or quality which are called into question by activities of the organisation or an individual seen as being representative of the organisation. The outcome is that behaviours or perceptions of external parties change adversely from those the organisation desires.

Commentary:

- Core to an organisation's reputation are the perceptions of groups and individuals external to the organisation. As such the organisation may have limited control over these perceptions. An important aspect of reputation management is the monitoring of how the organisation is perceived by its stakeholders, how those perceptions are propagated, and how they may be positively influenced. The rise of new technologies and social media illustrates both ways in which this may change and the rapidity with which such changes may take place.
- Addressing this risk reflects an aspect of the Solve element of the 'Specify-Solve-Monitor' actuarial control cycle.

Operational Risk:

This is the risk that the organisation may not meet its objectives due to failed, inadequate or incomplete internal processes, people, systems, controls, or due to external events.

Commentary:

- This includes legal risk, but excludes reputational and strategic risks. In contrast to strategic risks, Operational risks are more focussed on risks and issues relating to with the implementation of strategies, and so in some instances may have more short term focus. All activities of the organisation involve some element of operational risk. There remains, however, a strong interaction between operational capacity and appropriate strategic objectives.
- Addressing this risk reflects an aspect of the Solve element of the 'Specify-Solve-Monitor' actuarial control cycle.

Financial Risk:

This is the risk that the organisation may not meet its objectives due failed, inadequate or incomplete financing methods or outcomes.

Commentary:

- This includes both the income and outflow aspects of financial management and protection (including insurance covers). It also includes the management of financial objectives, including both revenue generation and investment management.
- Addressing this risk reflects an aspect of the Solve element of the 'Specify-Solve-Monitor' actuarial control cycle.

Risk Governance:

This is the risk that the organisation may not meet its objectives due to failed, inadequate or incomplete processes for the monitoring and reporting of risks and their management. It includes external compliance (legal, regulatory, tax, financial and so on) obligations, internal process documentation and compliance, and audit requirements and activities. It includes an organisation's approach to its risk management and resilience to risk events reflecting its culture, attitudes and incentives as shown through behaviours. It also includes 'implementation risk', the risk of implementing tasks in a way that delivers outcomes that are not those intended and may not address user expectations or needs.

Commentary:

- Corporate governance covers all aspects of the way an organisation governs and manages itself and is a broader concept than the way in an organisation manages its risk profile, which is the focus of Risk Governance.
- Addressing this risk reflects the Monitor element of the 'Specify-Solve-Monitor' actuarial control cycle.

Other Risk:

These are the risks that the organisation may not meet its objectives due to identified risks not included in other specific categories.

Commentary:

- Such risks may be transitory, due to specific environmental conditions or specific special circumstance of the organisation at a particular point in time. They may also be comparatively speculative, in that they are on the risk horizon of the organisation, but are not yet sufficiently well characterised to be able to be incorporated into a more standardised risk management process.
- Such risks also include those that may not yet have been specifically identifying as part of the ongoing risk management process.
- Such risks also include those which are currently ‘unknown unknowns’.

Annex 6 Risk impact

1 Impact of Risk Events

Each potential risk event is assessed in terms of its potential impact on the organisation.

As indicated before, assessing the impact of a risk event is split into three steps:

- Assess the likelihood (or frequency) of a risk event occurring.
- Assess the consequence (or severity) of the risk event, assuming the risk event occurs
- Assessing the overall resulting impact of the risk event on the organisation reflecting both the consequence and likelihood of the risk event.

The consequences and impact of a risk event may have a number of dimensions, such as a financial impact, a reputational impact, and so on. That is, a risk event may have a 'footprint' across more than one risk category. Where this is the case, the overall impact is taken as the worst of the impacts over the risk categories.

Since the impact depends on the assessed likelihood and consequences, there are discussed and then the overall assessment of impact is given in a table.

2 Likelihood of Risk Events

These indicative likelihoods represent the expected values for the five categories used.

Risk Likelihood Table

	Indicative Likelihood
Rare	Less than once every 5 years
Unlikely	Once every 2 - 5 years
Possible	Once every 1 - 2 years
Likely	Once every 1 month – 1 year
Almost Certain	More than once a month

3 Consequences of Risk Events

When indicative expected consequences of risk events, when they occur, are given the impact of a risk event can be assessed. Indicative consequences represent the expected values for the five specific categories used.

