BBC Trust

Review of risk management

Report by Alvarez & Marsal presented to the BBC Trust Value for Money Committee, 1 July 2015

BRITISH BROADCASTING CORPORATION

Review of risk management

Report by Alvarez & Marsal presented to the BBC Trust Value for Money Committee, 1 July 2015

Presented to Parliament by the Secretary of State for Culture, Media & Sport by Command of Her Majesty
July 2015

BBC Trust response to Alvarez & Marsal's Review of Risk Management

As the governing body of the BBC, the Trust is responsible for ensuring that the licence fee is spent efficiently and effectively. One of the ways we do this is by commissioning and acting upon reports from independent consultants such as Alvarez & Marsal. This report, which has focused on the effectiveness of BBC's risk management, has found that risk is well managed across the BBC's divisions.

Risk management matters

Risk – the combination of the probability of an event and its consequences – is a fact of life. Without taking risks, the BBC would be unable to produce distinctive dramas, report impartial news, broadcast unique radio shows, curate national events, or personalise online content. Risk needs to be well managed therefore to minimise the probability and consequences of negative events, and maximise those of positive events.

This independent review by Alvarez & Marsal asks how effectively the BBC manages risk. The review's scope covers virtually all types of risk the BBC as a public service broadcaster needs to manage; for example risks inherent in maintaining 24-7 broadcast continuity, developing new technology such as iPlayer, or producing ground-breaking programmes which also meet the high editorial standards expected by viewers.

The BBC's approach to risk management is on par with the average UK blue chip firm

Alvarez & Marsal conclude that the BBC's approach to risk management is well considered and provides effective and robust support to the business; in this regard they believe that the BBC's performance is on par with the median performance demonstrated by FTSE 100 companies.

During their review, Alvarez & Marsal carried out a detailed assessment of the BBC's risk management structures and processes which included a staff survey, workshops, interviews and document review. They found the BBC performed particularly well in identifying and assessing how best to respond to risk and in implementing associated control mechanisms to limit the likelihood or impact of risk occurring.

Alvarez & Marsal found that this performance was broadly consistent across all divisions of the BBC and at all levels of seniority within the organisation, which is

indicative of well-established risk management practices. They contrasted this performance with many other large corporate bodies they had encountered where knowledge and understanding of risk management tends to be more inconsistent across different levels of seniority.

The BBC continues to improve risk management

To achieve this degree of maturity in their approach to risk, Alvarez & Marsal found the BBC Executive have introduced and sustained a number of improvements in recent years. These improvements include enhancing the quality of risk information reported to the board, expanding the associated board discussions, transforming the role of the central risk team to offer more support to the business, streamlining pan-BBC boards, and ensuring greater individual accountability – particularly at senior level.

The Executive deserves credit for the significant progress which has been made but it is important to recognise that effective risk management is a continuous process. The following paragraphs set out the next steps needed to continue to improve how risk is managed.

The BBC needs to better define how much risk it wishes to take and where

The amount of risk the BBC wishes to manage varies across the different activities it undertakes. For example a high degree of creative risk taking is necessary to make original and distinctive programmes but at the same time the BBC has (and should continue to have) a very low tolerance for taking risk in relation to health and safety.

An organisation's risk appetite statement communicates to its staff the level of risk that is acceptable, and where risk may be taken. Staff can use this information to help ensure their actions contribute to the organisation's objectives without exposing it to excessive risk, or being too risk averse.

There is scope to improve the BBC's existing risk appetite statement by being more explicit about the different levels of risk the BBC wishes to take on in different parts of the Corporation.

Risk reporting has improved but we expect the BBC to make greater use of the information it holds

Alvarez & Marsal found that the reporting of risk at a senior level has been developing and improving over the past few years, helping to focus attention on the most important risks faced by the BBC.

Although risk reports record the movement since the last report, there was little consistent reporting of longer term trends in risk. For example, reporting did not record how key risks had changed over the past 12 months and whether such risks were generally stable, improving, or deteriorating. This information would help senior decision makers to identify, at a glance, what impact recent changes have had and if further action is required.

The BBC could also do more to use information it already holds to monitor and forecast how risks associated with specific activities are changing. Appropriately defined, such Key Risk Indicators could be used to flag increasing risk in a certain area. In turn, this would enable effective and timely mitigating action to be taken before a key risk becomes reality.

Alvarez & Marsal have identified an opportunity in the long term for the BBC to apply a 'total cost of risk' methodology to more accurately assess whether the organisation is getting value from its investment in managing certain types of well-defined and contained risks. Specific risks, such as cyber security and data loss, which can also be benchmarked, would be particularly suitable for this analysis.

The Trust expects the BBC to consider whether the cost of implementing this new methodology would be justified by the benefits.

Further risk management initiatives should be brought together into a coherent plan

The Executive has a number of ongoing initiatives to improve how risk is managed in the Corporation. These include identifying the organisation's risk management training requirements at each level, updating procedure guidance for managing risk, implementing an action plan to develop the BBC's risk culture, and holding risk identification workshops at senior levels.

The Trust supports all of these actions but we note there is no overarching plan which brings them all together. The absence of an overall plan makes it harder for the BBC to stand back and establish its objectives for risk management, identify how it will know when these objectives are achieved, and determine which activities are the most important.

Over the coming months we expect the Executive to share with the Trust a plan which brings these different activities together. The plan should define overall objectives, deliverables, resources, timetable and individual responsibilities.

This will put the Executive in a strong position to build on the good progress which has already been made and help maintain momentum as future initiatives are implemented.

BBC Executive response to Alvarez & Marsal's review of risk management

The BBC Executive welcomes this independent review of the BBC's approach to risk management commissioned by the BBC Trust from Alvarez & Marsal, which concludes that "the BBC's approach to risk management is well considered and provides effective and robust support to the business in delivering its public purposes."

We are pleased to be considered "on par with the median performance demonstrated by FTSE 100 and Fortune 500 companies."

This review notes in particular that "there is clear support and sponsorship for risk management at senior levels within the BBC. This has led to the implementation of a number of initiatives over the last two years that have improved the corporate process, the quality of controls and the quality of risk reporting, leading to an overall improvement in the visibility and understanding of risk across the BBC."

As acknowledged in the report, although we are already in a very good position, we are continuing to work to improve our risk management processes and culture. In the context of very scarce resources, we have, however, to balance the cost and benefits of further improvements carefully.

With this in mind, we will address the eight recommendations included in the report as follows.

We will implement recommendation 2, to finalise "the development, and achieve senior level sponsorship, of a coherent risk management improvement plan." We will agree in autumn 2015 a roadmap of activities which will include how and when we plan to implement the other seven recommendations in the context of overall BBC priorities.

We will immediately implement recommendation 4, by updating our Risk Management Procedure Guidance "to provide direction on the recording of opportunities as part of the evaluation process when considering and justifying specific risk management options."

We will also begin to work on the following recommendations, with the aim to complete their implementation by the end of 2016:

- Expand the existing Risk Appetite statement by adding more detail in relation to expected risk tolerance levels for different types of risks and renaming it a Risk Attitude statement (recommendation 3).
- Develop a risk awareness strategy that will address the needs of management and operational staff (recommendation 5).

- Determine whether we should upgrade or replace the current corporate risk management system, incorporating the findings of the on-going Governance, Risk and Compliance proof of concept (recommendation 6).

Over the course of 2016/2017, we will

- Review risk data reported to Executive Board to develop metrics "that support a better understanding of operational and strategic risk profile trends and can be used to justify the effectiveness of risk mitigation strategies" (recommendation 1).
- Complete the ongoing work in "developing and implementing a set of Key Risk Indicators, based on the current metrics, such as audience numbers and health & safety incidents, that are captured across the BBC" (recommendation 7).

We will consider how the implementation of a "proof of concept to assess the feasibility of producing a Total Cost of Risk assessment" (recommendation 8) fits with the BBC strategy and priority for resources. The report acknowledges that this is a very ambitious and innovative task, which would make the BBC a leader in cutting-edge risk management. This objective will need to be assessed against competing priorities when the assessment is completed, even if the methodology were only applied to specific risks.

Risk Management at the BBC

Report to the BBC Trust Value for Money Committee

July 2015

Contents

Background

Risk management has established itself as a board-level concern in recent years, partly due to the fallout from the financial crisis and following improvements to the UK's existing corporate governance code. As a result, companies are under increasing pressure from regulators, shareholders and other stakeholders to review and improve their approach to risk management.

Whilst the BBC Executive is responsible for the operational management of the organisation including managing risk, the BBC Trust maintains an active role in risk management as a consequence of its central role in the good stewardship of the licence fee.

Recent governance reviews have seen the relationship between the BBC Trust and BBC Executive develop with the Trust assuming more of an oversight role. At the same time, the BBC has found itself ever-more frequently in the public eye and a new strategy, Delivering Quality First, that aims to deliver £700m of ongoing savings has been launched. These factors, and a desire to continuously improve, have driven the requirements for this independent review of risk management in the BBC, on behalf of the Trust.

This report presents an evaluation of the BBC's approach to risk management, determines the impact of the BBC's culture on managing risk and assesses whether this framework is implemented robustly at both senior and operational levels across the BBC. The report sets out the findings in four key areas: risk management strategy and policy, or the 'tone from the top'; an assessment as to how those policies and processes are implemented; how the BBC's people and culture impact risk management; and an evaluation of how the central business assurance functions contribute to risk management.

Executive Summary

Overall Scope

Risk management is an essential function of the BBC. In delivering its mission to inform, educate and entertain, the BBC needs to take risk from a controlled and informed standpoint. From production to broadcast, technology to finance, major capital projects to talent management; good risk management enables the BBC to take informed decisions and increases its ability to achieve Value for Money (VfM) for licence fee payers.

The BBC Trust commissioned this VfM report on the BBC's approach to risk management. The study was structured around three questions developed to provide both an understanding of the existence of a risk management framework and its effectiveness in supporting the BBC to deliver its Public Purposes. The questions posed were:

1. Is the BBC's approach to risk well considered?

2. Is there evidence that the approach to risk is working well at a senior level?

3. Is there evidence that the approach to risk is working well at an operational level?

Under each key question, a number of factors were considered that related to governance: 'tone from the top', culture, process, quality of information presented and supporting IT systems.

Conclusion

The BBC's approach to risk management is well considered and provides effective and robust support to the business in delivering its public purposes. When considering the BBC's vision 'to be the most creative organisation in the world' and to produce entertaining and engaging content, risks have to be taken. There is clear support and sponsorship for risk management at senior levels within the BBC. This has led to the implementation of a number of initiatives over the last two years that have improved the corporate process, the quality of controls and the quality of risk reporting, leading to an overall improvement in the visibility and understanding of risk across the BBC. When comparing the amount of content that is regularly broadcast against the number of issues that have materialised, risk can be considered to be well managed across the BBC's Divisions. In our professional judgement, the quality of the framework in place can be considered to be on par with the median performance demonstrated by FTSE 100 and Fortune 500 companies. There is work in progress and further improvements are being implemented to drive both a better use of information and a more 'risk-aware' culture. Our recommendations should help the BBC on this journey.

Key findings

The BBC's approach to risk:

The BBC's framework for managing risk is fit for purpose. There is a clear understanding of how risk will impact the BBC's key objectives. Robust controls, such as the Editorial Guidelines and Fair Trading policy, deliver a consistent awareness and understanding of risk management. The 'tone from the top' has been improving but two areas in particular need more focus:

- The BBC has started to develop its Risk Appetite Statement. However, further work is required to define the levels of risk the BBC is prepared to tolerate; and
- The BBC has a number of initiatives, at varying degrees of maturity, that are focused on improving risk management. However, there is not yet an integrated or sponsored plan coordinating these disparate activities.

Risk management at a senior level:

There is strong ownership of risk at a senior level in the BBC, primarily driven by the Single Point of Accountability Initiative. The development of improved risk management information packs has helped to generate healthy discussions of risk and opportunity at the Executive and Divisional Board level and has provided greater understanding of the effectiveness of existing controls and mitigations. A period of stability is now required to engrain these reports across the business.

Risk management at the operational level:

The BBC has sound practices in place which gather risk and event related data at the operational level. A more analytical approach is now required to: provide a better understanding of trends; determine the efficiency and effectiveness of risk spend; and create improved emerging risk monitoring systems with the use of lead indicators.

Areas of strengths of the BBC's risk management approach

The BBC's corporate risk management framework is fit for purpose and aligns with the UK's existing corporate governance code and international standard principles and guidelines with certain areas exhibiting good practice. The cascade of the BBC's public purpose into strategy and related objectives underpins a solid understanding of how risk and opportunity can affect key business targets and ensures that the understanding of risk is integrated into the BBC's strategic and financial planning.

The BBC's existing control framework is an effective mechanism for reducing risk. For example, the BBC's Editorial Guidelines, which are widely distributed and have been refined and tuned over a period of time, are considered to be a mature and reliable control system. Relevant staff consider that the escalation mechanism for editorial related risks and issues is clear and robust. This has helped to drive a cultural approach at the BBC to refer up and consult if in doubt or when entering unknown territory. Staff throughout the BBC consider that the Editorial Guidelines provide them with a framework for content that is effective in enabling risk to be taken on an informed and controlled basis. At the operational level, most staff understand and use the Guidelines to support their judgement, but they do not necessarily equate this to risk management. Controls such as the Editorial

Guidelines are regularly reviewed for relevance and effectiveness and Guidance is updated accordingly; an example is updating Guidance to reflect the use of social media by high profile talent.

The BBC's key Corporate and Divisional risks are given appropriate attention and focus at senior level. Strong ownership of these risks is evidenced and progress and effectiveness in managing the risk to limits deemed acceptable is regularly monitored. Initiatives, such as the Single Point of Accountability approach and Finance Director Peer Reviews[1], have been instrumental in driving ownership and responsibility for risk management. Risk reports have been developing and improving on a regular basis and the latest heat-map style reports are considered to be effective by senior management as they create focused debate on strategic and operational risks at Executive and Divisional Board level. A period of stability is now required to ensure the latest reports can be embedded and 'bought-into' by the different Divisions. However, criteria need to be developed to support the rationale around the assessment and prioritisation of key risks. In addition, consideration should be given to understand how further use could be made of existing corporate and divisional risk data across the BBC to provide an improved understanding of past and present risk profile trends.

Recommendation 1: The BBC should undertake a review of existing risk data that has been reported to the Executive board, and develop metrics that support a better understanding of operational and strategic risk profile trends and can be used to justify the effectiveness of risk mitigation strategies.

The BBC's assurance functions such as Internal Audit, the Central Risk Team, the Project Management Office and Safety, Security and Resilience are well integrated and provide an effective risk management support mechanism to the BBC's Divisions. Risk management process and practice, and existing control effectiveness across different types of risks, are generally well understood across the BBC. The existing linkages of risk to strategy, policy and business plans provide a foundation for ensuring there is an effective risk-based approach to auditing. This should provide assurance to the Executive Audit Committee and Executive Board that in-place processes and controls are managing risks effectively.

The format and objectives of the BBC's Central Risk Team were changed in September 2012 to create more of an advisory role to the BBC's Divisions. Continuing to provide direct resource to support the Divisions will help drive change and, in turn, the businesses will take more ownership. The current format should remain in place.

