Management of Risk in Government

A framework for boards and examples of what has worked in practice

- A Non-Executives' Review

January 2017

Contents

Foreword 3
Part 1 – The Framework 5
Types of risk 6
Managing risks 8
Roles 9
Implementation 10
Part 2 – Example questions, tools, techniques & templates 11
Annex A – Suggested questions for the board to consider 12
Annex B – Suggested questions for risk practitioners 14
Annex C – Tools, techniques & templates 20
Creating positive risk management behaviours and culture 21
Building risk management capability 24
Scanning the horizon 25
Capturing risks 27
Articulating risk 29
Assessing risk 30
Establishing risk appetite 33
Reviewing risks 34
Reporting on risks - in summary 36
Managing and reporting on risk - specific risks 39
Communicating risk information 42
Building risk maturity 43
Annex D – Additional advice on risk management 44

Foreword

Risk is part of everything we do. We all manage risk – often without realising it – every day. We live in an ever-changing world and the pace of change is increasing. This carries with it uncertainty and that uncertainty brings new opportunities and risks. How we manage those has never been more important in helping us meet our objectives, improve service delivery, achieve value for money and reduce unwelcome surprises.

We believe in the value of effectively managing risk: it informs business decisions; enables a more effective use of precious resources; enhances strategic and business planning; and strengthens contingency planning.

None of this is possible without a supportive risk culture. A positive risk culture, one which encourages openness and discusses real business issues in a realistic manner, is absolutely essential to the effective management of risk. Everyone, from the board down, has a clear role to play in establishing and maintaining that risk culture.

Last year, we set out to use the non-executive network to try and break down departmental silos, encourage the elevation of best practice and strive for continuous improvement. Ian Barlow (Lead Non-Executive, HMRC) has led the collective efforts of non-executives to improve risk management across government. A key part of that work has sought to identify examples of risk management that work in practice and support government bodies in sharing and adopting this. This has been achieved through an on-going series of peer reviews between departments alongside support and advice from the Audit and Risk Assurance Committee Chairs Network and other government risk experts.

We have found that many principles and concepts for risk management, such as those laid out in HM Treasury's Orange Book, are now very well established. Whilst the principles and concepts have been implemented, the wide variety of approaches adopted by government bodies provides a clear opportunity for them to learn from one another.

This document does not aim to bring about a one-size-fits-all approach to managing risks, or to centralise risk management in government. This approach would be highly unlikely to work for departments, agencies and public bodies of different sizes, structures and needs. However, it does aim to provide a broad and high-level framework of good practice that can help organisations ensure their arrangements for managing risk are structured and comprehensive. It includes a high-level checklist of questions for both board members and risk practitioners to test and challenge the risk management arrangements for their organisation.

The rest of this document builds on, and extends, the risk management principles and concepts that have come before – see Annex D – to provide a simple yet structured framework to implement them in practice. This is further supplemented by some of the best examples of tools and techniques that have been used successfully in parts of government.

This guidance is intended to be useful to:

- Executive and non-executive members of the board
- Senior staff whose leadership is vital
- Managers
- Audit and Risk Assurance Committees
- All those involved in risk management

Each government department, agency and public body should now consider with their board how to implement the framework to suit their specific needs before 30th June 2017. Page 10 gives guidance on how to put together an implementation plan and we are sure the whole document can be used in support of this process.

Once in use, we expect this document to be a highly valuable source of ideas to continually refresh and improve the management of risk in government. By doing so, we will be better placed to innovate and deliver better results for the public.

John Manzoni
Chief Executive of the Civil Service
and Permanent Secretary for the Cabinet Office