The following table, 'IAA Risk Consequence Table' covers all the main risk categories considered in this survey and so contains a number of entries.

IAA Risk Consequence Table

Consequence	Insignificant	Minor	Moderate	Major	Catastrophic
Strategic Risk events					
	Ongoing issues that arise in the course of managing the timely delivery of strategic objectives that are managed by those responsible.	Minor threat of delivery or timing of a strategic objetives that can be addressed by those responsible for that objetcive.	Delay or threat to timely delivery of a major component of a stratgeic objective with a need to review or revise.	- Failure of delivery of a significant component of a strategy or - Significant delay in timely delivery of strategic objectives	Failure of delivery of a strategy which is unmanaged and unmitigated and so unexpected
			Inadequate project forecasting of resources necessary to meet strategic objectives(s)	Inadequate provision of resources to meet strategic objectives	Initiation of high profile legal action against IAA
Reputational Risk events					
	Little or no impact on reputation or member (Associations or individuals) numbers	- Minor issues addressed by management or - Member (Associations or individuals) numbers down by < 2%	- Negative image as a result of failures or - 2% to 5% decline in member (Associations or individuals) numbers	- Significant event(s) leading to negative publicity or member cirticiism or - 5% to 10% drop in member (Associations or individuals) numbers or - Failure to grasp a major opportunity	- Significant and sustained negative publicity or member public criticism or - More than 10% drop in member (Associations or individuals) numbers
Operational Risk events					
Operational matters	Activities disrupted for < 4 hours	Key activities disrupted for < 1 day	- Key activities disrupted for > 1 day but less than < 3 days or - Service delivery complaints received from > 5% of members in 1 month	- Key activities disrupted for > 3 days but less than < 15 days or - Service delivery complaints received from > 10% of members in 1 month	- Key activities disrupted for > 15 days or - Many sustained complaints about service delivery
Human Resources	Staff turnover within benchmark and no injuries	- Junior staff turnover above benchmark or - Minor injuries to staff needing first aid	- Senior staff turnover above benchmark or - Injuries to staff needing some medical treatment	- Staff turnover well above benchmark or - injuries to staff needing major medical treatment or - Loss of key staff	- Loss of multiple key Staff or - Prolonged vacancies or Loss of life
Financial Risk events					
	P&L or Net Asset impact < C$50,000, or	P&L or Net Asset impact C$50,000 to C$199,999, or	P&L or Net Asset impact C$200,000 to C$499,999, or	P&L or Net Asset impact C$500,000 to C$999,999, or	P&L or Net Asset impact > C$1,000,000, or
	Less than 1% Budget	1% - 2% budget	2% - 5% budget	5% - 10% budget	More than 10% budget
			Incurring significant unbudgeted expenses	Failure to meet reserve policy	Inability to pay expenses
Risk Governance events					
Culture	Lack of courtesy to fellow workers or members	Attitudes that may be defensive, unsupportive or uncooperative in achiveing goals	- Disrespectful or intolerant workplace attitudes and habits or - Staff or members are fearful of raising issues or questions or feel that such actions will not be treated appropriately	Inappropriate behaviours tolerated on an ongoing basis and supported by inapproriate incentives	Inapproriate or ineffective leadership that does not clearly demonstrate desired behaviours continuously ('walk the talk')
Reporting and Risk Event management	Late, lax or partial reporting or management of minor risk events tha result in no material adverse consequences	Lack of respect when reasonable potential risks or impediments to proposed actions are raised	Late provision of adeqaute reporting which inhibits proper monitoring, assessment and/or responses to risk events	'- Escalation, delegation and reporting procedures that are not comprehensive, efficient and implemented or - Correct procedures not followed on a consistent and significant basis or - Material breach of security, including possible to loss of confidential information	Deliberate and/or serial inappropriate management of a significant risk event
Regulatory or Compliance	Minor technical breaches or delays	Regulatory or professional breaches managed via normal processes and within budget	Regulatory or professional breaches requiring substanial unbudgeted resources to resolve	Significant regulatory or professional breach involving negative publicity	Major regulatory or professional breach involving external scrutiny or investigation and negative publicity

4 Risk Impact Table

The ROTF has specified a graduated set of impacts based on assessed likelihoods and consequences.