On-going improvement

The BBC has identified, and implemented, a number of initiatives aimed at improving its risk management process and culture. However, it would benefit from a formal plan that clearly brings these activities together to set out the overall direction, scope, and priorities for risk management at the BBC. The BBC has started the development of a plan, which contains clear objectives, incorporating both the work undertaken to date and the improvement activities that remain to be done. This approach, if it aligns with international standard principles and guidance, and good practice, should help drive the BBC's understanding of, and commitment to, existing and planned initiatives. Priorities may differ between Divisions based on their risk management needs.

[1] A review of whether risk and mitigation are being effectively considered for projects and business initiatives.

Recommendation 2: The BBC should finalise the development, and achieve senior level sponsorship, of a coherent risk management improvement plan, that clearly justifies the roadmap of initiatives (Figure 1 shows an indicative high level roadmap) by articulating how the improved risk management process and culture they generate will support the achievement of the BBC's public purposes, and how they will be measured.

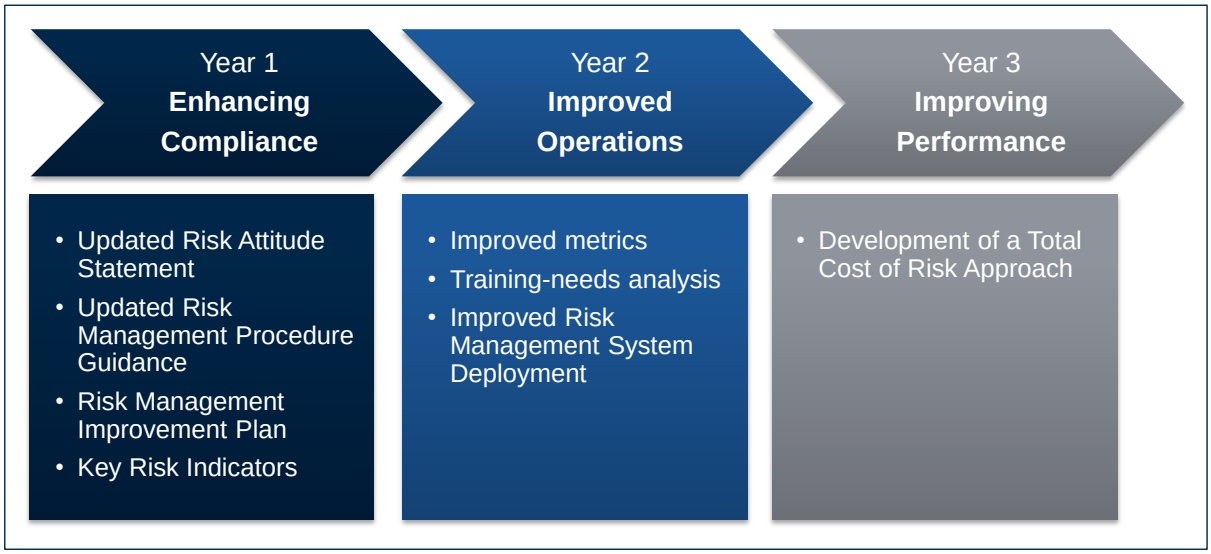

Figure 1 – Indicative Risk Management Improvement Road Map

The 'tone from the top' has been strengthened with the publication of a high-level Risk Appetite Statement by the BBC's Director General and Managing Director of Finance & Operations in January 2015, but this requires further development. The articulation of a risk appetite statement that is relevant to the BBC's business has proved challenging; this is because such a statement must reflect different levels of risk appetite across the BBC's diverse activities (from producing creative dramas to ensuring broadcast continuity). The current statement could be strengthened further by providing more direction regarding expected attitudes to risk across the BBC. The BBC should consider further expanding this statement and renaming it a Risk Attitude Statement. This Risk Attitude Statement should contain expected tolerance levels for key risk categories that the BBC currently use namely Audiences, Financial, Policy and Delivery. This will provide more direction as to where risk should be taken (e.g. creative risks) and where effort should be employed to ensure certain types of risks are kept to a minimum (e.g. health and safety). Whilst the Managing Director of Finance & Operations is seen as a real supporter and driver of the BBC's risk management framework, increased communication from senior management could help reinforce the 'tone from the top'.

In addition, to align with international standards and good practice, the BBC should also consider publishing a concise, high level BBC-wide risk management policy statement referencing the BBC's existing approach to risk management, its risk improvement strategy, key risk processes, and day-to-day behaviour expected of all staff and senior management. An initial draft of the pan-BBC risk policy has been developed by the Central Risk Team but has yet to be signed off by senior management.

Recommendation 3: The BBC should consider further expanding its existing Risk Appetite Statement by adding more detail in relation to expected risk tolerance levels for different types of risks and renaming it a Risk Attitude Statement. It should be considered to be a statement of intent and should guide staff to take controlled and informed risk.

The reporting of risk at Executive Board and Divisional Board in terms of content, scope and frequency has improved considerably in recent years. We consider the existing risk reporting framework to be effective in providing different levels of management with a good understanding of existing and emerging key risk themes. The BBC's 2007 Risk Management Board Reporting Policy is being updated to reflect the improvements and changes currently in place and ensure the content of the document is streamlined and simplified. To be effective, this updated policy document should reflect the tolerance limits which guide prioritisation and escalation decisions, and which are set out in the Risk Attitude Statement.

The reporting of risk has also been supported by a 'top-down' workshop undertaken by the Executive Team in 2014 to identify and assess key risks that could affect the achievement of strategic objectives. The initiative was considered a success, in that the Board discussed and agreed their priorities; and the approach is now being cascaded to Divisional level. The Executive Board is committed to an annual workshop to review the priorities.

The BBC's senior teams take a balanced approach by considering both risk and opportunity in the development of their strategic and business objectives. Risk and opportunity are identified and assessed in the development of Divisional business plans and form an integral part of performance monitoring against the delivery of specific objectives and targets. Whilst the corporate risk management process rightly outlines the need to capture and report opportunities, which is broadly done across the BBC, there is a propensity, particularly at the operational level, to only report on the downside of risk. Threats are reported much more extensively than opportunities, and in some areas risk is only seen as a 'negative'; this said, opportunities are regularly considered during the selection and development of appropriate risk mitigation strategies. Therefore, there are circumstances where it could be appropriate to consider upside for certain operations and ensure an appropriate trade-off is made between risk and opportunity. For example, aggressive cost reduction exercises are requiring the BBC to identify and take opportunities. BBC staff would benefit from more direction and process guidance in respect to recording opportunities as part of the justification for selecting a particular risk mitigation strategy

Recommendation 4: The BBC should consider updating its Risk Management Procedure Guidance to provide direction on the recording of opportunities as part of the evaluation process when considering and justifying specific risk management options.

Awareness and understanding of risk management principles is good and reasonably consistent across the different levels of seniority at the BBC. Across all levels of management, there was evidence of a good understanding of risk management principles including recognition that frameworks, such as Editorial Guidelines and Fair Trading Guidelines, are part of the control environment. It was also observed that in some operational and administrative areas of the BBC there is a cultural reluctance to take risks due to a fear of squandering, or being perceived to waste, licence fee payer resources. Management are addressing the cultural issues in this area but there is still more to do. The Central Risk Team is undertaking a training needs analysis to develop a strategy for understanding the portfolio of training materials and concepts required to address the differing needs across the different areas of the BBC. This strategy will build on existing initiatives such as those in place to improve awareness and understanding of Editorial Guidelines and Fair Trading requirements.

Recommendation 5: The BBC is currently undertaking a training needs analysis. This should enable the development of a risk awareness training strategy that will address the needs of management and operational staff. In particular, consideration should be given to the implementation of senior management awareness sessions that will provide an understanding of how effective risk management could be implemented at the BBC, supported by the use of relevant case studies.

The opportunity to develop good practice

The BBC uses a number of software systems to support the identification, assessment and reporting of different types of risks and controls including operational, strategic, project and environmental which are not integrated. The corporate risk management software system, supported by the Central Risk Team, is currently used to collate and report operational and strategic risks across the different Divisions. Whilst it is acknowledged as a risk management support tool by many areas of the BBC, it requires updating to support improved ease of use and new reporting formats. The BBC has indicated that a Governance, Risk and Compliance systems feasibility study was undertaken, which found the cost of implementing such a system would have been prohibitive. As a consequence, the BBC decided not to progress such an initiative any further. However, a Governance, Risk and Compliance system proof of concept, limited to information security risk, is currently being conducted, the results of which should be incorporated into an improvement roadmap for the corporate risk management system.

Recommendation 6: The BBC should determine whether it should upgrade or replace the current corporate risk management system. In doing so it should develop a risk system roadmap as part of the overall improvement plan outlined in Recommendation 2. This roadmap should incorporate the findings of the Governance, Risk and Compliance proof of concept. The roadmap should ultimately deliver an improved system which will support better processes and reports, as well as reducing the administrative burden on the Central Risk Team.

The BBC has an opportunity to improve its 'horizon scanning' including the monitoring of emerging risk across the different Divisions, with the implementation of a set of Key Risk Indicators. Key Risk Indicators are metrics that could be used by the BBC to provide an early signal of increasing risk exposures across the different Divisions. The BBC has started to look at the feasibility of using Key Risk Indicators based on existing metrics. The development of Key Risk Indicators for the BBC will involve the analysis of risk events that have affected the organisation in the past (or present) and then the pinpointing of the cause or events that led to the loss.

Recommendation 7: The BBC should look to improve its risk monitoring function by completing the work it has started in developing and implementing a set of Key Risk Indicators that will provide an early indication of increasing exposures and allow management to implement timely and cost effective actions to ensure key objectives are met. These should be based on the current metrics, such as audience numbers and health & safety incidents, that are captured across the BBC.

In the long term, a Total Cost of Risk analysis would enable the BBC to evaluate and benchmark whether its expenditure on managing certain types of risk is cost effective. Total

Cost of Risk analysis provides a greater understanding of the financial effectiveness of an organisation's risk management capability. In the BBC, such a methodology could be used to assess the total cost of managing specific risks such as cyber-attack and project delivery. This approach is very quantitative in nature, and focusing on particular risks would allow the BBC to benchmark themselves against similar organisations. In the future, applying this methodology to risks and related losses that are common in other organisations would help the BBC to understand how effectively it manages and finances certain types of key risks.

Recommendation 8: The BBC should consider undertaking a proof of concept to assess the feasibility of producing a Total Cost of Risk assessment. Such an approach would benchmark how much it spends managing risks that are common across a number of organisations. If successful, such an initiative should provide a sound basis for determining Value for Money of the BBC's implementation of risk management. Such an assessment is ambitious, and would be considered to be 'world-class' in terms of methodology adopted.

A Journey of Improvement

The BBC's vision is "to be the most creative organisation in the world". In order to produce entertaining and engaging content, risks have to be taken. When comparing the amount of content that is regularly broadcast with the number of issues that have actually materialised, risk can be considered to be well managed across the organisation. The BBC is on a risk management improvement journey and the changes implemented are having a positive effect in terms of compliance, visibility and quality of data, reporting and senior management focus. Other changes are being made, and the BBC considers that this is a continuous improvement process; we believe they should continue their efforts to drive better use of information and cultural acceptance of the value of risk management across the organisation.

1. Risk management is a vital function of the BBC that enables the organisation to achieve its public and strategic purposes. Risk management is reflected in every facet of the BBC, from production to content development, broadcasting to finance. The BBC's vision '*to be the most creative organisation in the world*' demands risk taking and does not naturally fit with conventional approaches to risk management. Encouraging creativity and managing risk is based on a delicate balance which demands agility and flair.

2. Over the past five years, the BBC has shown its commitment to reviewing and improving its risk management approach through a number of internal initiatives and external reviews. In 2012 two reviews were undertaken: the National Audit Office's Financial Management Review published in October 2012[2], which examined risk management as part of a wider review of the BBC's financial management, and a more focused independent external review of risk management at the BBC. These reviews provided the BBC with four overall recommendations:

    - Strengthen the Executive Board's input into risk management by implementing a risk management strategy;
    - Redefine the role of the Central Risk Team to oversee the development of risk policy and the provision of expert risk advice;
    - Improve the nature of risk reports to provide a more accurate assessment of risk in the BBC; and
    - Strengthen risk reporting by being clear on the levels of risk the BBC is prepared to tolerate and identifying risks most in need of action.

3. Since these reviews, a number of initiatives have been implemented allowing the BBC to take more informed and controlled risk decisions through improved awareness, transparency and visibility. These initiatives have broadly addressed the recommendations identified and have focused on:

    - Improving the quality of risk information and the format of senior level risk reports;

[2] National Audit Office (2012), *Financial Management Review.* Available at: http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/review_report_research/vfm/financial_management.pdf (Accessed 18 March 2015).

- Ensuring risk management, a regular agenda item at Divisional Board, Executive Board and Executive Audit Committee levels, is substantially discussed, thereby improving senior management focus and discussion of risk;

- Strengthening the link between the BBC's business objectives and risks that may affect these objectives, thereby improving the integration of risk management with business and strategic planning and review;

- Transforming the role of the Central Risk Team to become advisors to all Divisions and provide support in terms of process and culture change;

- Enhancing the top-down approach to risk identification and assessment at Executive level in relation to achieving strategic objectives;

- Developing a pan-BBC risk appetite statement;

- Streamlining pan-BBC Boards; an initiative instigated by the Director General in 2013 to speed up decision making enabling the release of bureaucratic resources to programme making; and

- Introducing the Single Point of Accountability and Finance Director Peer Review initiatives that have improved ownership and responsibility for managing risk. This has started to improve the sharing of information and lessons learned at senior levels within the BBC.

4. On the whole, the findings identified from our review at the senior level were consistent with those we saw from across the Divisions. Awareness and understanding of risk management remained consistent across the different levels of seniority that were involved in the review. However, there are a number of improvements that should be implemented which will help to create a more robust framework with a strong and consistent 'tone from the top'. These improvements cover both process and culture and are dealt with in more detail in various sections of this report.

5. A bespoke Risk Maturity Model was used to assess the quality of the risk management process implemented and the culture at the operational level. The model produces an overall score in the range 1 (*Ad-Hoc)* to 5 (*Exemplary*), based on input scores from respondents across the BBC to a series of focused risk management questions. Results indicate a framework and attitude at the BBC between 3 (*Organised*) and 4 (*Coherent*) out of 5 (see Figure 2, or Appendix for full methodology), that is on a par with the median performance demonstrated by FTSE 100 and Fortune 500 companies.