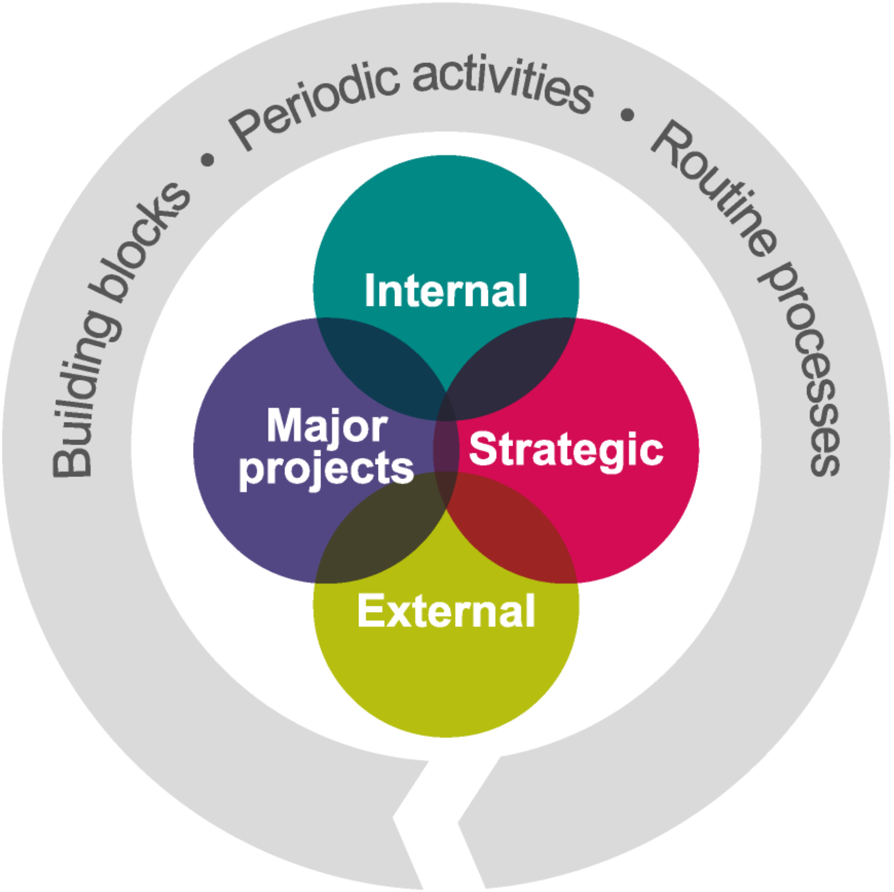
Sir Ian Cheshire
Government Lead Non-Executive
and Non-Executive Board Member

Part 1 – The Framework

The framework includes:

- **Four different types of (or lenses for looking at) risk, reporting to the board on each**
- **Three main elements of risk management, working together**
- **A model set of roles/responsibilities for the organisation to use or adjust to meet its needs - ensuring there is clarity over who does what without gaps**

The relationship between the types of risk – internal, external, strategic and major project - and the elements of risk management – building blocks, routine processes and periodic activities - are shown in the diagram below. All elements are needed across all risk types to allow effective risk management to flourish.



More detail on the four types of risk can be found on pages 6 and 7, the elements of risk management are covered on page 8, and roles and responsibilities discussed further on page 9.

An approach to implementing this framework is given on page 10. Note that implementation of this framework is not intended to replace, and should not stop, any good practices that the organisation has found to work well – these can and should continue.

Types of risk

Every organisation will face different types of risk - internal, external, strategic, and those arising from major projects. This framework asks that the board receive regular reports on the organisation’s general approach to managing each type of risk, as well as highlighting the organisation’s most significant risks and what is being done to address them. The types of risk in this framework, as outlined below, are not mutually exclusive: they can be used as four different lenses to ensure all major risks and all types of response are considered at board level. This approach builds upon the successful new framework championed by the Financial Reporting Council (FRC)[1] for the private sector and can lead to a comprehensive management of an organisation’s risks.

Understanding the type of risk being faced can also help determine what action is best to take. The table below provides examples.

Type of risk	Features and approaches	Examples
Internal	These are risks over which the organisation has some control, for example risks that can be managed through internal controls and, where necessary, additional mitigating actions. This often involves traditional risk management, such as risk registers, controls and assurance.	• Fraud • Health & safety • Capacity & capability • Data security • Delivery partners
External	This focuses on big external events/perils and then considers how to make the organisation more resilient to such events, in part because of difficulties on assessing likelihood[2]. A tried and tested approach to managing external risks is through considering the impact those external events could have on infrastructure, finance, people, operations and reputation. A common example of a resilience framework for infrastructure is a business continuity plan.	• Economic downturn • Terrorist attack • Extreme weather • Cyber attacks

[1] See C2.1, C2.2 and C2.3 in the FRC 2014 Corporate Governance Code. FRC code relates to public reporting so goes further than this framework is requesting.