The levels of risk event impact are:

- Extreme: Requires immediate action as the potential risk exposure could be devastating to the organisation.
- Very High: Requires action very soon (within 3 months), as it has the potential to be damaging to the organisation.
- High: Requires treatment with routine or specific procedures.
- Medium: Continue to monitor and re-evaluate the risk, ideally treat with routine procedures.
- Low: Continue to monitor and re-evaluate the risk.

Risk Impact Table

	Likelihood				
Consequences	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost certain
5 Catastrophic	Medium	Very High	Extreme	Extreme	Extreme
4 Major	Medium	High	Very High	Extreme	Extreme
3 Moderate	Low	High	High	Very High	Extreme
2 Minor	Low	Medium	High	High	Very High
1 Insignificant	Low	Low	Low	Medium	Medium

5 Inherent and Residual Risk

The likelihood and consequences, hence impact, of a risk event may be assessed either before or after the results of risk mitigation steps are taken into account. Likelihood, consequences and so impact of risk events are reduced by a variety of mitigation approaches. Making an assessment before taking into account risk mitigation steps means the inherent likelihood, inherent consequences and inherent impact are being assessed. Risk mitigation may focus on reduce either or both the likelihood and the consequence of the

risk event. Making an assessment after taking into account risk mitigation steps means the residual likelihood, and residual impact are being considered.

While the impacts of residual risks are the primary issues to be managed in practice, there is value in explicitly understanding both the characteristics of the inherent risk and the specific mitigation steps taken to arrive at the residual risks that remain. It is noted that the profile of residual risks may be very different to that of the inherent risks they arise from following risk mitigation steps. Consequently there is value and insight in understanding inherent risks, mitigation steps, and so the resulting residual risks.

In practice, many risks faced by organisations already have risk mitigation steps put in place as a result of natural prudence or past experience. For example, the holding of insurance policies, 'two pairs of eyes' reviewing key documents, and separations of the authorisation and making of payments, the need for a superior or a governing body to approve important activities and policy, and the need for proper accountability and reporting processes, and so on. The development of risk management provides a discipline that encourages the organisation to take a more structured and comprehensive approach to managing its risks with a portfolio perspective in contrast to considering them on a more ad hoc, reactive and individual basis.

6 Inherent to residual risk - Risk Mitigation

Risk mitigation therefore provides a means of adjusting the impact of a risk from being unacceptable to being acceptable.

That is, risk mitigation provides a means of managing inherent risks and transforming them into risks which are acceptable.

Annex 7 IAA Risk Appetite Statement

Key risk	Appetite and tolerances
Strategic	Action Plan execution. This is the major component of IAA activities. Tracking the effective and efficient development, execution and management of these strategies is thus a key component of managing the IAA risk profile. It is recommended that there be a separate RAS item for each IAA Strategic Objectives. Where Action plans for strategic objectives that are either large or have special characteristics, a separate RAS's should be considered. The presumption that all action plans have the same risk appetite is not necessary (the Appetite stated here is at a portfolio level, not the component level). Appetite: Low Tolerance: The IAA recognises that variance from action plans may occur for many reasons. The IAA will monitor progress of its strategic action plans on an ongoing basis and manage variance from those action plans proactively. In particular, this includes the proactive management of changes in stakeholder expectations.
	External opportunity. The environment in which the IAA is operating is constantly evolving and it must be expected there will be may arise significant opportunities for the future of the IAA and the profession. To remain relevant and sustainable, the IAA must monitor the environment on an ongoing basis, and respond to such opportunities when desirable and there is benefit to the IAA and the profession. In considering opportunities a disciplined approach to the management of risks must be taken. Appetite: Medium Tolerance: The IAA will endeavour to identify such opportunities, and respond to the underlying strategic issues in a coordinated way. The IAA will tolerate some non-financial business or professional risks where the long term rewards to the IAAA or the profession are considered to be sufficiently important to justify the risk.
	External threat. The environment in which the IAA is operating is constantly evolving and it must be expected there will be may arise significant threats to the future of the IAA and the profession. To remain relevant and sustainable, the IAA must monitor the environment on an ongoing basis, and respond to mitigate these threats where possible. Appetite: Low Tolerance: The IAA will endeavour to minimise the impact of such threats, and address the underlying strategic issues in a coordinated way.