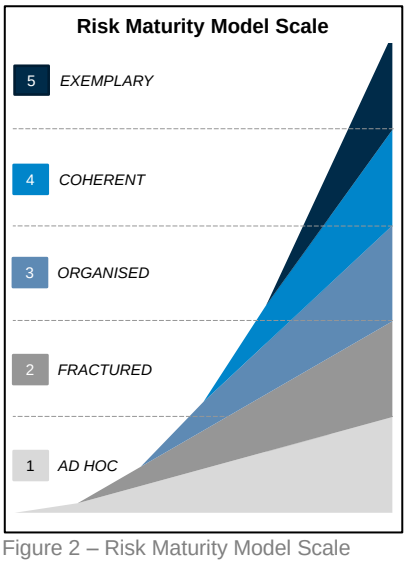

Figure 2 – Risk Maturity Model Scale

6. The risk management framework implemented across the BBC complies with corporate governance requirements and aligns with international standard principles and guidelines, with good practice being exhibited in a number of areas (see Figure 3). Particular areas of strength identified related to the control environment and ability to implement effective risk management responses. *Control Activities* are the policies and procedures that help ensure that management's risk responses are carried out. At the BBC

these include Editorial Guidelines, Safety, Security and Resilience and Fair Trading policies, and can also include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

7. Based on responses to the Risk Maturity Model, all Divisions score 3 (*Organised*) or above and therefore align with international standard principles and guidelines. Although there is some variation in the quality of the risk management framework (see Figure 4), the results demonstrate a good degree of consistency across the Divisions.

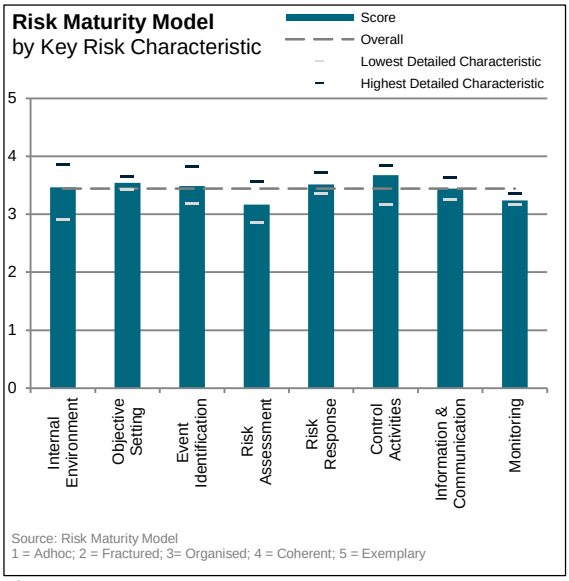

Figure 3

8. A strong ethical and integrity environment, the availability of robust policies and procedures and the ability to evaluate the most effective responses to manage risk were identified as key strengths across the BBC (see Figure 5). This view from the operational level is supported by findings from senior management interviews, which highlighted the use of risk management to support strategic and financial planning. The more mature areas demonstrated a strong link between business objectives, risk and existing controls. Particular areas identified for improvement are around the availability and awareness of data sources to help reduce the subjectivity of risk analysis and the application of recognised assessment.

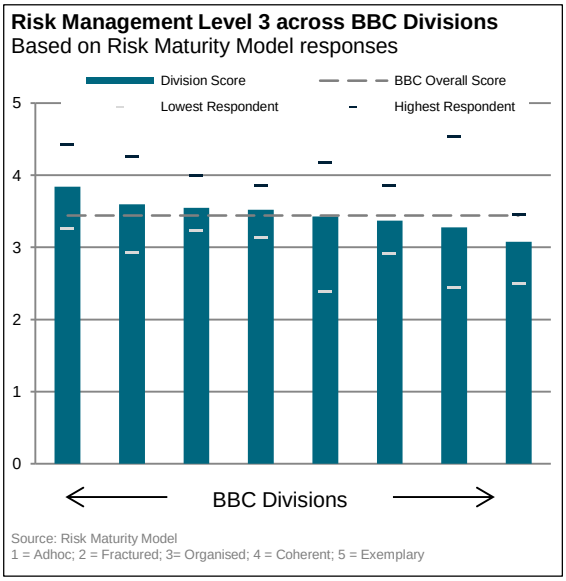

Figure 4

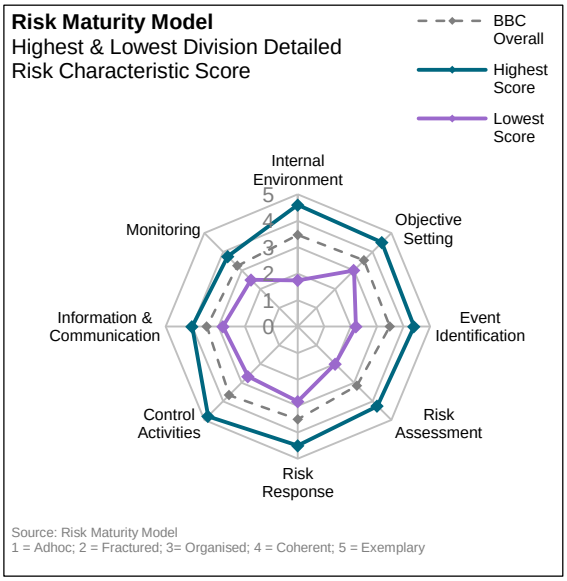

Figure 5

Strategy and Policy

Whilst the BBC has made some good progress in terms of risk management strategy and philosophy, the 'tone from the top' could be strengthened across the organisation. The pillars of a robust risk management framework are in place but the BBC's policies also need to be updated to support existing risk management practices, and to simplify and better present risk information. This will help to support the provision of a sound risk management policy and framework throughout the organisation, ensuring that risk is taken on a controlled and informed basis.

Risk Management Improvement Plan

9. The risk management improvement plan, sometimes known as the risk management strategy, is an important building block in creating an effective risk management environment for the BBC. The primary purpose of this document is to provide an over-arching plan for senior management that clearly sets the direction and priorities for improving risk management which must be aligned to the organisation's key objectives. The risk management improvement plan is the scheme within the risk management framework that specifies the approach, the deliverables and related activities, and resources to be applied to driving cultural change, improving process and therefore ensuring risk management is effective. The plan must also cover assignment of responsibilities, prioritisation and sequence and timing of improvement activities.

10. The BBC commissioned an independent review of risk management in 2012. Since this review, a number of improvement initiatives and objectives have been identified. Some have been implemented but others have still to be addressed. The improvement initiatives included:

- An action plan on the development of the BBC's risk culture following the debate by the Executive Board on 9 July 2014;
- Development of a fit for purpose risk appetite statement;
- Implementation of senior level risk identification workshops; and
- Development of a training needs analysis.

11. With the activities that make up the BBC's risk management improvement roadmap identified, including those already in train, the Central Risk Team has begun to bring these elements together into an over-arching improvement plan which clearly sets the overall direction, scope and priorities for risk management. Although it is still in development, this plan looks to explain how the objectives will be achieved within the existing resource base, planned timings and priorities for delivery, success measures and alignment with the BBC's Mission and Vision.

12. **The Central Risk Team should complete the risk management improvement plan which should encompass all of the work undertaken to date and clearly set out the direction, scope and remaining priorities for risk management at the BBC.** It should formulate a vision with supporting objectives and describe in clear terms the risk management capability that the Executive Board requires from the BBC in support of its mission statement and related public

purposes. The improvement plan should contain a roadmap of prioritised activities and be 'owned' by the Managing Director of Finance & Operations. Elements of the plan, including objectives, deliverables, timescales, and measures of success should be made available to all staff via the Business Assurance website.

Risk Management Policy

13. In addition to the BBC's existing components of risk management governance, an overall risk management policy document that reflects the BBC's philosophy and approach to risk management is being developed, in liaison with Executive Audit Committee. The first draft of the policy was submitted to the Executive Audit Committee in March 2015. This approach aligns with international standard guidelines and principles and provides the foundation for enabling good risk management governance and practice. The policy outlines the overall intentions and direction of the BBC in relation to risk management and articulates a set of shared beliefs and attitudes characterising how the BBC should consider risk in all of its diverse activities. There is a strong focus on compliance, ownership and accountability which is commendable. The document needs to be communicated to all staff to help promote a more consistent risk culture across the organisation.

14. The draft policy document does not identify the way risk management performance will be measured and reported. In support of this, the Central Risk Team would need to develop relevant Key Performance Indicators (KPIs). In addition, the policy does not include a commitment to review and improve the risk management policy and framework periodically or in response to an event or change in circumstances.

15. **The BBC should approve and publish its BBC-wide risk management policy statement that articulates expected behaviours and attitudes of all staff in relation to risk management in the current business environment.** The policy should be considered to be the key foundation that supports the BBC's existing risk management framework. There is an opportunity to further enhance the policy by considering: how risk management performance will be measured, and committing to a periodic assessment of the relevance and effectiveness of the policy in light of events and the changing environment.

Risk Management Board Reporting Policy

16. The Executive Board, supported by the Business Assurance function which includes internal audit, risk management and investigation services, is responsible for monitoring and delivering effective risk management across the BBC. This includes the reporting of risk and monitoring the effectiveness of the strategies that have been implemented to reduce risk to acceptable limits.

17. The BBC's Risk Management Board Reporting Policy document published in December 2007 provides guidance on the minimum reporting requirements expected from the Executive Board and Divisional Boards. The policy outlines how risks should be reported across the organisation, including fora where risks should be discussed, recording of audit trails, the BBC's risk management software, and reporting of threats and opportunities. Whilst it is a comprehensive document, it requires updating to reflect changes in the BBC's organisation structure and

reference should be made to culture, behaviours and attitude to risk. In addition, there are some areas that should be considered for further improvement:

- The format and presentation of the content can be simplified – this is being done as part of the Business Assurance website refresh;
- On the proviso that the recommendations to improve the Risk Attitude Statement are implemented, the section on risk escalation can be enhanced to include the triggers and thresholds used to escalate risk; and
- Reference should be made to the role of the Central Risk Team in terms of assisting the Divisions in the escalation and aggregation of risk needed to produce the Board risk update reports.

18. A strong governance framework is apparent, underpinned by the cascade of BBC objectives across the Divisions and supported by a risk reporting structure. Due to the work of the Central Risk Team, the existing risk reporting framework (outlined in Figure 6) can be deemed to be effective in providing different levels of management with a good and regular understanding of existing and emerging key risks and the effectiveness of the risk management strategies being employed.

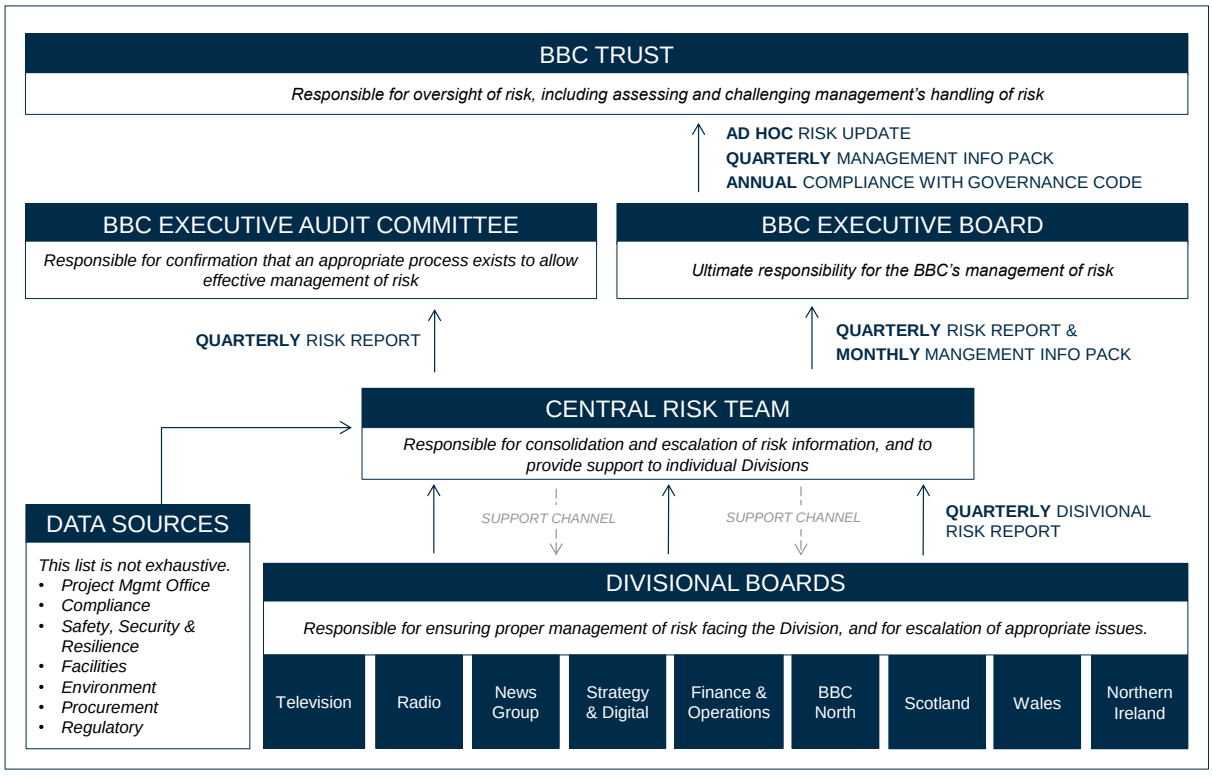

Figure 6 – The BBC's Risk Reporting Framework

19. Responses to the Risk Maturity Model findings verify the existence and operation of a strong governance framework at the operational level (see Figure 7). This is reflected in detailed risk characteristics for *Risk Reporting Structure* and *Risk Management Philosophy:* they are notable as the only two areas for which no respondents score below 3 out of 5 (*Organised*). The former indicates that the Divisions are aware of the procedure and framework for reporting and escalating risks from Divisional level to Executive Audit Committee and Executive Board. The latter, which covers the communication of shared beliefs and policies, such as the BBC's

Editorial Guidelines and talent management framework, indicates that there is a common understanding of the BBC's philosophy, with a strong degree of consistency and clarity across the organisation. *Risk Information* is also a relative strength, indicating that pertinent risk information is captured and that this enables individuals to carry out their management responsibilities and deliver the BBC's objectives.

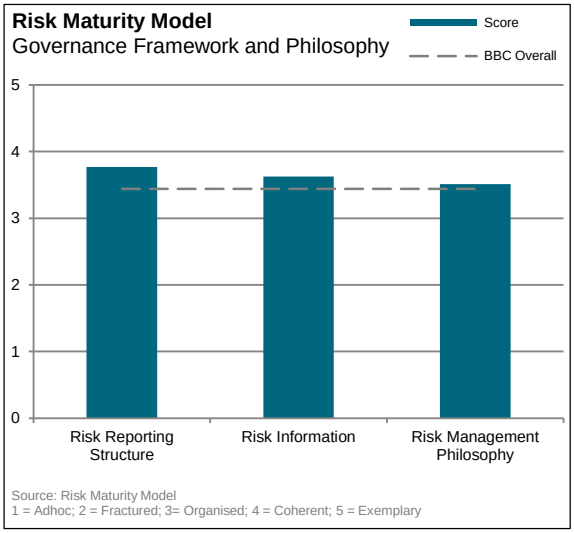

Figure 7

20. **The BBC should complete the update to the Risk Management Board Reporting Policy, as part of the Business Assurance website refresh initiative, to reflect the existing organisation structure and simplify the format and enhance the content.** If the BBC decides to enhance its risk attitude, more guidance should be provided on risk escalation and aggregation as well as the role of the Central Risk Team in the risk reporting process. The Risk Management Board Reporting Policy should be referenced as a sub-policy within the proposed risk management policy.