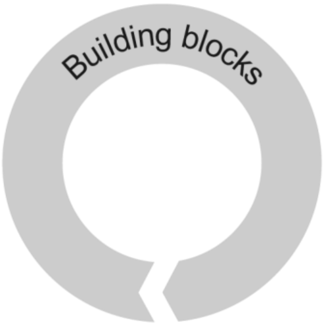
[2] The rationale for managing and mitigating external events like this is that there can be hundreds of such events, of which most have a very low likelihood. Yet the chance of one such event among the hundreds occurring in any one year is not low. The problem is that nobody can predict which one it will be.

Strategic	This third element concerns the organisation’s raison d'être and key objectives (such as the organisation’s enduring purpose and the objectives set out in the Single Departmental Plan), identifying the principal risks to the achievement of those within a set timeframe. For some this could be the lifetime of a parliament. Risks in this area would be accompanied by regularly monitoring and adjusting interventions, as necessary. Forward-looking charts are often helpful here.	Can be: • immediate impact risks to the organisation’s ability to continue operating, e.g. loss of customer data; or • slow-burning risks that grow and eventually prevent delivery of objectives, e.g. staff turnover or leadership capability.
Major projects	Major projects form such a critical part of the plans for many government bodies. Experience suggests that one or two critical projects for that organisation should be considered at board level in their own right. The key is to only report to board level on the two or three that really matter This should be via whatever tools, techniques and reporting are appropriate for each.	These risks will be specific to the major project in question, and could involve: • shifting requirements • slippage in delivery timeframes • failure to deliver

Managing risks

The framework comprises three main elements. These elements – building blocks, routine processes and periodic activities – are regularly found in effective risk management arrangements and encompass the three lines of defence.

The table below provides examples of activities that make up the three main elements. Whilst this list aims to be reasonably comprehensive, the framework only requires each department to consider which activities it will adopt and prioritise under each heading. The list is provided to help risk practitioners decide what action to take. There is no requirement to use every item below. The list can also be used as a tool for the board to challenge the risk practitioner at the appropriate time.



Essential building blocks include:

- Creating positive risk management behaviours and culture
- Establishing roles and responsibility
- Communicating risk information
- Building risk capability, including training for risk practitioners

Essential routine processes include:

- Identifying risks, including those responsible for managing them
- Assessing risks and establishing tolerance
- Addressing risks, including contingency arrangements
- Reviewing and monitoring risks, including ‘deep dives’
- Reporting on risk

Recommended periodic activities include:

- Assuring the board that risk is being properly managed
- Assuring risks from arm’s length bodies
- Scanning the horizon/ environment, including National Risk Register risks
- Building risk maturity
- Peer reviews
- Learning lessons
- Exploiting data and data analytics
- Building and testing resilience frameworks

Roles

The management of risk must not be left exclusively to the specialists. If consideration of risk is integral to all our work, we will be better placed to innovate and to deliver better results for the public. Ministers, the board, Accounting Officers, the Audit & Risk Assurance Committee and the organisation's sources of risk assurance (often referred to as the three lines of defence) all have a part to play in creating an environment where the effective management of risk can flourish. The table below highlights those key roles.

Post	Role (with regard to risk)
Ministers	Set the direction against political imperatives and articulate a high-level appetite for the risks to those imperatives.
Accounting Officers	Should set an appropriate tone from the top, for example by articulating risk appetite, championing and driving the effective management of risk and ensuring the risk function is supported in carrying out its role.
The Board / Senior Executive Team	Should support the Accounting Officer in articulating risk appetite and by leading the assessment and management of risk.
The Audit & Risk Assurance Committee	Should support the board and Accounting Officer by reviewing the comprehensiveness and reliability of assurances on risk management.
Managers (part of the 1st line of defence)	Should actively identify and manage risks as part of their everyday business, escalating them promptly as and when necessary.
The Risk Management function (part of the 2nd line of defence)	Should support and facilitate the organisation's management and oversight of risk. For example by building the organisation's risk capability and defining the organisation's risk management practices and framework.
Internal Audit (part of the 3rd line of defence)	Should provide independent and objective assurance on the effectiveness of the organisation's risk management arrangements, and share good practice through comparative assessment.

Implementation

The board should decide how it intends to implement this framework, as set out in the preceding pages.