Key risk	Appetite and tolerances
Reputational	Appetite: Nil There is no appetite for damage to the reputation of the IAA and/or the profession Tolerance: It is possible that some reputational damage may occur that is outside the control of the IAA. The IAA will act to minimise and/or mitigate such damage where possible.
Operational	Operational matters - Stakeholder services Appetite: Low. There is a low appetite for running the organisation in manner that does not meet the service expectations of members and stakeholders. This implies the need to clarify member and stakeholder reasonable expectations so they can be assessed against identified benchmarks. Tolerance: See Risk Consequence Table. The IAA objective is to provide good member and stakeholder service at all times. However the lean resources of the Secretariat and heavy reliance on volunteers suggest that poor service incidents may occur. Every reasonable effort will be made to minimise the number and impact of such incidents.
	Operational matters - IAA processes and systems Appetite: Very Low for operational decision making, processes or systems that do not have a sound and justifiable basis. Tolerance: From a Secretariat perspective, breaches will be tolerated for minor day-to day operational decisions which are corrected, but all other breaches must be reported to Audit and Finance Committee and Executive Committee. From the perspective of IAA committees, sub-committees, Working Groups, task forces or Sections minor breaches will be tolerated subject their correction and reporting to Executive Committee and Audit and Finance Committee. Breaches with a possible larger impact in any dimension, with all mitigating steps being taken, are to be reported to the Audit and Finance and Executive Committees
	Human resources – Volunteers Appetite: Very Low. There is very low appetite for a reduction in volunteer support that materially impacts the IAA's capacity to provide services and fulfil is strategic objectives. Tolerance: It is acknowledged there will be times when volunteers for key roles cannot be found, and that may impact of service levels and the attainment of strategic objectives in a timely manner.
	Human resources - Secretariat Appetite: Very Low. There is a very low appetite for compromising staff safety and welfare Tolerance: Some breaches may occur in the course of normal operations but they should be minor and will be rectified immediately.

Key risk	Appetite and tolerances
	Risk management process and controls – implementation Appetite: Low Tolerance: It is recognised that implementation of risk management processes and controls is an imperfect science'. Consequently; effective risk management is supported by good processes and controls, but is not replaced by such. The role and value of judgement and experience is assessing risks, both in terms of prospective impacts and in terms so consequences of risk events should not be discounted.
	Business Continuity (this covers the external events item in the standard OpRIsk definition) Appetite: Low Tolerance: It is recognised that 'stress testing' Business Continuity Plans may be difficult in the absence of actual events. However, scenario testing and independent expert review should be sought considered.
	Compliance. Audit, professional, regulatory and legal requirements (that is all these items are attributed the same risk appetite) Appetite: Nil Tolerance: Any breach or identified potential breach of legal or regulatory obligations is to be rectified with an urgent and immediate response. Every effort will be made to repair any breaches or potential breaches and to take steps to prevent such breaches from compromising the public reputation of the IAA, the actuarial profession, or IAA members.
Financial	Appetite: Very Low Financial viability of the IAA over the short, medium and long terms must be highly certain (that is all these items are attributed the same risk appetite) Tolerance: See Risk Consequence Table
Risk Governance	Risk culture: It is widely accepted that the risk culture of an organisation is crucial to its success in the context of risk management and that clarity and commitment of leadership ('tone from the top") to both members and employees is a core component in defining the risk culture. An effective risk culture supports the asking of questions and accepts that 'false alarms' ere an inherent aspect of an open and inclusive risk management culture Appetite: Very Low. The tolerance of behaviours and attitudes that do not support an open and inclusive risk management culture is very low. Tolerance: It is acknowledged that different cultural perspectives may influence perceptions of risk and how it may be best managed. However, such differences should not impede to effective management of the underlying risks.