Risk Appetite / Attitude Statement

21. The objective of a risk appetite statement is to articulate the level and nature of risk that an organisation is willing to take in order to ensure that its strategy and related business plan are delivered in accordance with stakeholder expectations and within the constraints set by regulatory bodies. The articulation of a risk appetite statement that is relevant to the BBC's business has proved challenging; this is because such a statement must reflect different levels of risk appetite across the BBC's diverse activities, from producing creative dramas to ensuring broadcast continuity. Furthermore, it is clear that attitudes to risk taking should and do vary considerably across the BBC's Divisions making a single, encompassing statement difficult to formulate.

22. Historically, the BBC's risk appetite has developed interactively and slowly. Two issues have repeatedly come to the fore:

- Whether the intended use of the statement is internal or external. Is it designed to help people do their jobs and act as a support tool, or is it for conveying a message to the outside world?

- How should the Risk Appetite Statement take into account changing priorities, attitudes to risk and emerging concerns?

23. Between 2006 and 2012, four iterations were submitted to the BBC's senior management for review and approval which varied in terms of complexity and approach. The last version, submitted in November 2012, was more ambitious and was based on four over-arching risk related themes: Finance, Audiences, Policy and Delivery. These, in turn, were divided into a limited number of sub-headings, with statements written to summarise the BBC's attitudes to each of these risk types. The approach also drew from earlier work and previous statements. The draft was taken to the Management Board[3] who provided feedback on the need to better understand how the statement could be used in practice as a tool to manage the business. The Management Board's view was that the statement needed to be punchier and less wordy, with an emphasis on what could be achieved by a roll-out.

24. In a paper to the Executive Audit Committee on 17 June 2014, a proposal was made that the development of an understanding of the BBC's attitude to risk, together with a roll-out of this understanding across the organisation, should be pursued hand-in-hand with the work to build stronger culture across the Corporation. In January 2015, a high level Risk Appetite Statement was approved and endorsed by the Director General and Managing Director Finance & Operations. The intention is to roll-out this statement to Divisions via Divisional board meetings.

25. To be successful, the BBC's newly approved Risk Appetite Statement needs to be integrated into existing policies and processes. It needs to be recognised that risk profiles, and therefore culture, are different for each Division as the risk appetite varies for creative, operational and strategic risks. Whilst the overall risk appetite for the BBC can be considered low, especially for operational risk, the appetite for creative risk is considered to be high. The current definition of risk appetite does not reflect this and does not provide enough clarity around tolerance levels. The existing Risk Appetite Statement fails to provide an understanding of the levels of informed and controlled risk that need to be undertaken in order to deliver the Mission of the BBC. For the statement to help the BBC better manage risk, it needs to include tolerance levels (high, medium,

[3] Now the Executive Team

low) that are linked to the BBC's existing risk scoring criteria (used to assess operational and strategic risks) for each major risk category.

26. Risk appetite implies a degree of quantification, whereas a risk attitude statement refers to a more qualitative approach to risk, as defined by ISO 31000; it is a statement of intent. An organisation's attitude towards risk influences whether risks are taken, tolerated, retained, shared, reduced or avoided, and whether mitigating actions are implemented or postponed. A risk attitude statement would be more appropriate for the BBC as the organisation's risks, such as editorial issues or reputational risks, can be difficult to quantify. Such a statement is a more practical approach which also offers additional flexibility with shifting risk priorities.

27. Responses to the Risk Maturity Model indicate a good awareness by BBC staff of the existence of a *Risk Appetite* statement and its use in strategy planning (see Figure 8). All Divisions score *Risk Appetite* at least 3 out of 5 (*Organised*). Staff would benefit from further guidance on the BBC's appetite to risk to reduce variation across Divisions.

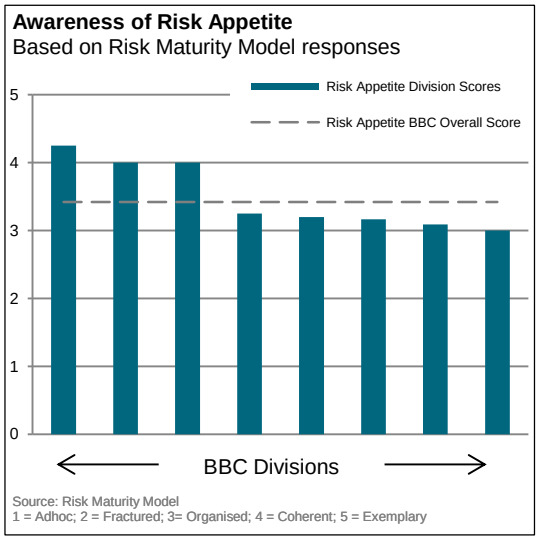

Figure 8

28. **The BBC should rename its Risk Appetite Statement a Risk Attitude Statement.** The Risk Attitude Statement should be seen as a statement of intent from senior management, which will be compatible with BBC culture and will be more closely aligned with international standard guidelines and principles.

29. **The BBC should expand its Risk Attitude Statement to provide more guidance on the levels of risk it is prepared to tolerate with regard to key risk categories.** The Risk Attitude Statement should reflect the 'tone from the top' and be compatible with the BBC culture. It should contain qualitative tolerance levels (high, medium, low) based on the criteria used for creating senior management risk heat maps. Tolerances should be defined for each of the following key corporate risk reporting categories: Audiences, Financial, Policy and Delivery. This approach should provide more direction as to where informed risk can be taken and where concerted efforts should be employed to ensure certain types of risks are kept to a minimum. An initial review on how to improve the current Risk Appetite Statement with associated tolerance levels has been undertaken. An updated Risk Attitude Statement should be effectively communicated throughout the BBC once it has been endorsed by the Executive Board.

Processes and Tools

The BBC's corporate risk management process is fit for purpose and aligns with existing international standard guidelines and principles. At the operational level, risk management processes vary but certain elements of good practice are evident.

The BBC's Risk Management Process

30. The BBC has an established risk management process which is described in the Risk Management Procedure Guidance for Managers, last edited in 2014, that aligns with international standard guidelines and principles. It can be accessed by all staff on the Gateway intranet via the Business Assurance homepage. The process is relevant at all levels throughout the BBC including project level, Divisional level and Executive Board level.

31. The Risk Management Procedure Guidance for Managers provides clear guidance on the need to identify events that can affect the BBC's objectives. However, the Procedure Guidance does not cover the different risk identification tools and techniques, such as risk prompt lists and loss databases that could be applied at the BBC to identify an initial list of potential risks and opportunities. Relevant and up-to-date information sourced using these tools and techniques is important in identifying risks and should include appropriate background information and involvement of people with relevant experience and knowledge.

32. From initially describing the risk, the BBC's Procedure Guidance outlines two concurrent processes that need to be followed in order to complete the evaluation process (see Figure 9); this approach aligns with good practice. This first step looks to identify the causes and consequences of a risk. Once this is completed, the existence or otherwise of controls, detective or preventative for risk causes and corrective or directive for the controls themselves, can be confirmed. With this information, scores capturing the likelihood and impact of the risk materialising can be determined. Assessment criteria exist to support the scoring of both likelihood and consequence. The guidance consequences cover: reputation, financial/commercial, infrastructure, safety and environmental compliance.

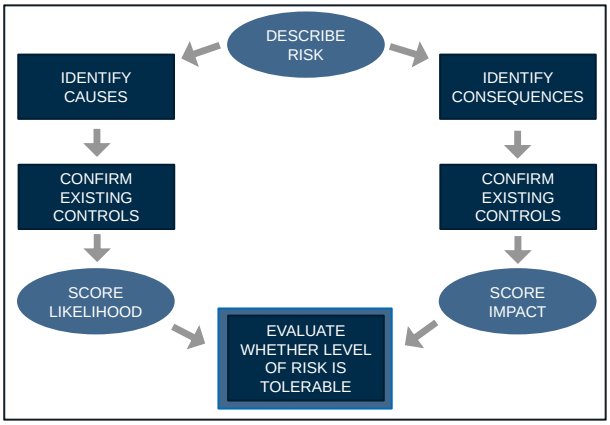

Figure 9 – The BBC's Risk Evaluation Process

33. Combining the likelihood and impact scores, an assessment is made as to whether the residual risk, after accounting for controls, is tolerable. If the risk is not tolerable, the next step is to determine further required risk responses: to treat, transfer or terminate the risk. This decision should be based on a cost-benefit analysis that is not currently a prescribed element of the BBC Risk Evaluation Process. The risk likelihood and impact scores are then re-evaluated, and the assessment on whether the residual risk is tolerable updated. This process does not cover the concept of risk preparedness that is used in the senior management operational and strategic heat-maps.

34. The process clearly highlights risk roles and responsibilities covering the Executive level, specialist functions and the Central Risk Team. The specialist functions include BBC Safety, Business Continuity, Information Security, Editorial Policy, Fair Trading and Procurement. The reporting and monitoring of risk is covered in the BBC's Board Management Reporting Policy. The Risk Management Procedure Guidance is supported by a glossary of terms providing guidance on the terminology used in describing the risk management process.

35. Within the Divisions the focus tends to be on smaller and operational risks as these are delegated to and dealt with at that level. Cross-Divisional risk management is considered an area for improvement at the operational level. However, senior management believe that at the strategic level, on the whole, there is an improved understanding of BBC wide risks and how they will affect the different Divisions.

Risk Event Identification

36. The identification of risk at the BBC is aimed at identifying potential events that, if they occur, will affect the BBC's ability to successfully implement its strategy and achieve its objectives. A 'bottom-up' and 'top-down' process to risk identification is followed at the BBC.

37. In July 2014, a workshop with the Executive Team was undertaken to get an understanding of key strategic risks that could affect the BBC. The exercise was well received by senior management. Not only did the workshop improve the understanding of the BBC's key risks, their severity and how well they were being managed, it also helped Divisional leaders drive process improvements within their businesses. It was agreed that workshops will be held on an annual basis.

38. At the operational level, risks are identified on a regular basis across the different Divisions with support from the Central Risk Team. *Risk Events* (3.8) scored near to 4 out of 5 (*Organised*), based on Risk Maturity Model responses. This indicates that in most Divisions risk events are actively identified and tracked. Furthermore, the desktop review and Risk Maturity Model showed that whilst the BBC's risk management process refers to the identification and management of both risk and opportunity, there is a propensity to focus on reporting the downside risk. Feedback from the risk maturity workshops indicated that risk is seen as a 'negative' which could be apportioned to the 'fixed income' environment that staff work in, and therefore threats are reported more extensively than opportunities. At the same time, while opportunities are regularly considered when determining and evaluating the risk management actions that need to be undertaken, they are not necessarily recorded as part of the process. Staff would therefore benefit from more direction on the need to record opportunity as part of the justification in deciding on a particular risk management action plan.

39. At strategic, operational and project levels there is a strong link between risk and objectives. *Strategic Objectives* is also a relative strength identified in Risk Maturity Model responses, indicative that management identify risks associated with a range of strategy choices and consider the implications of these risks. This provides clarity between BBC-wide objectives and the BBC's purpose and mission. When setting the BBC's objectives at Executive Board and Divisional level, risks and opportunities are considered to help provide a realistic understanding of the feasibility of delivering the objective. This process was followed in setting the BBC's 2015/16 objectives (see Figure 10).

Figure 10 – BBC 2015/16 Objective Cascade Diagram

40. In the Divisions, for example, TV uses a planning document with strategic and operational risks in order to develop the Division's business plans. This shows good integration of risk management with strategic business and financial planning. A risk forum has been created to support a top down approach to risk identification and assessment and help break down silos within the Division. The key risk themes are driven down through the Division to ensure the top down approach aligns with the bottom up approach.

41. The link between risk and objective is facilitated in part through the BBC's cascade of strategic to operational objectives. The Risk Maturity Model responses produce a score for the key risk characteristic *Objective Setting* comfortably between 3 out of 5 (*Organised*) and 4 out of 5 (*Coherent*), driven in part by a good understanding of how *Divisional Objectives* link to overall BBC objectives, and the use of risk event identification in the BBC's *Strategic Objectives* (see Figure 11).

Figure 11

42. **The BBC should update its risk management process guidance to ensure opportunities are captured and monitored when evaluating the best risk management strategies to implement.** The Risk Management website should offer more direction on the identification, assessment and management of opportunities. The guidance should make it clear that whilst for certain circumstances opportunity can be considered on a stand-alone basis, it should also be considered and recorded when determining the most effective strategy to manage identified risk and achieve an appropriate balance between risk and reward.

Risk Assessment

43. The BBC's process for assessing risk provides an understanding of the extent to which identified potential events could have an impact on the achievement of objectives. The process fully aligns with international standard guidance and principles. The assessment process uses a combination of likelihood and impact; risk criteria have been defined to score against five different levels for each of these characteristics. For impact, the following categories are considered: reputation, financial/commercial, infrastructure, safety and environmental compliance.

44. The impacts can be considered relevant based on the type of risks faced by the BBC in the business environment it operates within. The criteria used to describe different levels of frequency should be slightly more actuarial in approach and describe for each level (high, medium, low) a timescale and number of occurrences that is appropriate for the BBC, e.g. 'remote – no more than once in 50 years', 'probable – more than 4 times per year'.

45. Consistent guidance is required on the determination of an overall score (used for prioritising risk) based on a combination of frequency and impact. This can then be used to place the risk on a pre-defined heat-map to determine its overall severity and priority when compared to other risks. Guidance is currently held in the BBC's risk management software system, but for consistency this also needs to formally documented in the Risk Management Procedure Guidance for Managers.

46. For each potential event, two levels of risk are assessed: residual and forecast. Residual risk is the degree of risk that is known will remain following the implementation of controls and actions to reduce it. Forecast risk is the degree of risk which is predicted will remain after proposed actions or additional controls are implemented. This is an important element in the assessment process since it can provide an indication as to whether the risk will be managed to an acceptable level and the cost effectiveness of doing so. It is referenced in the glossary available on the Business Assurance website but the methodology should also be included in the Risk Management Procedure Guidance for Managers so that complete guidance is available in one document.

47. In the long term, the BBC has an opportunity to implement a 'best-in-class' approach to risk management through the development and implementation of a Total Cost of Risk methodology, to be applied to specific risks. Total Cost of Risk provides a greater understanding of the financial effectiveness of the organisation's risk management capability. As part of the Total Cost of Risk methodology, expected losses and risk aversion to specific risks need to be quantified. Together, these two values represent the amount of money that the organisation would be willing to allocate to eliminate the identified risks. To achieve value for money, the cost of mitigation and associated level of remaining risk should be less than the potential cost of eliminating the risk.

Case studies related to cyber-attack and project delivery could provide an initial understanding of how the BBC could implement an effective Total Cost of Risk methodology in managing and financing certain types of risks. Consideration should be given to the benchmarking of specific risks that are common across a number of different organisations. Whilst such an approach will not be possible across the BBC due to the unique nature of the organisation and the lack of benchmarking data from other similar organisations. This methodology and benchmarking would help improve future VfM assessments.