Whilst there is no prescribed approach to implementing this framework, government bodies may wish to consider the following when preparing their implementation plan:

1. An articulation of the key issues – ‘the difficult questions’ – for the organisation
2. The role of the Minister(s) in the management of key risks
3. Who, at board level, will sponsor the implementation of the framework
4. How to report to the board on the organisation’s key internal, external, strategic and project risks
5. Of the activities in the three main elements:
    a. which should be applied in that organisation;
    b. how will they be operated; and
    c. how and when they will be reviewed by the board.
6. How the key risks for the organisation’s arm’s length bodies will fit into 4 and 5 above
7. The respective roles of, and interrelationship between, the Audit and Risk Assurance Committee, any executive bodies and main board, in terms of who does what and when
8. The role of Internal Audit in assuring the effectiveness of risk management arrangements
9. Other risk intelligence from other parts of government, such as horizon scanning and the National Risk Register

Part 2 – Example questions, tools, techniques & templates

The board and risk practitioners, in particular, have an essential role to play in making the framework, discussed in Part 1, a reality.

In the annexes that follow:

- Annex A suggests some questions that board members may wish to ask to help test and challenge their organisation's risk management arrangements
- Annex B highlights the areas risk practitioners can consider in implementing the common elements.
- Annex C provides risk practitioners with tools, techniques or templates that have been used successfully in parts of government.

These tools, techniques, templates and questions are provided here to help risk practitioners learn from approaches that have worked in the past. Neither the tools, processes or templates nor the example questions form an exhaustive list, and not all items or questions will be relevant to every department.

Annex A – Suggested questions for the board to consider[3]

Members of the board have a critical role in establishing the environment that will allow the effective management of risk to flourish. The following table provides example questions that board members may wish to ask to test and challenge the risk management arrangements in their organisation. These questions are simply provided as suggestions, they are not a requirement, nor are they comprehensive.

Activity	*Example Questions.*	*Frequency*
Creating positive risk management behaviours and culture	1. How has the organisation set its desired values towards the effective management of risk?	Every year
	2. How have you assured yourself that these have been communicated by management?	Every year
	3. How have you assured yourself that desired behaviours are encouraged and inappropriate risk behaviours are discouraged?	Continuous consideration
Communicating risk information	1. How have you assured yourself that the board has clear and easy processes for bringing significant issues to its attention more rapidly when required?	Every year
	2. How does the organisation's management of risk capture and learn lessons from past events?	Ad hoc
Building risk capability	1. What suitable training, skills, knowledge and experience do the organisation's risk practitioners have?	Every year
	2. How does the organisation periodically assesses its risk maturity to identify areas for improvement?	Every year
	3. How has risk management been integrated into business as usual management?	Continuous consideration
Identifying risks to objectives	1. What events could derail the achievement of the organisation's business priorities?	Twice a year
	2. How have you assured yourself that the National Risk Register risks, which are particularly pertinent to your organisation, are recognised in risk discussions?	Every year

[3] This list of questions is based on Section 3 of the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting. For the purposes of this document, the list has been shortened and made applicable to the public sector

Activity	*Example Questions.*	*Frequency*
Assessing risks and establishing tolerance	1. To what extent does the organisation's assessment of its top risks resonate with your knowledge of the organisation?	Continuous consideration
	2. How comfortable are you with the amount of risk the organisation is carrying?	Continuous consideration
Addressing risks	1. What possible combinations of events might make a "domino" risk, where one big event causes other big events, much more likely?	Twice a year
	2. What contingency arrangements are in place for high impact risks, and are they sufficient?	Twice a year
Reviewing and monitoring risks	1. How have you assured yourself there is clear accountability for each of the organisation's top risks?	Continuous consideration
	2. How have you assured yourself that the quality of risk information is sufficient to support decision-making?	Continuous consideration
	3. How have you assured yourself that there is an active management of risks, i.e. the risk picture is dynamic and mitigating actions are delivered?	Quarterly
	4. How have you assured yourself that the organisation is sufficiently aware of the top risks faced by any arm's length bodies (ALBs)?	Frequency will be relative to the number of ALBs
Reporting risks	1. How has the board laid out its requirements for risk information, in terms of the nature of that information, its source and its format and frequency?	Every year
	2. How have you assured yourself that those reports help the board focus on what really matters - in a clear, succinct and accessible manner - that enables the Board's decision-making?	Continuous consideration
Assuring the board that risk is being properly managed	1. How do you periodically check that the organisation's risks are being properly managed?	Twice a year
	2. How do you periodically check whether the organisation's processes for risk management are effective?	Every year
	3. How have the respective roles of the board, executive and Audit & Risk Assurance Committee been established with regard to risk?	Every 2 years

Annex B – Suggested questions for risk practitioners

The following table provides example questions that risk practitioners in various organisations have found helpful in improving the effectiveness of risk management in their organisation. Asking these questions is not a requirement nor does asking these questions guarantee to address all risks properly. That said, they have proved useful in the past and can significantly help risk practitioners in future.