Key risk	Appetite and tolerances
	Risk policy (Council and its delegates): The intent of an RMF is to be fully inclusive. It is acknowledged that, in practice, this is unlikely to occur. This indicates the need for flexible and open-ended risk management policies, processes and controls, designed and open to catering to the unexpected and unforeseen. Appetite: Low Tolerance: It is recognised that in some instances risk policy may not have consider particular risk and their consequences. The tolerance for new issues should therefore be higher than that for repeating issues. The processes for dealing with new issues also needs to be flexible and adaptive, responding to the reality that new issue may also not initially be well defined.
	Risk monitoring and reporting (by Secretariat to various Committees and relevant interested parties) Appetite: Low Tolerance: As with all reporting, reporting of risk related issues (both prospective and for risk events that have occurred), needs to be timely, concise, reliable and informative to the intended audience and consistent with its users objectives.
	Risk event management. The management of risk events after they occur. This is an essentially different topic compared to risk mitigation prior to risk events occurring, since it addresses managing the consequences of risk events that have taken place. Appetite: Medium Tolerance: The initial focus on risk events is to contain and quarantine possible damage, both financial and reputational. Then appropriate investigation into root causes and so appropriate corrections can be made. Learnings from risk events should be incorporated into future risk management approaches. Particularly in the case of risk event that may have an adverse impact of IAA reputation, it is noted that recant times may need to be quick and precise in order to limit damage. Scenario testing and having expert advisors on in place prior to risk events occurring is recommended.
Other	Such risks, since they are not covered by/include in the key high level risks identified above are, by their nature, unknown or unexpected. Consequently they require attention and analysis, and should not be ignored. Appetite: Low Tolerance: Difficult to specify as it requires analysis of the risks which implicitly remains to be addressed. Scenario testing is recommended as means of developing risk management capacity in this area.

Annex 8 Business Continuity Planning

1 Definition

A Business Continuity Plan (BCP) provides a plan to enable an organisation to continue in operation in the face of some kind of interruption to its normal operation. The BCP needs to be appropriate to the nature and severity of the interruption and objectives, resources and complexity of the organisation.

Notes:

- Business Continuity Planning is the process by which a BCP is developed, reviewed, and maintained over time. Disaster Recovery Planning (DRP) is a subset of BCP.
- In terms of the IAAs risk classification, BCP is a component of Operational Risk.

This definition focuses on the actions to be taken when a business interruption occurs. It does not address the broader risk management concern of assessing the likelihood of such interruption occurring. It may be that he likelihood of an interruption occurring is a factor the effort (cost) borne in addressing its consequences, particularly if there are limited resources available to allocate. It is also presupposed that a workable definition of 'interruption' is in place. That is, establishing what criteria need to be met in order for the BCP to be activated to avoid relatively small issues (which may just be 'noise' in the context normal operations) inadvertently triggering a reaction that may then be an over-reaction. It is likely that some judgement may be required to manage borderline cases and so an unambiguous process for the determination of when a BCP is to be triggered should be in place.

2 Discussion

Interruptions to the normal operations of an organisation are typically, but not necessarily, due to external sources. Consequently the level of control/risk mitigation with regard to preventing such events occurring may be limited for the organisation (subject to a decision not to participate in activities which may be impacted by such events).

Typical sources of business interruptions often include (some tailoring for the IAA would likely be appropriate):

- Natural disasters (earthquake, flood, hurricane, storm etc)
- Fire
- Disease (epidemic, pandemic)
- War and civil disturbance
- External manmade events (power outage, utility outage, terrorism/piracy, hacking, cyber-attack)
- Theft and sabotage, internal or external (loss of confidential/critical information, loss of business capacity)
- IT systems failure (including severe degradation)

- Failure of (other) mission critical systems (failure of mission critical suppliers)

There may be 'knock-on' effects from one source of interruption to another. For example, loss of people (say from a pandemic), may then compromise the capacity of the business to continue as normal.

3 Typical steps in developing a BCP include

The typical steps in developing a BCP are similar to the following. Sometimes the first 4 steps are put together under the title 'Analysis'. This has not been done here as these steps are each considered important on their own right.