48. At Divisional and Executive Board level, a new concept has been introduced to prioritise risk known as 'risk preparedness'. This concept has been well accepted at senior levels within the BBC. A draft definition of 'risk preparedness' has been produced by the Central Risk Team which now requires formal approval. Preparedness can be described as how well the BBC is equipped to manage risk. This dimension is combined with risk severity: a combination of frequency and impact. It is used to place the risk against a heat-map that provides a pictorial depiction of the risk and its overall priority when compared to other operational or strategic risks (see Figure 15). The Executive Audit Committee approved this approach in a paper submitted in December 2014. With acceptance of the concept by members of the Divisional and Executive Boards, there is an opportunity to improve the robustness of the methodology by defining criteria for different levels (high, medium, low) of risk preparedness. It is recommended that consideration should be given to the use of factors such as: senior management attention, availability of appropriate skills and experience, risk velocity (how quickly could it occur) and availability of resources such as finance.

49. Risk assessment was highlighted as an area for improvement during the desktop review and the workshops conducted with BBC employees. Risk assessment at the BBC focuses primarily on qualitative judgement, but can be complemented with the use of quantitative data where appropriate. This already exists for assessing financial impact. It should be noted that, in some areas of the BBC, advanced modelling techniques are also adopted – for example, the finance function conducts financial modelling of risks related to securing sports rights.

Rank of 8 Risk Characteristics in each Division

	← BBC Divisions →							
Internal Environment	2	3	5	7	6	7	1	4
Control Activities	3	2	4	3	1	4	3	1
Objective Setting	4	1	1	2	5	6	2	5
Risk Response	1	5	3	8	3	2	5	3
Event Identification	5	7	2	1	3	1	6	6
Info & Communication	7	4	7	4	2	2	4	7
Monitoring	6	6	8	4	7	8	7	2
Risk Assessment	8	8	6	6	8	4	8	8

Figure 12 – Rank within BBC Divisions

50. From an operational perspective, *Risk Assessment* consistently scored lowest of all key risk characteristics (see Figure 3). Risk Maturity Model responses demonstrate that, for even the more mature Divisions, *Risk Assessment* is a comparative weakness. 7 of the 8 Divisions indicate *Risk Assessment* as an area for improvement relative to other key risk characteristics (see Figure 12).

51. The low score is driven in part by Risk Maturity Model responses to detailed risk characteristics (Figure 13) on the availability of varied *Assessment Techniques* and for *Event Relationship,* signifying some lack of understanding of the interdependency between risks and whether the event relationships exist within or outside the Division. The issue may be exacerbated by a lack of awareness and information flows across Divisions. At the strategic level, it was noted that there is a much clearer understanding of the interdependency of risks due to the improved holistic view of risk across the BBC.

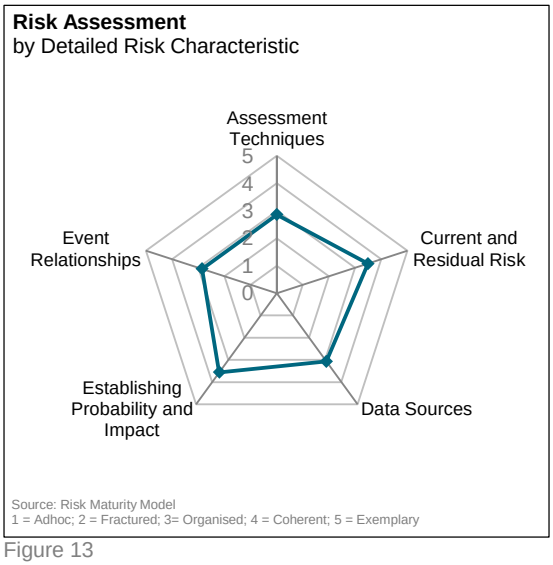

Figure 13

52. There is inconsistency of access and awareness of risk *Data Sources* across the BBC. Risk specialists in each Division are aware of the locally available data sources (e.g. audience research by the BBC and independent audience research; the occupational health and safety management system capturing near misses and events; the project risk tracking system; and the risk management software system). They monitor and review this data on a regular basis. However, at the operational level, more could be done to improve the awareness of the availability of data sources across different Divisions to support the identification and analysis of risk.

53. The monitoring of relevant data to help the BBC identify the effects of past events and quantify associated losses is not conducted consistently across the organisation. Improving this can help to predict future occurrences. A more consistent approach to monitoring loss data will improve the understanding of risk interdependencies and help develop improved risk forecasting. Access to loss event databases, available from third party service providers, or the development of an internal loss event database, will help the BBC improve its risk assessment process by providing a baseline for fact-based discussion.

54. The different Divisions across the BBC use risk assessment techniques suited to their specific requirements. There is an opportunity, however, to create a more collaborative environment in relation to risk identification and assessment by sharing good practice across Divisions.

55. **The BBC should improve its approach to risk assessment by adopting a more quantitative method where it is practical to do so.** This includes more guidance around the definition and use of frequency. The approach will improve the assessment of the financial impact of a risk and will provide a better estimate of savings achieved through risk mitigation.

56. **The BBC should consider undertaking a proof of concept in order to assess the feasibility of adopting a Total Cost of Risk approach to specific risks.** Such an approach would benchmark the BBC's risk spend on specific risks against organisations with similar risks, such as cyber-attack and project delivery. It would provide an understanding of how to apply the methodology across the organisation in order to support management in their decision making process. A Total Cost of Risk approach is likely to be easier to implement in certain areas of the BBC than others.

57. **The BBC's Central Risk Team should consider setting up a loss event data tracking system.** This will monitor relevant data that will help the BBC identify past events that have had, or continue to have, a negative impact and quantify the associated losses in order to help predict future occurrences.

58. **The BBC's Risk Management Procedure Guidance for Managers document should clearly set out the methodology for prioritising risk in the existing operational and strategic risk heat-maps.** This should provide an explanation of the criteria for different levels of preparedness, which could include characteristics such as available skills, senior management attention, timing and available finance.

Risk Escalation

59. At the BBC, risk is managed through line management with an escalation process that is based on significance or strategic importance. The escalation process across the BBC can differ by Division. The guidance for operational and strategic risk escalation and aggregation from Divisional to Executive Board or Executive Audit Committee is covered in the Risk Management Board Reporting Policy; this should be clearly referenced in the Risk Management Procedure Guidance for Managers. The BBC should ensure that all of this documentation is consistent with the recommended improvements to the Risk Attitude Statement. At the operational level, some risks, such as editorial risks and talent management, have a clear escalation process.

60. Responses to the Risk Maturity Model indicate that the risk escalation procedure is satisfactory and clearly understood across the BBC at the operational level. *Risk Reporting Structure* (see Figure 7), which covers the procedure for referring and escalating risks, is scored 4 out of 5 (Coherent) by half of the Divisions.

61. The BBC is developing an approach to define and implement Key Risk Indicators, which are linked to compliance reporting. This methodology is mentioned in the BBC's risk management glossary but has not yet been implemented. Increasingly, boards and senior executives are looking to develop metrics or indicators to help to better monitor potential future shifts in risk conditions or new emerging risks. This enables management and Boards to more proactively identify potential impacts to the organisation's portfolio of risks. Doing so enables senior management to be in a better position to manage future events in a more timely and strategic manner. An example of a relevant Key Risk Indicator is audience levels against a socio-demographic segmentation, including major cultural groups. Key Risk Indicators provide an early warning that risk is about to become a reality. They are also useful in providing escalation triggers for operational risk. The Central Risk Team should complete the development and implementation of these indicators making sure they are simple to operate and relevant to the BBC's operations and objectives.

62. **The BBC should improve the guidance on how operational and strategic risks should be escalated to ensure consistency between different Divisions.** Once the recommendations to the Risk Attitude Statement are implemented, the BBC will be in a position to more clearly define escalation triggers for strategic risks and operational risks in support functions. It should be noted though that escalation processes in relation to editorial and talent management are considered to be robust and at this stage do not require further refinement.

63. **The BBC should complete, in the short to medium term, the development and implementation of a set of relevant Key Risk Indicators.** This approach is used to establish a monitoring mechanism across the BBC's key processes and activities for identifying events that can indicate whether the probability or likelihood of a related risk is increasing or decreasing. Key Risk Indicators will provide early warnings to identify potential events that may harm the continuity of an activity or project, and therefore provide real time actionable intelligence to decision makers

Risk Response and Control

64. Across the majority of Divisions, the linking of objectives, risk events, assessment and response was a strong feature that provides the basis for understanding the effectiveness of existing risk reduction strategies across the BBC. Having assessed relevant risks, at both strategic and operational levels, the BBC have in place a set of guidelines that will help determine the most appropriate action. This could be one or a combination of: tolerate, treat, transfer or terminate. Controls are measures already in place that mitigate risk, BBC examples of these being Editorial Guidelines and Fair Trading Guidelines. Proposed actions are measures planned to further reduce the impact or likelihood of the risk occurring.

65. Selecting the most appropriate risk mitigation option involves balancing the costs and efforts of implementation against the benefits derived. At the strategic level within the BBC, there is evidence that this is undertaken when considering the need to manage risk and the delivery of potential related benefits.

66. At the operational level, there is less evidence that a cost-benefit analysis is considered when deciding on the type of mitigation to implement. Feedback has indicated that this analysis is undertaken but details justifying the choice of treatment actions are not recorded in the Divisional and other operational risk registers.

67. *Risk Response* and *Control Activities* provided above average scores in the Risk Maturity Model responses. These were driven by key strengths in *Policies and Procedures*, suggesting the consistent application of policies and procedures across all levels within the BBC, and *Controls over Information Systems,* indicating staff feel the IT environment is effectively protected (see Figure 14).

68. A number of effective enterprise level controls have been implemented at the BBC examples of which are described in Appendix 2.

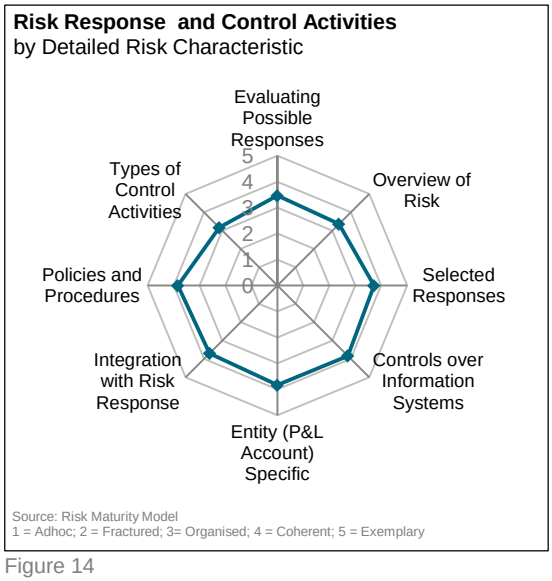

Figure 14

69. **The BBC should consider expanding the current risk register format to include the cost of mitigation which should be used to support a cost-benefit analysis on planned risk reduction initiatives, where proportionate.** Virtually every risk response will incur some direct or indirect cost, and this should be weighed against the benefits it creates. The initial cost to

design and implement a response (processes, people and technology) should be considered, as should the cost to maintain the response or control on an ongoing basis.

Risk Reporting

70. The BBC has a comprehensive risk reporting process ensuring that established and emerging risks are regularly reported at all management levels. Senior boards across the BBC regularly report on the risks their businesses are currently facing. Whilst the BBC recognises that reporting is only an element of risk management, it considers the process to be key because it facilitates a regular focus on what is most important by the people who are in the best position to implement change. A standard report template is not prescribed, leaving it up to the Divisions to develop formats which best suit their target audience.

71. Risks are reported on a quarterly basis at Divisional Board level. Divisional Boards are required to identify risks which, by virtue of their significance and strategic importance, warrant the attention of the Executive Board and the Executive Audit Committee. These risks are submitted to the Central Risk Team who then undertake an exercise of aggregation and comparison using other sources of risk information such as reports from the Project Management Office, Compliance, Safety, Security and Resilience and Procurement. Quarterly update reports are then produced for the Executive Board and the Executive Audit Committee. A monthly Executive Board Management Pack is produced that contains a section on key strategic and operational risks facing the BBC. This report is submitted to the Trust who also receive ad-hoc risk update reports. A review of this strategic risk data would help to better understand risk profile trends and mitigation strategies.

72. The Executive Board and Executive Audit Committee quarterly risk updates provide overall commentary on the BBC's risk profile and risk information in terms of description, causes and mitigation. The reports would benefit from information on the effectiveness of existing controls as the Executive Board and Executive Audit Committee should be provided with assurance that risk is being effectively controlled. The reports should also use trends or metrics to provide an indication of improvement or deterioration over a number of reporting periods as a number of senior managers commentated on the need to improve metrics, particularly in relation to the use of trend analysis.

73. At senior level, risk reports have been developing and improving on a regular basis and the latest heat-map style reports are considered to be effective in creating focused strategic and operational risk debate at Executive and Divisional Board levels (see Figure 15). These heat-map reports use a combination of risk severity and risk preparedness and trend arrows (movements since the last review) to identify key risk priorities for the BBC. Levels of risk tolerance are also superimposed on the heat-maps to support decisions on risks that could be tolerated and those that require further management attention. Senior management have stated that the format of these reports now works and they should be embedded across the business.

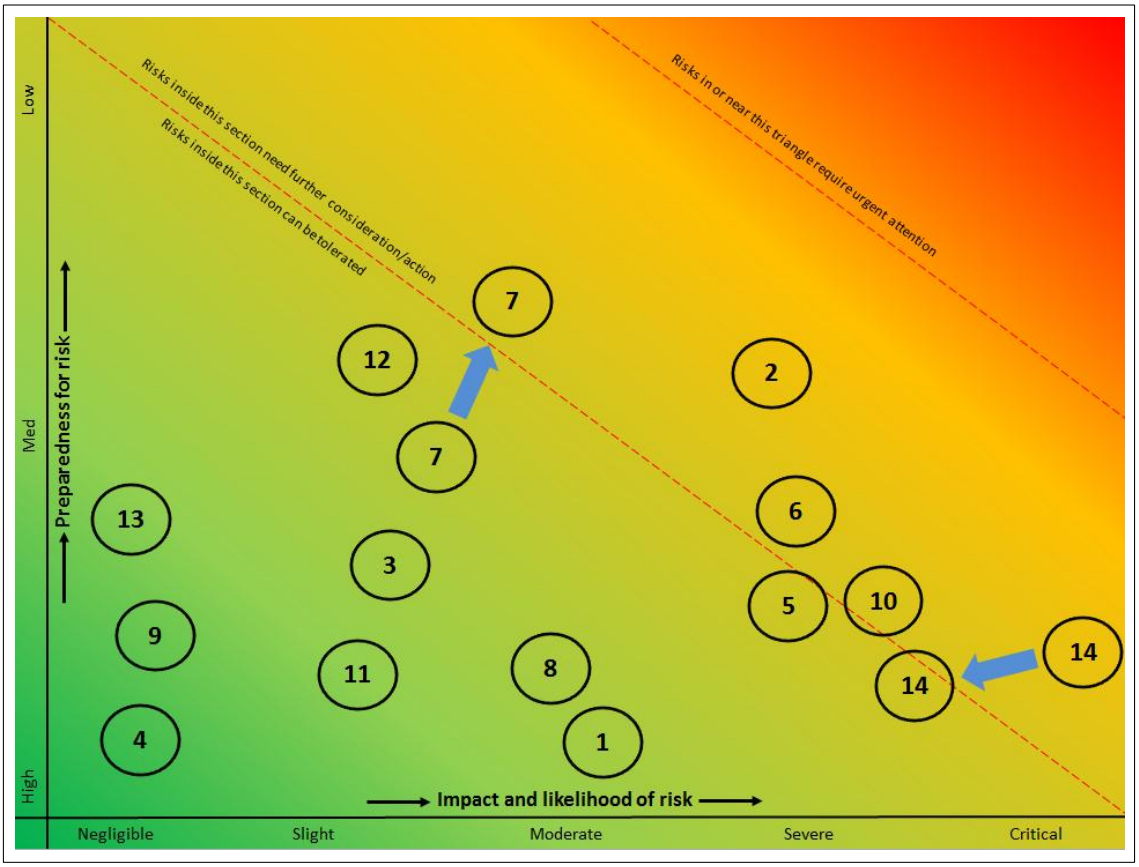

Figure 15 – Illustrative Heat-Map

74. The use of and support for heat maps at a senior level suggests key strategic and operational risks are given appropriate focus at senior levels within the BBC and the information presented is used to support the decision making process both at Divisional and Executive Board levels. In addition, strategic pan-BBC, Divisional and functional risks are given focused attention and are discussed at appropriately senior levels. In many cases, the nominated risk owners, particularly at Executive Team level, are asked to present progress reports on the effectiveness of controls and response actions being implemented to reduce the risk.