Element	*Activity*	*Example Questions.*
Building Blocks	Creating positive risk management behaviours and culture	1. How have you gauged your organisation's risk culture and people's attitude to risk management? 2. How have you made your organisation's risk management strategy and/or policy widely available to all staff? 3. How have you made explicit, in those documents, the importance of a positive risk management culture, where the active management of risk is considered integral to good business management? 4. How have you obtained your executive team's explicit commitment to positive risk management? 5. And how have you make that commitment widely available to all staff? 6. How have you ensured your risk management processes incentivise, rather than deter, positive management of risk behaviours?
Building Blocks	Establishing roles and responsibility	1. How have you made clear in your organisation who is responsible for the risk management function? 2. How have the respective roles of the board, the Audit and Risk Assurance Committee, managers of risk and risk practitioners it been made clear?
Building Blocks	Communicating risk information	1. What arrangements are in place to ensure the quality of risk information supports decision-making? 2. What are your organisation's existing upward reporting mechanisms for escalating risks in a timely fashion? 3. How have you ensured those escalation and de-escalation routes are clear and easy to use? 4. What feedback mechanisms are required following escalation?

Element	*Activity*	*Example Questions.*
Building Blocks	Building risk capability, including training	1. How are risk considerations integrated into other business processes, such as strategic planning, business planning, performance reporting and policy development? 2. How does the risk management function work in partnership with your organisation's performance and business planning functions, in order to bring a more holistic picture together for decision-makers? 3. What formal training in risk management, for example the Institute of Risk Management (IRM) qualification or the Management of Risk (MoR) practitioner qualification, is provided to risk management practitioners. 4. How have the organisation's risk guidance and tools been made available to all staff? 5. Which communities of risk management practice do you belong to, in order to share developments and learn from one another, both within your organisation and across central government (such as the Risk Improvement Group)?
Routine Processes	Identifying risks to objectives	1. To what extent have your organisation's risks been articulated so that the risk cause, event and effect are clear? 2. When will you next carry out a top-down 'what's keeping you awake at night' risk identification session for the top of your organisation? 3. From which perspectives are new risks identified, for example risks: a. internal to the organisation? b. external to the organisation? c. to the organisation's strategy? d. to major projects? e. to internal controls? f. to the organisation's viability? g. identified from past experience? 4. To what extent have techniques like 'pre-mortem' workshops been used to help stakeholders identify their key risks 5. How do you ensure a single owner for each risk is identified, making them responsible for the effective and timely management of that risk?

Element	*Activity*	*Example Questions.*
Routine Processes	Assessing risks and establishing tolerance / appetite	1. How have you ensured the process is as simple and easy to use as possible? 2. Have you used a risk matrix that assesses risk in terms of likelihood and impact? 3. To what extent does your organisation have a clear and consistent criteria to assess the impact and likelihood of a risk occurring? 4. How have you used an understanding of risk tolerance, risk appetite or target risk to decide what level of assessed risk is acceptable to management?
Routine Processes	Addressing risks, including contingency arrangements	1. For actions identified to mitigate risk, to what extent are they: • Appropriate to the risk in question? • Owned by a single individual, at the appropriate level of the organisation? • Clear? • Measurable? • Time-bound? 2. To reach an optimum position in responding to the risk, how do you use: • An understanding of the costs of risk impacts? • An understanding of the costs and effectiveness of each of the possible mitigating actions? • Comparisons with other risks and priorities? 3. How is the progress of the mitigating actions monitored? 4. How does your organisation assess the effectiveness of mitigating actions (once taken)? 5. To what extent is there an emphasis, for external risks, on resilience and contingency-type arrangements? And do these aim to reduce the impact of the risk on the organisation’s infrastructure, reputation, people or finances?

