

# AAE Risk Policy

## RISK REGISTER

The first step, if it does not already exist, is for the AAE Executive to create a Risk Register for the AAE. This should itemise the main risks that the Executive thinks that the organisation faces, and then for each risk identify:

1. A general description of risk to indicate why relevant to AAE, and perhaps category, to the extent that it seems appropriate to group risks into different types
2. What mitigations are in place, e.g. one risk could be sending out erroneous material. A mitigation could be to have checking procedures in place to limit the risk of this happening
3. Likelihood (maybe scored 1 low to 5 high) (both gross and net of mitigations)
4. Impact (maybe also scored 1 low to 5 high) (both gross and net of mitigations)
5. Some combined score derived from (c) and (d) (there is no universally agreed approach on how to do this)
6. Who 'owns' the risk (i.e. who is responsible for the risk and for making sure that any mitigations the organisation is relying upon to limit the risk are actually being applied in practice)
7. When the risk will next be reviewed within the Executive

## BOARD SUB-COMMITTEE

Alongside a risk register, it is likely to be helpful to establish a Board sub-committee focusing on risk management, or to add specific responsibility for risk management to an existing Board sub-committee. The sub-committee would then:

1. Review the risk register from time to time, challenging the Executive when a risk does not appear to be included that should be, or is mis-specified, or where existing / proposed mitigations and/or ownership or policies to address the risk seem inadequate
2. Prepare some articulation of the organisation's risk appetite, bearing in mind the types of risks to which the organisation is exposed (hence the need to do alongside (1)), its financial position (so typically the Treasurer or equivalent would be heavily involved in and probably chair the risk management sub-committee)

3. Hold the Executive to account if the actual risks the organisation is running fall outside its agreed risk appetite
4. Report to the Board from time to time about the risks being faced by the organisation. This could take the form of the Board receiving the latest available risk register and the sub-committee chair indicating the level of challenge of the risk register by the sub-committee and issues that need addressing

## WHAT HAVE OTHER ORGANISATIONS DONE?

To assist with the previous chapters, it is likely to be helpful for the AAE to reach out to other similar organisations to get hold of which risks they think are relevant to them and their experience in how best to set up formal structures to look after them. For example, I believe that the IFoA now has a specific employee who is charged with looking after their risk management (Kartina is perhaps best placed to introduce him to you or Monique), and maybe other AAE Member Associations do likewise.

## DEFINITIONS

### Board

By “Board”, in the above, I mean the body that is legally responsible for the operation of the organisation, which for the AAE presumably means its Board. To ensure that the Board does take adequate responsibility for the risk management of the organisation for which it is responsible, it helps to have a formal structure, i.e. either a formal Board sub-committee, probably chaired by a Board member, looking after this activity, or for the Board itself to do so (but it would then be necessary to ensure that adequate time is given to this topic in the Board’s agendas).

An advantage of establishing a specific sub-committee is that it may then be easier to involve others not on the Board in such debates. I could for example, approach the RMC to see if there are members of the RMC who would like to join such a sub-committee. A sub-committee is probably also a good way of capturing other related topics. For example, a charity, say, would typically need to articulate its risk management approach in its published report and financial statements, and a sub-committee structure would provide a ready sounding board for how best to do so.

### Executive

“Executive”, in the above, I mean the body that actually runs the organisation (under the instruction of the Board).

An important rule in risk management is to ensure that risk management is embedded within the business itself, rather than being an add-on to one side. This means that day-to-day risk management needs to sit within the business, even if alongside this there is a need to have a governance structure in place which ensures, as far as possible, that the organisation’s risk management appetite, policies and practices are up-to-scratch.

## IN ADDITION

In terms of risks to include in the risk register I would certainly include risks along the lines of the following ((a) because it is probably the biggest strategic risk the AAE faces, and hence there should be an emphasis on how it is being mitigated and (b) because I couldn't see from the GDPR paper I was asked to comment on recently how this risk was currently being mitigated by the AAE):

1. Member Associations pull out of the AAE (e.g. because they consider belonging to the IAA is sufficient for their international engagement)
2. AAE incurs legal liability from material it publishes (e.g. material that purports to be factually accurate and is relied upon as such by actuaries or organisations but which is subsequently shown to be erroneous, or e.g. defamatory material)

Malcolm Kemp  
16 May 2018