75. Risk is not solely reported in Executive and Divisional updates. There are a number of other reporting formats which incorporate risk and mitigation to support the decision-making process, including:

- **Critical Projects Portfolio - Performance Summary.** This is produced by the Project Management Office. A summary is presented to the Executive Board and the full report is presented to the BBC's Managing Director Finance & Operations and Executive Audit Committee Chair. The headline section is supported by a detailed table outlining project, phase, ownership, assurance and key points the Executive should note. Risk information, which is collected in a project risk tracking system, feeds into this report. Direct references to project risk in terms of delivery and cost are implicit in the projects summary reporting dashboard and directly referenced in the supporting Project Management Office Observations and Recommendations report.

- **Compliance Report.** This is prepared quarterly for the Executive Board and submitted to the Trust on a regular basis. The reports cover both strategic and operational risks normally associated with compliance and regulatory matters. Areas covered include: diversity, Health

and Safety, freedom of information, overdue audit actions, child protection, environmental targets and editorial compliance.

- **STaR Quarterly Review (Procurement).** A section of this report is dedicated to portfolio risk. Vendors are reported against in terms of risks or issues. Existing mitigation controls and actions are included against each supplier.

76. **The BBC should review risk data that has been reported to the Executive Board.** Reviewing data that has been presented, and developing metrics to support a better understanding of risk profile trends, will help with the justification of risk mitigation strategies.

77. **The BBC's Quarterly Executive Board and Executive Audit Committee top risk submissions should include more information on the effectiveness of existing related controls.** Effectiveness statements should be related to the most recent audits on the controls in question to provide assurance that the controls are effective and fit for purpose.

78. **The BBC should support the current quarterly Board risk reports with trend analysis**. The BBC has the opportunity to use historic risk data to provide analytics in support of trend analysis. A simple but effective example could be the number of high, medium and low risks over a number of reporting periods for each of the BBC's key risk categories, namely: Audience, Delivery, Financial and Policy. This will provide senior management with an understanding of risk management performance, the effectiveness of risk management strategies and whether additional response actions are required.

79. **The format of the strategic and operational risk heat-maps used to report risk at senior level should be fully deployed at Divisional board level and above.** The report is fit for purpose but effort is now required to ensure the format is bedded into the culture and fully accepted by all management teams. These heat-maps should also include more trend analysis.

People and Culture

The BBC's Executive Board is aware that good progress is being made in relation to driving a risk aware culture across the BBC. The Single Point of Accountability approach has been instrumental in driving ownership and responsibility of risk. However, the BBC is considering which type and degree of training is now required by different groups of staff, depending on their roles and responsibilities.

80. The Six Monthly Risk Update paper submitted to the Executive Audit Committee in June 2014 requested the Committee's consideration to create an initiative to further develop the BBC's risk management culture, aimed at improving the management and attitude to risk across the business. An analysis of the BBC's risk culture undertaken by the Central Risk Team was included in the paper. The key areas of strength related to:

- A commitment to ethical principles (ethical profiles of individuals, application of ethics and consideration of a wider stakeholder positions); and
- Sufficient diversity of perspectives, values and beliefs to ensure the status quo is consistently and rigorously challenged.

81. The Central Risk Team's analysis identified one main area of weakness: information did not flow up and down the organisation in a timely manner. Furthermore, bad news was not rapidly communicated without fear or blame, and staff were not encouraged to report risk events or actively seek to learn from mistakes and near misses.

82. The Central Risk Team's analysis also identified several areas for improvement including:

- A distinct and consistent 'tone from the top' regarding risk taking and avoidance;
- A common acceptance through the organisation of the importance of the continuous management of risk, with no process or activity too large or too obscure for risks to be understood; and
- Risk management skills and knowledge should be valued, encouraged and developed.

83. The BBC Executive Board discussed the paper in July 2014; they concluded that whilst risk was well managed across the BBC, risk management did not go far enough or deep enough. Key measures designed to improve risk culture were approved as part of an action plan. They included:

- Extension of the portfolio of training materials;
- Provision of more fora for risk debate; and
- Continued emphasis to ensure risk is included in all appropriate agendas.

All of these improvements were to be underpinned by the Executive Board's support for a wider strategic approach to improving the organisation's risk culture; including communicating the BBC's risk priorities to the Divisions and risk management professionals.

84. A number of actions have already been undertaken to improve the free-flow of information around the BBC, particularly at Divisional level. Following the risk workshop undertaken at Executive Board level in July 2014, the BBC is in the process of implementing additional workshops at Divisional level, to improve the wider understanding of the key strategic and operational risks that were identified at Executive Board level.

85. In general, the findings regarding the BBC's risk culture from this VfM Review are consistent with the Executive Audit Committee paper from 2014. The key issue faced by both has been to gain a clear understanding of the BBC's staff's attitude to risk. Whilst a significant number of staff at the operational level are not familiar with the standard risk terminology as set out in the Risk Management Procedure Guidance for Managers document, this does not equate to non-compliance. Many staff that comply with the Editorial Guidelines or Fair Trading Guidelines do not necessarily equate these Guidelines with risk control, or the fact that by abiding by these Guidelines, they are actively managing risk.

86. Senior management feedback indicated that the culture in some areas of the BBC is constraining risk taking. In the content areas of the BBC the risks are calculated, taken and well managed. However, in some of the operational and administrative areas of the BBC it was observed that a cultural reluctance to take risk still existed in some pockets. This has been driven by a fear of squandering, or being perceived to waste licence fee payer resources and an associated desire to protect the BBC's reputation from criticism.

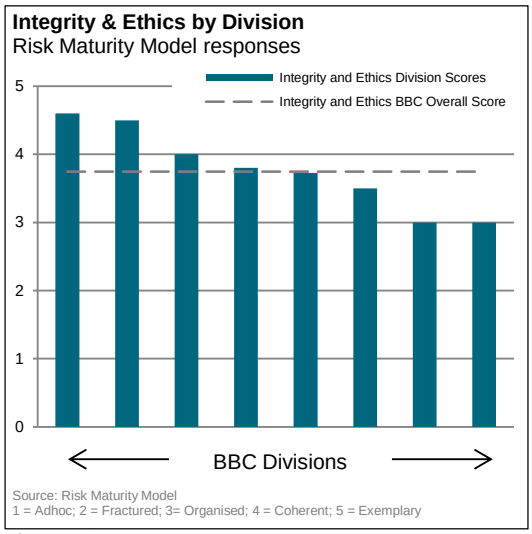

Figure 16

87. Responses to the Risk Maturity Model indicate a very mature level across the Divisions in relation to *Integrity & Ethics*, one of the highest scoring detailed risk characteristics. There is however some variation across the Divisions here (see Figure 16). This risk characteristic captures the existence and application of a clear code of conduct within the Divisions regarding information gathering, content production and conflict of interests.

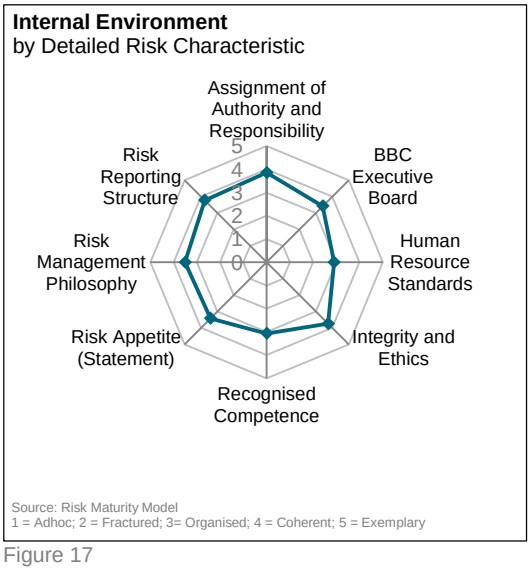

Figure 17

88. The BBC's Director General and the Managing Director of Finance & Operations in particular, are seen as key drivers in the improvement of the risk management process at the BBC. However, some feedback, both at senior management and operational level, indicated that the 'tone from the top' could be further improved with greater communication on existing improvement initiatives as well as clearer articulation of the needs and benefits of effective risk management.

89. The detailed risk characteristic *BBC Executive Board* scored below other areas of governance

captured in the *Internal Environment* key risk characteristic, based on Risk Maturity Model responses (see Figure 17). This is reflective of views on the commitment of senior management to risk management. There was a sense of a good degree of top-down focus but a lack of direct interaction or visibility of Executive Board decisions and actions.

90. **BBC senior management should engage in more dynamic communication of risk improvement initiatives.** By articulating the importance of initiatives, progress and expected behaviours, this will help to achieve consistency, understanding and support from across the BBC.

Reward

91. Senior management and operational staff at the BBC are not financially incentivised to manage risk effectively in a way that is comparable to the commercial sector. Instead, pride in the organisation and its public service ethos, creative accolades and job satisfaction are perceived to be appropriate reward. At the operational level, employees are expected to understand and manage risk; however the competencies involved in risk management are not sufficiently recognised and promoted.

92. Risk Maturity Model responses identify the *Recognised Competence* characteristic, which covers whether risk management is reflected in employment profiles and the appraisal process, as a relative weakness in the risk management framework (see Figure 17). The low score indicates scope for improvement in the organisation-wide recognition of management, excepting the availability of formal risk management training through the BBC Academy.

Ownership and Accountability

93. Strong ownership of risk is evidenced throughout the BBC. Progress and effectiveness in managing the risk to limits deemed acceptable is regularly monitored. The Single Point of Accountability approach has been instrumental in driving ownership and responsibility of risk. It is clearly recognised throughout the organisation that the processes for managing risk are in place.

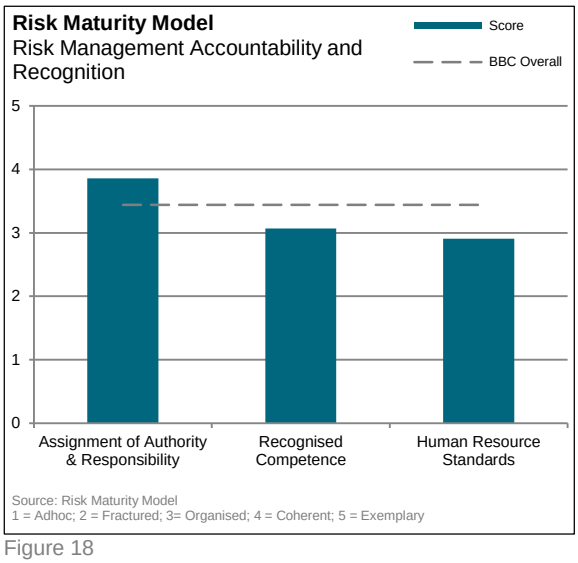

Figure 18

94. The strength of the Single Point of Accountability is reflected in Risk Maturity Model responses. *Assignment of Authority and Responsibility* is a top scoring detailed risk characteristic with roughly 75% of respondents scoring it as 4 out of 5 (*Coherent*) or 5 out of 5 (*Exemplary*). This is indicative of clear and managed responsibilities for risk management, risk response management and reporting across the BBC (see Figure 18).

95. However, supporting and incentivising effective risk management is apparent from the Risk Maturity Model as an area for improvement. This is reflected in responses to the detailed risk characteristics covering recruitment, training and the reward system.

96. *Human Resource Standards*, capturing the existence or otherwise of a resource pool of skilled risk managers across the corporation that can be seconded to a Division or project as needs arise, is one of the lowest scoring detailed risk characteristics (see Figure 18). Whilst 30% of respondents scored this 1 out of 5 (*Ad-Hoc*) or 2 out of 5 (*Fractured*) indicating a lack of awareness of the existence of such a resource pool, it should be noted that this should not be seen as problematic due to the nature of the BBC's business. Different resourcing models can be used to provide effective support for different types of organisations.

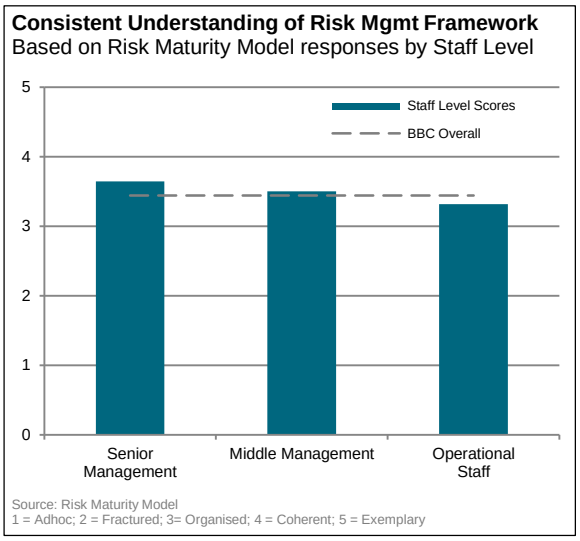

Figure 19

97. There is a consistent awareness and understanding of risk management across the different levels of seniority that participated in the Risk Maturity Model (see Figure 19). This demonstrates good degree of maturity when compared with other large organisations where risk management understanding can differ considerably across different levels of seniority, generally with knowledge and understanding deteriorating as seniority decreases.

Training

98. There is little formal risk management training currently in place at the BBC. The Business Assurance homepage on the BBC's intranet Gateway did provide all staff with access to a basic risk management training module. However, this module has been disabled until decisions are made on who the appropriate audiences are and what the content they require.

99. The Central Risk Team is in the process of undertaking a training needs analysis across the BBC to ensure risk management skills and knowledge can be valued, encouraged and developed. The key objective of the analysis is to develop an appropriate portfolio of training materials, building on existing training modules, targeting the differing needs of a variety of audiences. The training portfolio will include materials formally delivered by the BBC Academy, training and communications materials available for use by the Central Risk Team, and also informal learning materials that will be made available via the Business Assurance homepage.

