The OfS approach to risk management

Introduction

The attached paper was discussed at a meeting of the Risk and Audit Committee (RAC) on 26 January. The Committee would welcome comments from the Board on the overall approach set out in the paper, the categories of risk and the initial risk appetite approach and assessment set out in the paper. The senior team will then take forward work on the risk management approach and associated risk register under the oversight of the Committee.

OfS Risk Management Approach

OfS Risk and Audit Committee
26 January 2018

Issue

1. For the Risk and Audit Committee (RAC) to discuss how the OfS will approach risk management.

Recommendation(s)

2. The RAC is invited to consider the:

   a. suggested risk appetite and tolerance levels
   b. draft risk escalation process
   c. suggested three lines of defence
   d. suggested approach to reporting against risk

Timing for decisions

3. The RAC is invited to have a discussion now in order that it can make recommendations to the OfS Board meeting on 26 March on the risk management approach.

Discussion

Background

4. In November the OfS Shadow Board considered a paper on the 'OfS Proposed Approach to Risk'. This paper outlined, at a high level, an initial approach to risk which was endorsed by the Board. In addition, the Board agreed that:

   a. The OfS Risk Register should be taken forward with the advice of the OfS Audit and Risk Committee (now renamed the Risk and Audit Committee (RAC)), with a view that the Register should be operative from January 2018.

   b. A Provider Risk Committee should be established, to be responsible for authorising any significant registration decision affecting providers as part of the OfS responsibilities under the Regulatory Framework. This will be a separate OfS Board committee and is outside the scope of this paper.

   c. There are 5 categories of risk:

      i. Strategic
      ii. Regulatory
      iii. Reputational
      iv. Operational
      v. Transitional

5. A draft risk log was also tabled at its November meeting, providing the Board with an initial overview of the key risks. This was informed by the DfE risk register and the outcome of a risk pre-mortem session on 22 November 2017. This session identified the challenges that could cause failure for the OfS and was attended by the OfS senior leadership team and the DfE HE Reform team.

6. Following both the pre-mortem and the Board discussion we have been considering what the OfS' approach to risk might look like. To do this we have drawn on the HMT Orange Book[1] which sets out guiding principles for how Government Departments should manage risk and promotes robust risk management practices in Government sectors. We have also drawn on the experience of UKSBS[2] which has extensive experience and a mature risk management approach. In addition, we have also drawn on other management standards such as Prince2.

7. As the OfS' risk maturity increases over time the RAC may want to refine its approach, however we have taken a more standard approach at this point because:

   a. the OfS is a new organisation

   b. it will support the OfS in its discussions with the NAO (its external auditors) and Ernst and Young (its internal auditors) during its first year of operation. The experience at UKSBS supports this approach where it has seen the number of NAO audit days reduce by 50 percent as its risk maturity has grown and it has implemented a recognised standard (the HMT Orange Book).

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

[2] UK SBS is a Company wholly owned by its public sector customers and shareholders: the Department for Business, Energy and Industrial Strategy (BEIS), the seven UK Research Councils, Innovate UK and HEFCE. It is a recognised government Shared Service provider.

Risk appetite

8. The OfS Board will need to agree its risk appetite and risk tolerance levels following advice from the RAC. In order to provide this advice we would like the RAC to consider Table 1 below. Specifically, we would like the Committee to consider whether the right risk appetite has been attached to the risk categories. So, for example, is setting the risk appetite for the Operational risk category as 'Minimalist' correct.

9. It should be noted that the risk appetite statements set out in Table 1 are taken from the HMT Orange Book.

Table 1: Risk appetite statements

Ref	Risk Category	Risk appetite statement	Risk appetite
1		Avoidance of risk and uncertainty is a key objective	**Averse**
2	Operational	Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited reward.	**Minimalist**
3	Regulatory, Reputational and Transitional	Preference for safe options that have a low degree of residual risk and may only have limited potential for reward.	**Cautious**
4	Strategic	Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.	**Open**
5		Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risks).	**Hungry**

Risk tolerance

10. Based on the risk appetite statements above we have suggested the risk tolerance levels for each risk category, which are set out below. We would like the Committee to consider whether the risk tolerance for each category is appropriate. To do this the Committee may want to note that for some areas the OfS would be accepting more risk than in others. So, for example, because Strategic is set at 'open' we would be accepting more risk than Regulatory, which is set at 'cautious'.

11. The Committee may also wish to note that the risk category influences what action will need to be taken. For example, if the probability and impact of a risk was scored at 6 for a Strategic risk, we would not envisage any action being taken because it falls in the green shaded area. However, if a risk was scored at 6 for a Regulatory risk we would expect action to be taken because for these risks the OfS is more cautious and it falls within the amber shaded area.