Element	*Activity*	*Example Questions.*
Routine Processes	Reviewing and monitoring risks, including ‘deep dives’	1. How are your organisation’s top risks reviewed, in terms of continuing relevance and significance, before being reported to the top of your organisation to inform decision-making? 2. How does that review obtain a suitably senior and broad perspective to add value? 3. How are perceived risks and risk exposures challenged in the light of available performance information? 4. How are periodic deeper discussions on the way specific risks are being managed carried out?
Routine Processes	Reporting on risks	1. How have you ensured risk information is presented in a clear, succinct and accessible fashion that enables stakeholders to focus on the key points and decisions that are required? 2. How do you brief key stakeholders on risk matters ahead of senior discussions of risk? 3. How have you ensured your risk information is presented in a way that encourages senior stakeholders to engage with it? 4. How do you explicitly include the direction of travel for the risks being reported? 5. For major project risks, how do you convey the key information stakeholders need to know about status, milestones, key obstacles and dependencies in order for them to make informed decisions? 6. For reporting on individual risks, how do you show the expected risk exposure over time, for a more active management of risk conversation? 7. What thought-provoking questions do you use to support your risk reporting? For example: • Are we doing enough to mitigate this risk? • Are we doing enough at the right pace? • How will we know if the actions have had the intended effect? • Who can help manage this cross-cutting risk? • What contingency arrangements do we have in place should this risk occur? 8. How do you convey the target risk exposure and explain what management is doing to get there?

Element	*Activity*	*Example Questions.*
Periodic Activities	Assuring risks from arm's length bodies	1. If necessary, for ALBs, how do you: • Identify which risks are cross-cutting and need a joined up response to mitigate them effectively? • Apply consistent criteria for identifying which risks should be made visible to the parent organisation? • Ensure a consistent set of risk management principles – not necessarily processes – are applied in both the ALB and the parent organisation? • Obtain routine and periodic risk assurance from ALBs to the parent organisation? • Make the parent organisation's top risks available to ALBs for context and visibility purposes?
Periodic Activities	Scanning the horizon and the environment, including National Risk Register risks	1. When will you next undertake an exercise with your board or senior executives to scan your environment, for technological, social, demographic, etc, developments? 2. What risks do they pose to the achievement of the organisation's objectives? 3. How do you categorise those risks in terms of when they are likely to impact the organisation (proximity)? 4. How do you ensure explicit inclusion of relevant National Risk Register risks in your organisation's management of risk?
Periodic Activities	Building risk maturity	1. What tried and tested framework would you use to assess your organisation's risk maturity? For example, HM Treasury Risk Management Assessment Framework or the Management of Risk maturity model?
Periodic Activities	Peer reviews	1. What opportunities exist to engender a culture of sharing ideas and learning from one another, through peer reviews with risk practitioners from other government bodies?

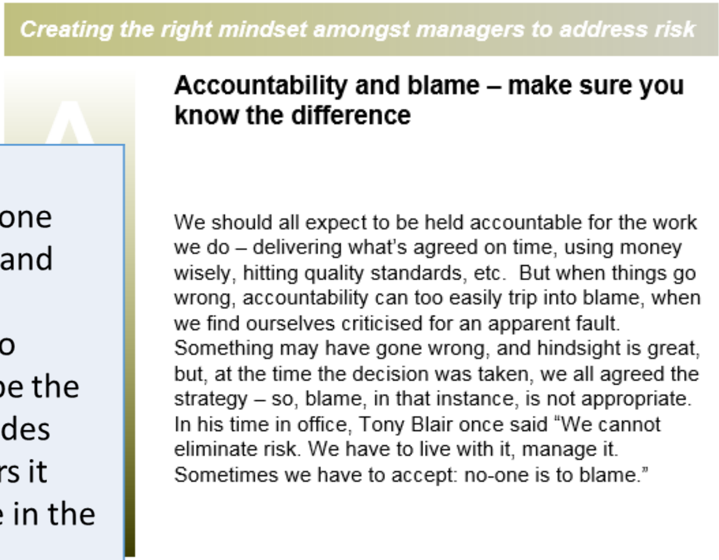
Element	*Activity*	*Example Questions.*
Periodic Activities	Learning lessons	1. How do you convene special sessions, for example when the organisation is commencing a major new project, to identify and learn relevant lessons from past experiences? 2. When a risk - including 'black swan' events - materialises and becomes an issue, how do you ensure your risk management arrangements learn the lessons from that experience?
Periodic Activities	Exploiting data and data analytics	1. How do you use your organisation's data sets and/or data analytics function to help identify new risks and refine assessments of known risks?

Annex C – Tools, techniques & templates

There is a wide variety of risk management practice across government bodies. This variety provides a clear opportunity for those government bodies to share what works for them and learn from one another. This Annex provides examples of some tools, techniques and templates that have been used successfully elsewhere. The examples shown here are not mandatory, they are simply provided to foster the sharing of good practice.