100. Senior management believe that they would find it useful to have focused risk awareness sessions to provide a strategic level understanding of how risk management is being implemented across the BBC. These sessions should be supported by relevant case studies covering good practice and lessons learned thereby providing an understanding of what works in the BBC environment.

101. Whilst staff do not undertake formal risk management training, they do receive comprehensive training on existing risk controls such as the Editorial Guidelines, Fair Trading and Safety, Security and Resilience with many modules included as part of staff induction courses. This is a key area of strength even though some staff do not necessarily equate this type of training to formal risk management education.

102. **The BBC's ongoing risk management training needs analysis should be completed and implemented.** The analysis should help develop a more extensive portfolio of training materials covering the different needs of different audiences across the BBC. The approach should develop a more formal awareness of the risk management competence which could be then be incorporated into the annual appraisal process for appropriate staff.

103. **The BBC should consider implementing practical senior management risk awareness sessions.** These awareness sessions should not be theory based, but should focus on real and relevant case studies covering both good practice and lessons learned. This approach should provide senior management with an understanding of the various elements of good practice that could be implemented across the BBC.

Central Functions

Supporting assurance functions such as the Central Risk Team, Internal Audit and the Project Management Office are well integrated throughout the business and are seen as advisors to drive change, improve the quality of data and support the decision making process. The BBC uses a number of over-lapping IT systems to manage and control risks, which can create duplications and inconsistencies.

104. Functions such as Business Assurance, including the Central Risk Team, and the Project Management Office provide an effective risk management support mechanism to the Divisions. They support initiatives such as project gate reviews and Finance Director Peer reviews[4] that provide assurance on how effectively the risks are being managed; they also support cultural change, help improve outputs and data quality, and provide risk identification and assessment facilitation sessions. These resources and activities help to ensure that the risk management process and practice, existing control effectiveness, and key strategic and operational risks are well understood. The Central Risk Team and the Project Management Office have also worked together to integrate project performance and risk reporting; as a result this is an effective mechanism for providing a clear understanding of project delivery performance.

105. The annual 2015/16 Internal Audit Plan was developed using a risk-based approach in order to provide assurance on both strategic and operational risk. The plan was made up of three parts: coverage of main risks, core assurance activity and number of audits. The plan was developed following discussions with management on key risk areas and assurance needs, as well as a review of key Divisional and strategic risks. The plan aims to provide assurance for both executive risks and operational or business as usual risks. The following activities were undertaken:

    - Divisional leaders interviewed on views of risk areas and assurance gaps;
    - Top risks summary reviewed;
    - Potential audits identified that address some of these risks;
    - Main lines of defence[5] identified for each corporate risk, including planned audits from the steps above;
    - Gaps in assurance considered and audit plan refined, taking into account gaps and the skills and resources available; and
    - Assurance maps produced. Key risks identified in the standard heat-map were listed and three lines of defence mapped. The third line of defence includes the audits that are conducted by the audit team, with audits planned for the forthcoming year highlighted.

106. At the operational level, respondents for every Division scored the key risk characteristic *Control Activities* was scored above average in the BBC's overall risk management framework by every Division (see Figure 12). This is indicative of a good linkage between risks, related responses

[4] A review of whether risk and mitigation are being effectively considered for projects and business initiatives.
[5] The first line of defence is operational controls and Divisional Boards; the second line of defence is the Executive Board and the Central Risk Team; and the third line of defence is the Executive Audit Committee and the internal/external audit.

and existing controls, with the ability for each Division to manage its own controls, such as Editorial Guidelines, Fair Trading guidelines and Safety, Security and Resilience processes and procedures.

107. However, respondents scored *Types of Control Activity* low relative to the other Risk Maturity Model characteristics, indicative that there is room for improvement on the consistency of controls across the organisation (see Figure 14).

108. Internal audit has had a positive impact within the BBC. The existing linkages of risk to strategy, policy and business plans provide a foundation for ensuring there is a risk-based approach to auditing. Some senior executives requested more visibility as to how all the various assurance functions fit together to provide assurance that all the enterprise level of controls are in place to address the key risk categories the BBC needs to manage.

109. There is good integration and collaboration between the Central Risk Team and Safety, Security and Resilience. The Safety, Security and Resilience team capture safety and environment risks and provide the Central Risk Team with the latest trends and observations that can then be incorporated into Divisional and Executive Board risk registers.

110. *Monitoring* is the second lowest scoring characteristic from Risk Maturity Model responses (see Figure 3). The score, which shows the BBC's approach is compliant, also indicates that more can be done in terms of validating and auditing risk related information, and the risk management process. Process deficiencies, completeness and integrity of data and timely completion of agreed actions should be reported and rectified.

111. **The BBC should maintain the current format of the Central Risk Team.** The Central Risk Team should continue to be seen as advisors providing direct resource to support the business in order to drive change and increase the level of ownership and accountability.

112. **The BBC should consider the feasibility of undertaking a risk and assurance mapping exercise to provide confidence that assurance functions, policies and controls are relevant and effective.** The existing framework used by Internal Audit to map key risks against the three lines of defence should be an input into this process. This approach will provide a good understanding of how all the assurance functions fit together and provide a degree of confidence that the BBC's enterprise level of controls are addressing its key risk themes.

Technology

113. In 2006, the BBC deployed a corporate risk management software system across all Divisions. The aim of the system was to capture risks and related mitigation at corporate, Divisional and business unit levels and to monitor the effectiveness of existing mitigation and control activities. With 194 live users, the system contains risk information from all parts of the BBC. It is referenced in the Risk Management Procedure Guidance for Managers document. The system is a key support mechanism for the BBC's risk management process.

114. The risk management software system covers all of the basic enterprise-wide risk management needs in terms of risk identification, assessment, evaluation, reporting and review. Users of the system also have the ability to create their own controls and map identified risks against controls. Access to the system is controlled by the Central Risk Team and is provided to individuals who are leading risk management proponents in any particular part of the business, at either

Divisional or team level. Each Division has access to a separate section within the system, allowing users to only see risk information pertinent to the area of the business they work in. The system is also fully compatible with the BBC's IT environment and no technical compatibility issues have been identified to date.

115. The BBC is considering upgrading the current risk management software system and has already commissioned the software provider to tailor specific forms and reports. The current version is due to go out-of-support and an upgraded system is required to support recent improvements to the risk management process. The alternative is to look at the feasibility of completely replacing the existing system with a new system that has the flexibility to support future integration needs.

116. Risk and control data in relation to the BBC's projects, the Safety, Security and Resilience team and security matters are stored in a project risk tracking system and an occupational health and safety management system, separate to the risk management software system. The Internal Audit function also uses a separate internal audit system to manage audits, record findings and monitor remedial actions. The internal audit module within the BBC's risk management software system is disabled. This approach has the potential to create duplication and inconsistencies in relation to control data and can lead to unnecessary management and administrative costs.

117. The availability of *Risk Information* is identified as a relative strength by Risk Maturity Model respondents (see Figure 20). This indicates a general awareness that risk management information is made available across the organisation via software systems and reports in order to support the decision-making process.

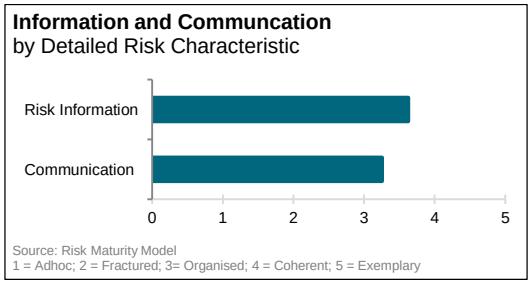

Figure 20

118. Nonetheless, at both senior and operational levels, some issues were raised concerning ease of use and reporting limitations of the BBC's risk management software system. Despite a number of strengths, more flexibility is required in terms of reporting and use of different scoring criteria that are required for operational and project related activities. For example, the system is not configured to produce the current heat-map reports that are presented at Divisional, Executive Audit Committee and Executive Board levels. This increases the administrative burden on the Central Risk Team who need to produce the reports manually.

119. One option to improve the level of integration of the existing risk and audit systems is to create a holistic Governance, Risk and Compliance environment to unify these functions (see Figure 21). In 2014, the BBC undertook a benchmark review assessing the feasibility of implementing such a Governance, Risk and Compliance solution; functions that were assessed include Corporate Risk and Investigations, Internal Audit, Legal, and Information Security. According to the BBC, a number of governance and risk management requirements were identified and an overall recommendation was made that due to the number of existing systems, any chosen GRC solution should not aim to displace these existing systems, but should be able to integrate with them. Two main options were outlined:

- The selection of one of the market leading Governance, Risk and Compliance suites but with an emphasis on the integration and customisation elements as a major selection criteria; and

- The development of a bespoke BBC over-arching cloud-based offering to consolidate and move data between existing tool sets which would offer a high level management capability for the disparate suites of software.

120. It is understood that, at a meeting in August 2014, the BBC decided that the implementation of a pan-BBC Governance, Risk and Compliance environment would be prohibitive in terms of cost and postponed the initiative. However, the Information Security function has decided to conduct a limited proof of concept for the implementation of a Governance, Risk and Compliance system within their specific function. The findings from this proof of concept should be fed into a central risk system improvement roadmap that addresses the specific functionality and integration needs of risk management across the BBC.

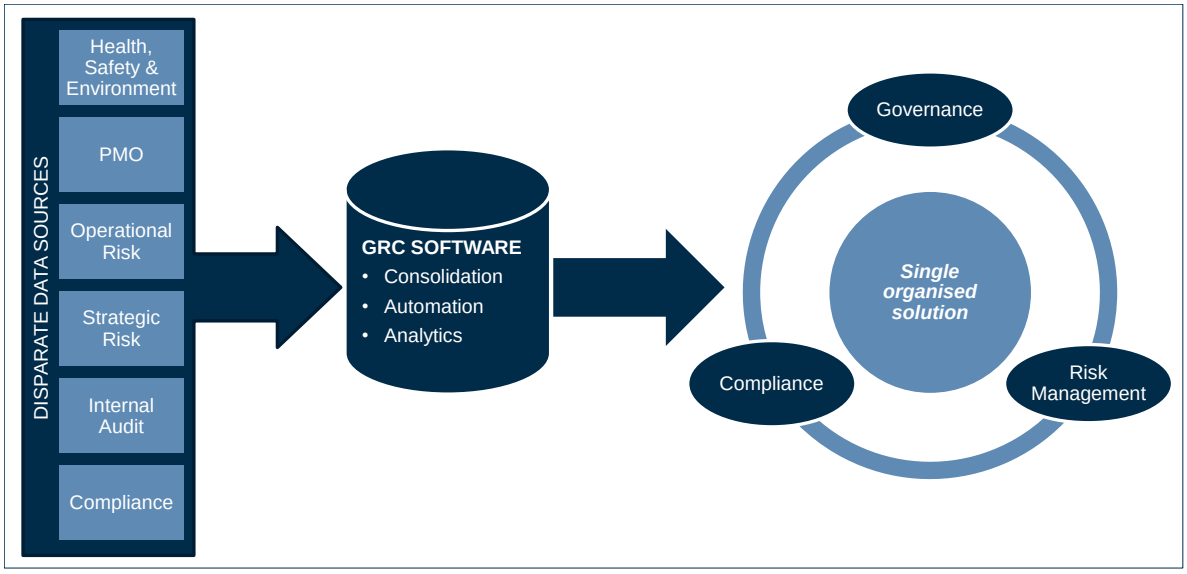

Figure 21 – Overview of an Integrated Market-Leading Governance Risk and Compliance System Approach

121. In the meantime, in order to improve the aggregation and monitoring of risk, and support improvements in the current risk management process, an upgraded or new risk management system, if implemented, should deliver additional functionality. This should include features such as:

- The development of strategic and operational risk heat-maps currently used at Executive Board level;
- Improved portfolio view of risk and response plans;
- Support the use of Key Risk Indicators for improved monitoring of risk related events;
- Recording of risk interdependency to support aggregation and escalation of risk;
- Improved access and review for customised groups of users; and
- Support different sets of scoring criteria.

122. The risk register module within the project risk tracking system is integrated with all the other project controls (milestones, contacts, RAG, dependencies, etc.). This allows project managers to consider the joined up picture rather than viewing risks independently. Interfacing with the

existing Project Management Office tool or migration of project risk data into a new risk management system, if implemented, may therefore not be straightforward. The key challenge is to ensure that any new risk management system can support the different risk identification and scoring mechanisms that are used with the existing risk management software system and project risk tracking system. This will ensure that genuinely large scale outcome risks can be escalated from the project domain to the business domain within the same system.

123. All data contained within the existing risk management software system was assessed as part of the desktop review, including Divisional risks, and specific risk registers. In general terms, the majority of risks contained within the database were well articulated. Their relevance to the BBC's business is outside the scope of this review. Basic inconsistencies or shortfalls requiring attention were related to:

- Some risk descriptions failed to provide sufficient background and underlying causes. This is important since response strategies are aimed at managing/controlling causes;
- Some risks were very generic in nature and not specific enough to the BBC environment;
- Confusion in terms of the use of control and response actions making it difficult to understand how risks should be mapped to local controls and enterprise level of controls; and
- Some risks did not contain forecasted scores which are used to provide a degree of confidence that the combined controls and mitigations will have the required effect.

124. **The BBC should complete the on-going Governance, Risk and Compliance system proof of concept in Information Security and feed the lessons from this initiative into the development of central risk system improvement roadmap.** This system improvement roadmap should include basic integration needs for the corporate risk management system. For example, whilst the existing project risk tracking system is heavily integrated into the BBC's project management environment, consideration should still be given to understand how key project risks could be extracted and reported via the enhanced and up-to-date central risk management system.

125. **The BBC's Central Risk Team and Divisional risk representatives should undertake an integrity and quality review of the current risk data sets.** Risk management data contained within the various systems should be reviewed for quality and integrity purposes to ensure the risks are relevant, consistent in format and provide a clear understanding of the underlying causes, controls, and mitigation objectives/scores.

126. **The BBC's Central Risk Team should complete a feasibility assessment that considers upgrading or replacing its current risk management system.** It is in the BBC's interests to ensure that it has a fully supported risk management system in place that can satisfy existing reporting needs and process improvements, reduce the existing reporting burden on the Central Risk Team, and have the flexibility to support future integration needs with other risk-related BBC systems.

Gateway Business Assurance website

127. The Business Assurance website on the BBC Intranet is being updated to contain the latest information on processes and training. However, at the time of the review, a digital and accessible knowledge base of BBC case studies, prompt lists, lessons learnt and identified good practice did not exist. The current risk training module, entitled Business Risk Awareness, has been disabled as it is out of date and new on-line training modules are being devised. These modules are planned for implementation on completion of the training needs analysis and will be designed to help drive awareness and understanding.

128. **As part of the BBC Business Assurance website refresh, the BBC should consider implementing a knowledge base of 'lessons learned', industry-specific case studies and identified good practice from across the Corporation**. The website should provide access to typical risks and opportunities that could affect the Corporation, and could therefore act as an effective prompt during risk identification and assessment sessions.