- Critical functions: Determine which functions are critical (and to which stakeholders), and the timeframes for restoration (perhaps not complete) that are acceptable.
- Threats Analysis: Identify the threats and their potential consequences when they occur
- Impact Analysis: Assess the scenarios due to the impact of potential threats on critical functions. It is the impact on the organisation which is addressed, not the cause of the impact. For example if non access to workspace is the threat, the cause of that non access may vary. This may permit some simplification of the BCP when it addresses events.
- Recovery requirements: Identify how issues may be controlled, and then the needs for remediation. This includes physical resources needed (eg temporary office space, temporary staff (training and instruction), key backup systems and data need to be accessed, temporary/ manual 'workarounds' for critical functions, supplies of materials, how to defer/manage non-critical functions, financial resources to be called on (including insurances), expected time frames for full recovery
- Solution design: identify cost effective solutions which meet the requirements of the recovery requirements. This includes all the management aspects for implementing a recovery. For example, identification of relevant people and processes to make decisions (for example, ensuring key people are contactable), determination of secondary worksites and equipment, communications with and management of stakeholders and their expectations (including timelines for resolution of services).
- Implementation: Executing the design requirements identified. Develop a BCP manual which explains roles, responsibilities and governance processes. Ensure the appropriate training takes place and access to the manual is assured (in the interruption). At the very least a sheet with appropriate contact details and high level governance responsibilities should be prepared. Clear and comprehensive documentation in the BCP manual is important.
- Testing and Acceptance: This is to achieve organisational acceptance of solution and to check it satisfies the organisation's recovery needs. It also is to ensure that people have sufficient familiarity with the needs of and approach to managing stressful or crisis situations before these situation arise. Various level of testing can be conducted depending on the nature and severity of the disruption to the organisation.

- Maintenance: This often consists of three elements: Confirmation of ongoing currency and completeness of information in manual, testing of solutions in the manual (testing may be at different levels from desk top review, through enacting scenarios with varying levels of complexity and severity), confirmation the solutions in the manual remain pertinent and adequate for the organisation. Maintenance is usually recommended to be done on an annual or biannual basis to retain familiarity with the BCP and to address staff and stakeholder changes. The control cycle link back from testing to analysis and subsequent updates of the BCP is noted.

There are national and international standards (ISOO 22301:2012, ISO 22313:212) available to support to development of BCPs. There is also information and guidance available on the web. This includes a considerable range of free material, guidance and templates (often provide from governmental sources).

Annex 9 ROTF Survey

Results from the 2015 ROTF Risk Survey were organized by category and summarized by the major risk categories given in section 3.2 and Annex 5.

Risk	Count	Risk category	Subtotal
Failure of IAA to achieve recognition	11	Strategic	
Failure to recognize/ lack of quality of ISAPs	9	Strategic	
Profession becoming irrelevant	8	Strategic	
Failure of actuaries to perform	3	Strategic	
Governance failure	3	Strategic	
Political risk	2	Strategic	
Instability of insurance market	1	Strategic	
Missing growth opportunities	1	Strategic	
Education failure	1	Strategic	
Overproduction of actuaries	1	Strategic	
One or more FMAs try to usurp IAA position	1	Strategic	41
IAA embarrassing statement (officer or published paper)	11	Reputation	
Actuary embarrassing statement	9	Reputation	
Irrelevance of IAA to actuaries in day to day practice	2	Reputation	
Communication with regulators	2	Reputation	24
Membership drop	9	Financial	
Funding failure	8	Financial	
Compliance costs	1	Financial	18
Office disasters	13	Operational	
Member problems	9	Operational	
Caliber of staff and volunteers	8	Operational	
Staff turnover	2	Operational	
Inability to react timely	2	Operational	34
Staff or officer fraud	2	Risk governance	2
-	0	Other	0
Total	**119**		**119**

Annex 10 IAA risk management responsibilities

1 Council

- Has the ultimate responsibility for IAA risk management, its policy, processes an controls
- Delegates operational oversight of risk management related matters to the Executive Committee and Audit and Finance Committee
- Approves the risk management framework and its ongoing appropriateness
- Reviews and approves the IAA Risk Appetite Statement annually
- Monitors progress towards achievement of strategic objectives within the context of the Risk Management Framework
- Monitors the management of IAA risks and risk events, supported by reporting from the Risk Register
- Monitors the appropriateness of Executive control of risk management related matters

2 Executive Committee

- Ensures risks are appropriately managed in line with current Risk Appetite Statement as approved by Council
- Owns and manages the processes and controls required to operationalise the risk management framework supporting the strategic direction set by Council
- Reports regularly to Council on risk management activities, progress and issues
- Provides and receives reports to and from the Audit and Finance Committee and responds formally to the Committee on any decisions taken and matters discussed
- Ensures that appropriate Risk Management is included in the activities of Committees, sub-committees, Working groups, Task forces and Sections.
- Oversees the operation and risk management of the IAA and holds the Secretariat accountable for their activities
- Contributes individual professional expertise to risk identification and evaluation
- Considers overall risk environment when making policy decisions and recommendations