Creating positive risk management behaviours and culture

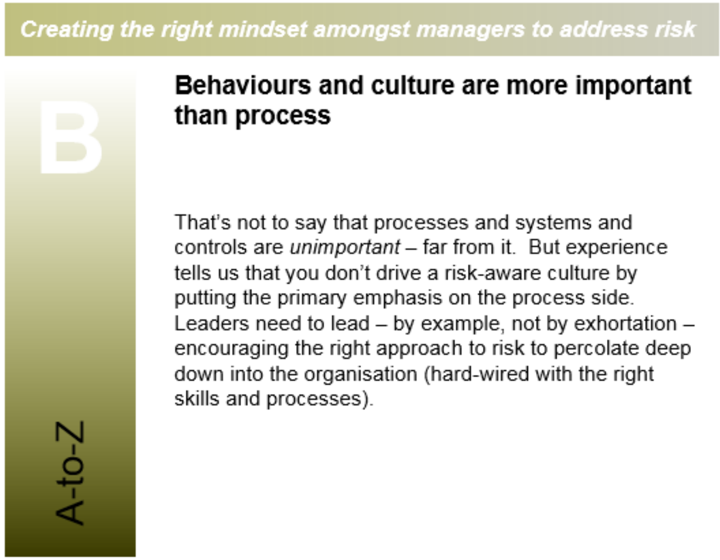
This helps because…	… it sets an appropriate 'tone from the top' and enables an organisation to clearly describe the positive attitudes and behaviours it expects to see in the effective management of risk
Used by	Various government bodies
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Building Blocks



Creating the right mindset amongst managers to address risk

Accountability and blame – make sure you know the difference

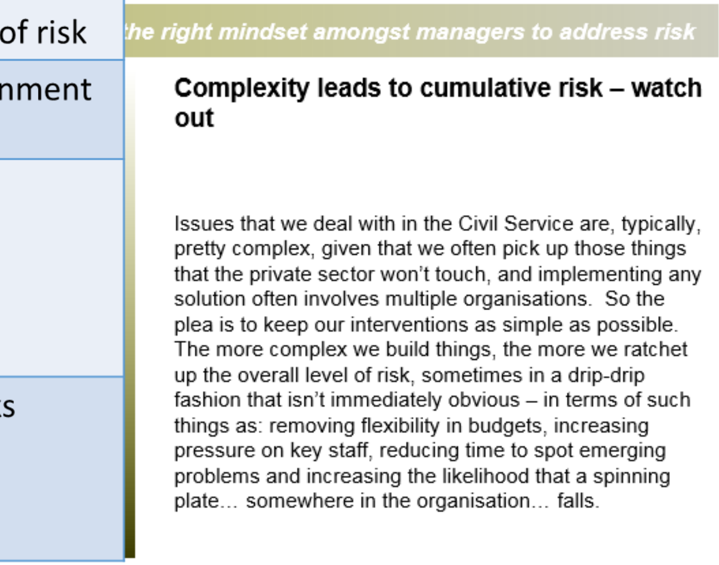
We should all expect to be held accountable for the work we do – delivering what's agreed on time, using money wisely, hitting quality standards, etc. But when things go wrong, accountability can too easily trip into blame, when we find ourselves criticised for an apparent fault. Something may have gone wrong, and hindsight is great, but, at the time the decision was taken, we all agreed the strategy – so, blame, in that instance, is not appropriate. In his time in office, Tony Blair once said "We cannot eliminate risk. We have to live with it, manage it. Sometimes we have to accept: no-one is to blame."