Appendix 1

Scope

The over-arching question for the review, posed by the BBC Trust, was *does the BBC manage risk effectively?* This breaks down into three key questions, as follows:

1. Is the BBC's approach to risk well considered?

    - An assessment of whether the BBC's risk management policies and procedures are fit for purpose.

2. Is there evidence that the approach to risk is working well at a senior level?

    - An assessment of risk management at a senior level and the extent to which information on risk is used to support strategic decision making.

3. Is there evidence that the approach to risk working well at an operational level?

    - An assessment of the culture of risk management, whether risk management processes are being following in practice, and whether operational decisions are supported by information on risk.

The review includes all of the public service broadcasting elements of the BBC. It does not include the Corporation's commercial subsidiaries such as BBC Worldwide, except to the extent that their risks feed into the corporate reporting structure at a senior level.

The review covers the BBC's existing arrangements for managing risk, and any work in progress to develop these arrangements. The review does not seek to assess how risks have been managed in the past. In addition, specific risks relating to child protection, and the management of on-screen and on-air talent were not reviewed in depth as these have already been assessed by other recent reviews commissioned by the BBC.[6]

[6] Child protection at the BBC: policies and practices, and a review of the BBC's arrangements for managing on-screen and on-air talent

Appendix 2

Overview of Approach & Methodology

Alvarez & Marsal (A&M) undertook a full Risk Diagnostic for the BBC, providing an in-depth review of the BBC's risk management process, culture and attitude. A&M's Risk Diagnostic solution is built around three pillars: a desktop review, the senior executive interviews and the Risk Maturity Model.

Desktop Review

As part of the desktop review, the BBC's documentation and data sources relating to risk were reviewed and examined to gain a sound understanding of internal risk management structures and processes. Materials and systems reviewed included:

- Executive Board risk update papers;
- Divisional Board risk update papers;
- Executive Audit Committee risk update papers and audit plans;
- Outputs of the BBC's risk management software system;
- Project Management Office performance dashboards;
- Business Assurance Homepage on Gateway; and
- Process and policy documentation.

Senior Executive Interviews

Discussions took place with senior executives whose role or responsibilities gave them accountability for risk. These discussions were conducted on a one-to-one basis and took the form of a conversation, rather than a verbal questionnaire. The results of these discussions, when aggregated, provided a qualitative view of the attitude of the BBC's key personnel to risk management.

Executive interviews were conducted with the following people:

Trust, Non-Executive Directors and DG's office

- Simon Burke – BBC Non-Executive Director
- Rona Fairhead – Chairman BBC Trust
- Phil Harrold – BBC Company Secretary
- Nick Prettejohn – Chairman BBC Trust Value for Money Committee
- Fiona Reynolds – BBC Non-Executive Director

Television

- Sonia Magris – Finance Director for TV
- Bal Samra – Commercial Director and Managing Director TV

Radio

- Helen Boaden – Director Radio

News

- David Jordan – Director, Editorial Policy and Standards

Finance & Operations

- Anne Bulford – Managing Director Finance & Operations
- Mike Ford – Director of Risk and Assurance
- Paul Greeves – Director of Workplace and Safety
- Ian Haythornthwaite – Director of Finance
- Valerie Hughes D'Aeth – Director of Human Resources
- Sarah Jones – BBC Group General Council
- Matthew Postgate – Chief Technology Officer

Strategy & Digital

- James Heath – Director, Policy and Charter
- Gautam Ranganjaran – Director of Strategy
- Ralph Rivera – Director, Future Media

Scotland

- Alan Dickson – Chief Operating Officer, BBC Scotland

Wales

- Rhodri Talfan Davies – Director, BBC Wales

Risk Maturity Model

A&M's bespoke Risk Maturity Model provides an overview of risk behaviour set against COSO ERM Framework, ISO 31000 and good practice captured over the last ten years. This process assesses risk management within the organisation's culture and provides an objective baseline for measuring progress, behaviours and the organisation's risk management maturity. The model complemented the senior executives' interviews by adding a perspective of risk management from across the breadth and depth of the organisation. The aim of the model was to provide a structured means of highlighting

the current effectiveness and consistency of the risk management process used across the BBC. The process was delivered in a group format either on-site or remotely. Participants selected had a degree of risk management responsibility.

The model covers eight key risk characteristics:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

These are broken down to 37 detailed characteristics, covering both process and behavioural risk maturity. The characteristics are based on the key requirements and guidance points outlined by the international standard and risk management frameworks.

The model consists of five levels maturity (see Figure 22), ranging from 1 out of 5 (*Ad-Hoc)* to 5 out of 5 (*Exemplary*). An organisation operating at 3 out of 5 (*Organised*) is regarded as being fully compliant with corporate governance requirements for managing and reporting risk. For levels above 3 out of 5 (*Organised*), risk management is seen to be driving business performance with closer integration to strategic and financial planning.

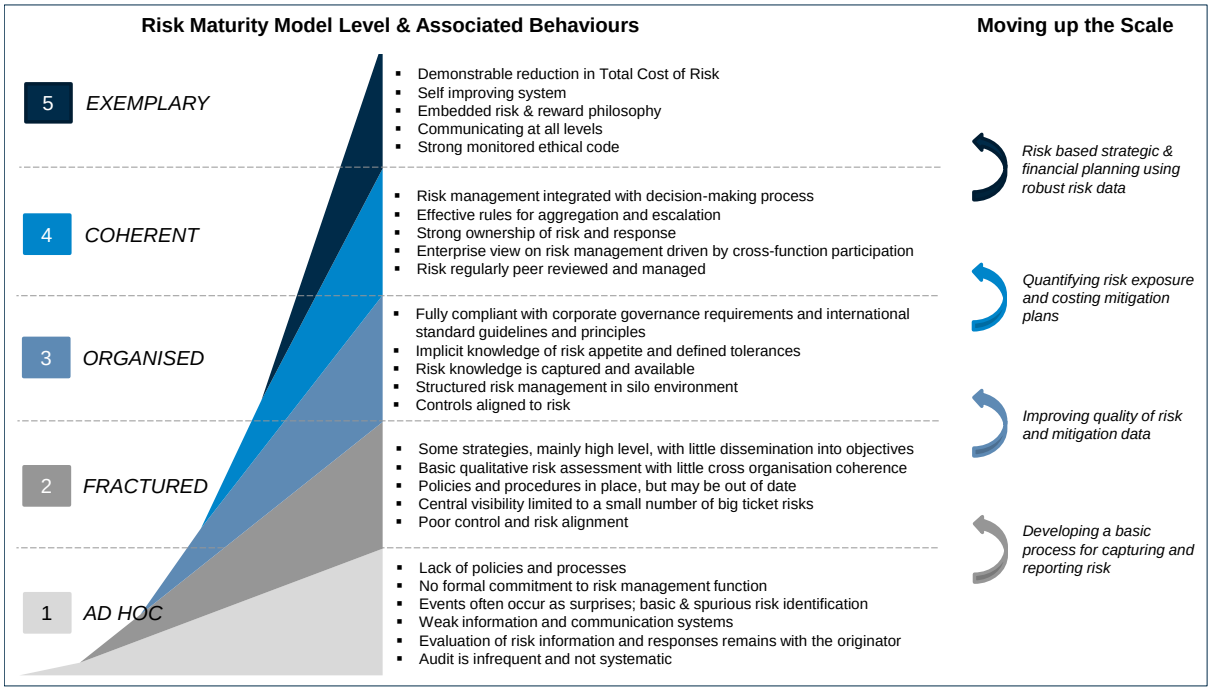

Figure 22 – Risk Maturity Model Summary

This model was used as the basis of the workshops and one-to-one meetings with key stakeholders or risk champions across the BBC Divisions. These meetings were supported by BBC personnel and consultants from A&M. Verbal guidance was provided in terms of the meaning for each of the risk characteristics, coupled with examples of behaviours by organisations with high and low levels of maturity. Follow-up calls were organised to provide additional guidance to some of the participants.

For each of the risk characteristics, contributors were asked to choose the scenario that was most relevant to their Division. Maturity scores were then averaged for each risk characteristic, collated and analysed for each Division. The results indicate a framework and attitude between 3 out of 5 (*Organised*) and 4 out of 5 (*Coherent*) with clear areas of strength and opportunities for improvement across Divisions and characteristics.

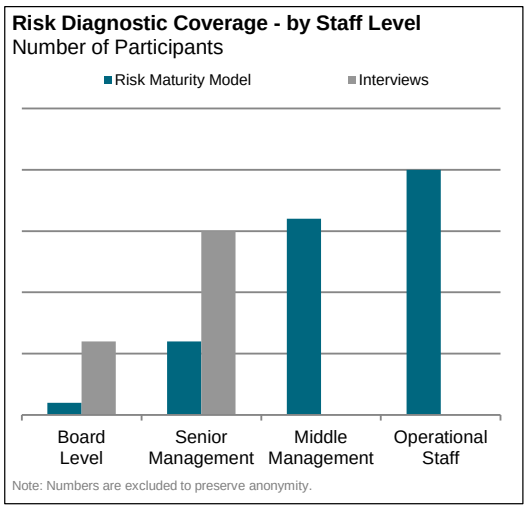

Figure 23

Responses were gathered from staff across the operational level and all Divisions, covering both content areas and administrative/operational functions (see Figure 23).

Appendix 3

Enterprise Level Controls at the BBC

Examples of effective enterprise level controls that have been implemented at the BBC are provided here. This relates to the Risk Response and Control section (paragraphs 64-69) of Processes and Tools (Chapter 4).

Editorial Guidelines

1. The Editorial Guidelines are seen as a robust and effective risk control at all levels of the BBC and are made available to all staff. These guidelines have been refined and developed over a long period of time and are considered to be a mature and robust control system. They provide the BBC with a control and escalation framework for content that is considered to be effective both by management and staff. The different Divisions believe that the escalation mechanism for editorial related risks and issues is clear, robust and adhered to. The Guidelines are sometimes described as 'the Bible' by BBC staff and are considered a first point of reference by many. Neither the hard copy or online versions of the Guidelines are changed between iterations; variations are reflected in Guidance, both new and updated, which is available online.

2. At the risk maturity workshops, some employees said that, under certain circumstances, they combine their judgement and experience with the requirements set out in the Editorial Guidelines to determine the most appropriate course of action. However, they still consider the Editorial Guidelines to be an excellent guidance tool. At the operational level, whilst most staff understand and abide with the Guidelines, they do not necessarily recognise that by doing so they are actively managing risk.

3. The Editorial Guidelines are widely distributed. The BBC issued initially 19,000 copies of the 'Green Book' to programme makers in 2010, 1,000 of which were to Independents. They continue to be distributed to new joiners and Independents. The quality and relevance of the Editorial Guidelines is assessed through a regular user survey. A good reaction was given to the Guidelines in the last survey, carried out in autumn 2014, with responses from 785 programme makers.

4. There are a number of editorial controls in place including compliance forms for recorded programmes. These forms must be signed off by a senior programme executive, confirming that all aspects of risk have been addressed. The form must be completed and signed pre-transmission of all programmes. Therefore, for every recorded programme produced, editorial risks are identified and those that may have significant reputational or financial impacts are escalated to the Managed Risks Programme List, which is reviewed on a weekly basis by the Director General. In addition, there is Live Output Guidance which offers advice on how to manage editorial risks in live programmes. Controls are also included in talent contracts to ensure there is compliance with Editorial Guidelines. There is a second route of escalation whereby potential issues in relation to Editorial Standards and talent management are red flagged and reported to the Director General on a twice weekly basis. In addition there is a 365 day / 24 hour Editorial Policy help line where advice on editorial decisions can be obtained. All journalists undergo Editorial Guidelines training, including freelance/casual journalists.

5. The Director of Editorial Policy and Standards is consulted on editorial items that are regarded as high risk with direct escalation, if necessary, to senior output directors and the Director General if programme makers intend not to follow advice. The Guidelines are subject to a major review every four to five years to account for the changing environment that the BBC operates.

On-air Talent Management

6. The BBC has a robust framework for managing risks around talent based on a number of control and mitigation mechanisms. The risk assessment and approval of talent is driven by the production team as part of the risk assessment of programmes. The standard pre-recorded programme compliance form assesses the casting brief and key on-screen talent, and will ultimately serve as an audit trail. In addition, the Compliance Conversation Checklist provides guidelines around necessary training for talent and conflicts of interest.

7. The production team is accountable for controlling risks around talent management. Executive producers and heads of departments are responsible for assessing the suitability of talent, reviewing experience, specialisation and credibility. Additionally, the producers are accountable for ensuring compliance with regulations and standards, including standards around health and safety. They will also set up pre-production discussions to raise and enforce risk awareness with talent.

8. Two formal escalation routes are in place to raise risks, including talent risks: the 'red flag process', which is reviewed by the Director-General twice a week, and the Managed Risks Programme List. The seniority of individuals consulted in the escalation process will be proportionate to the issue at hand. In serious cases, the issue may be raised immediately to the Directors or Director General. In all cases, the level of escalation is a judgement based decision.

9. Contracts also form part of the control mechanism around talent management. The clauses in on-air talent contracts clearly define expected behaviours, including rules around impartiality whilst on air and activities outside the working environment. These contractual clauses represent a significant control mechanism as the BBC has clear responses in case of breach of contract. These contractual obligations are not homogenous; they vary by talent depending on the role of the individual.

10. Most of the high profile talent at the BBC are employed on a freelance basis for predetermined periods based on the length of the engagement. Standard contracts contain similar clauses relating to behaviour and BBC standards. As these contracts are for fixed periods, the BBC has an opportunity to review and recalibrate contracts, including role-specific clauses. Renewal of contract discussions can take place up to Board level.

11. The BBC also provides mandatory and voluntary training courses for people involved in production, including health and safety. Completion of these modules is monitored by the BBC Academy on a regular basis.

Fair Trading Guidelines

12. It is recognised that in the promotion of its Public Purposes as set out in the Charter, the BBC may engage in the provision of Commercial Activities. These activities could have an impact on competition in the markets in which it operates. As a publicly funded organisation, the BBC has a responsibility to ensure that whenever it engages in trading activities, whether public service or otherwise, it does so in a way that reflects its commitment to Fair Trading and does not compromise the achievement of its Public Purposes. Fair Trading accounts for a number of

requirements contained within UK and EU Competition Law, specific obligations in the BBC's Charter and Agreement and Fair Trading policies which sets out, inter-alia, how the Trust will ensure the BBC takes account of its competitive impact on the wider market. Compliance with Fair Trading obligations is mandatory and is the responsibility of every BBC employee.

Contract Management – StaR Forum

13. The STaR (strategic relationships with suppliers) forum was created to act as a control to ensure strategic, outsourced contracts are run effectively to deliver services at optimum cost whilst meeting the current and future needs of the BBC. The forum is accountable for ensuring that the contribution from StaR contracts is visible and meets expected quality and value. The focus is to ensure contract management teams are well supported and that interdependencies between contracts are clear and well managed. Part of the remit is to identify and manage common risks and periodically review contracts and suppliers to ensure that risk to operational activity is adequately managed.