Strategic - open

probability	Impact				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Regulatory - Cautious

Probability	Impact				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Reputational – cautious

Probability	Impact				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

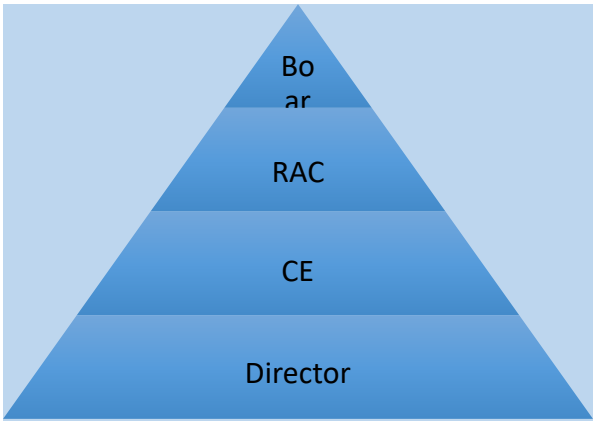
Operational - minimalist

Probability	Impact				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Transitional - cautious

Probability	Impact				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

12. Where a risk falls outside of its tolerance, actions will need to be taken to bring it within tolerance. This will include the development of comprehensive response plans. In addition where this is the case an escalation process will be put in place. A suggested escalation hierachy is shown below for discussion at this meeting:



3 lines of defence

13. In the Three Lines of Defence model, management control is the first line of defence in risk management, the various risk control and compliance over- sight functions established by management are the second line of defence, and independent assurance is the third.

We propose that the OfS risk approach incorporates the 3 lines of defence in the following way:

1st line of defence	2nd line of defence	3rd line of defence
Manage Risk	Oversight	Assurance
Business Owners	Governance Team	RAC/Audit
• Manage risk in line with agreed strategy, risk appetite and tolerance • Establish and operate directorate risk and control structure ensuring operation within agreed policies, procedures and limits	• Establish risk management policies and procedures, methodologies and tools, including risk appetite framework • Facilitate establishment of risk appetite statements with input from senior management and the board • Set risk limits	• Perform independent testing and assess whether the risk appetite framework, risk policies, risk procedures and related controls are functioning as intended • Provide assurance to the board related to the quality and effectiveness of the risk management

• Conduct self-testing against established policies, procedures and limits • Report and escalate risk limit breaches	• Monitor risk limits and communicate exceptions via the agreed escalation hierarchy • Provide risk oversight across all risk types, business units and locations	program, including risk appetite processes

Reporting

14. We propose that the RAC receives a risk report from the OfS at each of its meetings. Given the OfS is a new organisation we propose that this would cover the following:

a. Full risk register
b. A summary report of the amber and red risks
c. Analysis of risk trend

15. We propose that the RAC provides a risk report to the OfS Board at each of its meetings. We propose that this covers the following:

a. A summary report of the amber and red risks
b. Summary/analysis of risk trend
c. The full risk register would be available should they wish to see it.

As the risk maturity grows we expect to review this approach and propose to do so after a year of operation.

Guidance for OfS staff

16. Detailed guidance for OfS staff will be developed once the RAC and Board has agreed the organisations approach to risk management. In addition, we propose staff training is made available.

17. The detailed guidance will be based on the outline process in the table below. Colleagues would be expected to identify risk, assess it, respond, manage and close risks as appropriate.

Table 2: Risk process

OfS RISK PROCESS				
Identify	**Assess**	**Respond**	**Manage**	**Close**
Anyone Anytime Anywhere	Probability Impact Proximity	Avoid Reduce/Mitigate Transfer Accept Enhance	Review Report Escalate Advise Action	Review Resolve Approve Close
• Initial risks identified through facilitated workshops with each directorate • Risks can be raised by anyone at anytime and will be recorded on the risk register by the appropriate directorate or the PMO	• Output of assessment recorded on directorate/programme risk register. • Risks escalated to the corporate risk register if RAG Status is Amber or Red. • Risks measured against tolerance levels set by Board • Outside of tolerance risks reported to the relevant Director and the PMO	• Allocate an appropriate risk response • Develop risk response plan for out of tolerance risks	• Review risks on a weekly basis • Take Action to manage risks down to an appropriate level • Outside of tolerance risks reported to the relevant Director and the Governance team • Receive Advice from SMT/RAC/Board • Action advice received	• When risk is resolved or managed down to an acceptable limit document the reasons why the risk should be closed and request closure of the risk • Governance team to approve closure of risk

In relation to the risk response (column 3 in Table 2 above), some further explanation is provided in Table 3 below:

Table 3: Risk Response

Response	**Explanation**
Avoid	A change is made (e.g., to project scope) to remove the threat or neutralize its effect on project objectives. By taking these steps, the uncertain event can never occur.
Reduce/mitigate	Action to reduce either the probability or the impact of the risk. This, like “Avoid,” is a proactive response category (i.e., action is taken before the risk occurs).
Transfer	The financial impact of a risk can partly be transferred to a third party (e.g., by taking out insurance, or by building penalty payments into suppliers’ contracts for late delivery).
Accept	This is a conscious decision to do nothing. If a risk is accepted, then the situation must be monitored carefully, to make sure that the risk does not move beyond an acceptable level of probability or impact.
Enhance	Proactive response, increasing either probability or impact of the risk (direct opposite to ‘Reduce’).

Risk Register

18. Following the discussion with the Committee a risk register will be created