3 Audit and Finance Committee

- Provides oversight to help Council ensure that key risks are identified and addressed. This includes the IAA adopting a sound approach to assessing the financial impacts of risks and their reporting

- Reviews the approach to the identification of the key risks that might affect the achievement of strategic objectives, how these risks are being monitored and the steps that are taken to mitigate those risks with a view to ensuring they are within the parameters of the IAA Risk Appetite Statement.
- Reviews Executive Committee's reports on the effectiveness of the IAA processes and control systems for risk management and the financial consequences of risk management and risk events
- Reviews the policies and processes for identifying and assessing risks and the management of those risks by the International Actuarial Association
- Reviews the Risk Register and its effective operations

4 Committees, subcommittees, Working groups, task forces and Sections

- Ensure that their terms of reference and activities include risk management assessments and, when appropriate, projects have in place adequate risk mitigation steps
- Risk management considerations are to be included in the operational component of their terms of reference and consequently are to be reported on at least annually
- Consider overall risk environment when undertaking projects and activities
- Manage identified risks in line with the Risk Appetite Statement as approved by Council
- Report to Executive Committee on identified risk events and their management

5 Secretariat

5.1 Executive Director (Chief Risk Officer)

- Responsible for the operations of the Executive
- Ensures the Risk Management Framework is maintained and manages all relevant risks and risk events in accordance with the current Risk Appetite Statement as approved by Council
- Ensures Executive Committee is regularly advised on the current and future relevant risks to the IAA and the management of risk events
- Contributes professional expertise to risk identification and evaluation
- Considers overall risk environment when making policy decisions

5.2 Director of Operations (Risk Management Function)

- Responsible for co-ordination of all risk management activity and providing appropriate Operational and Strategic Risk input to the Secretariat Directors Group

- Reviews all operational risk management activity and provides additional guidance to Directorates and Projects as appropriate
- Conducts research into market and other developments which could develop into potential new strategic risks or opportunities for IAA
- Maintains up to date Risk Register of all potential risks to the IAA and the management of risk events
- Produces reports on an agreed regular basis from the Risk Register to effectively inform the Secretariat, Audit and Finance Committee, Executive Committee, and Council.
- Agrees Risk Mitigation Action Plans for managing risks with relevant Directorates and Projects

5.3 Secretariat Directors Group

- Responsible for reviewing all IAA Risk Management activities and agreeing appropriate recommendations for the Executive Committee and Council.
- Implement risk management decisions agreed by Council and Executive Committee respectively.
- Evaluates continuing operation of Risk Management Framework and supporting processes and controls
- Reviews IAA Risk Register and reporting from it
- Agrees IAA wide action plans for dealing with specific risks
- Prepares Risk management reports for all Council and Executive Committee meetings
- Reports to Executive Director on experience and outcomes of current Risk Appetite Statement parameters
- Contributes individual professional expertise to risk identification and evaluation
- Considers overall risk environment when making policy decisions

5.4 Individual Secretariat Directorates

- Responsible for day-to-day operational risk management and identification of potential new strategic risks within the Directorate
- Identifies and evaluates potential new risks
- Manages a Directorate (Project) Risk Register which is integrated into the IAA Risk Register as maintained by the Director of Operations (Risk Management Function)
- As a Risk Owner manages risks in accordance with IAA operational risk management processes

- Identifies risks of potential strategic significance to IAA and raises with Director of Operations (Risk Management Function) and Secretariat Directors Group
- Manages Directorate aspects of IAA action plans for all risks

5.5 Individual members of Secretariat staff

- Be aware of the need to manage the risks to achieve their agreed objectives
- Work within the defined risk management processes and controls for their respective directorates
- Contributes their knowledge and experience to help develop the process
- Reports any potential new risks or risk events they have identified
- Identifies any inefficient or ineffective risk management practices or controls

5.6 Internal Audit function

- Develops a risk based internal audit programme
- Audits the risk processes across the organisation
- Receives and provides assurance on the management of risks and risk events
- Reports on the efficiency and effectiveness of internal processes and controls
- Audits ongoing compliance with external legislation and regulation

International Actuarial Association
1203-99 Metcalfe St.
Ottawa, ON K1P 6L7
CANADA
secretariat@actuaries.org