Creating the right mindset amongst managers to address risk

Behaviours and culture are more important than process

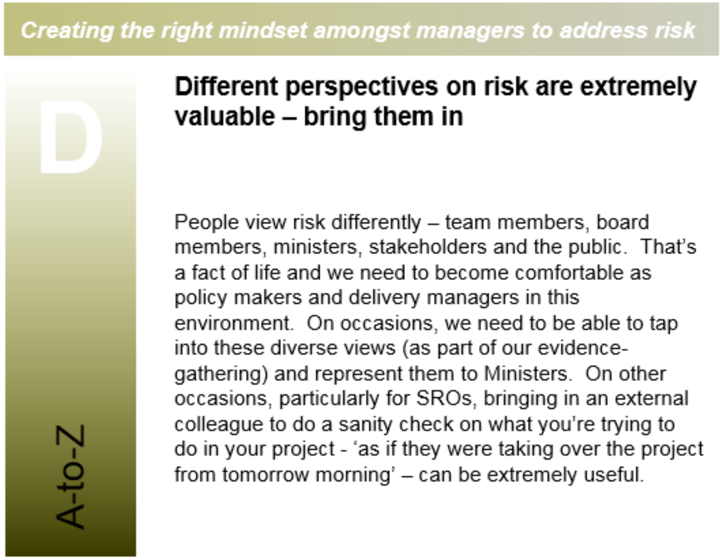
That's not to say that processes and systems and controls are *unimportant* – far from it. But experience tells us that you don't drive a risk-aware culture by putting the primary emphasis on the process side. Leaders need to lead – by example, not by exhortation – encouraging the right approach to risk to percolate deep down into the organisation (hard-wired with the right skills and processes).



the right mindset amongst managers to address risk

Complexity leads to cumulative risk – watch out

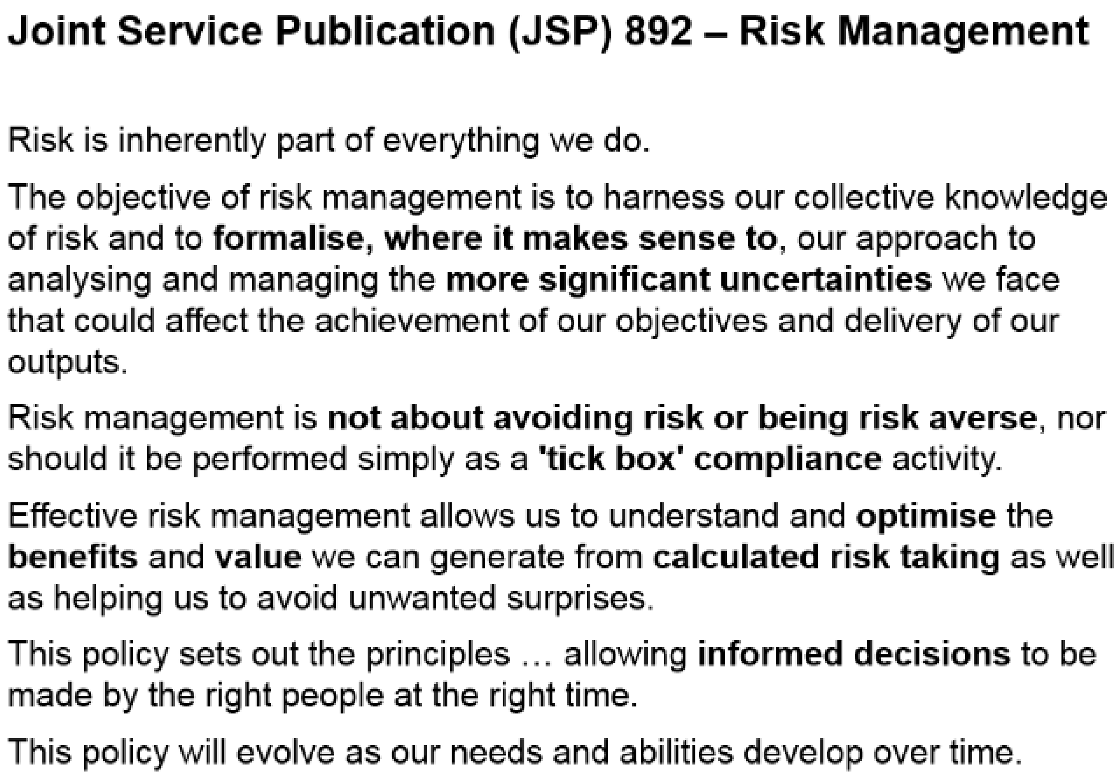
Issues that we deal with in the Civil Service are, typically, pretty complex, given that we often pick up those things that the private sector won't touch, and implementing any solution often involves multiple organisations. So the plea is to keep our interventions as simple as possible. The more complex we build things, the more we ratchet up the overall level of risk, sometimes in a drip-drip fashion that isn't immediately obvious – in terms of such things as: removing flexibility in budgets, increasing pressure on key staff, reducing time to spot emerging problems and increasing the likelihood that a spinning plate… somewhere in the organisation… falls.



Creating the right mindset amongst managers to address risk

Different perspectives on risk are extremely valuable – bring them in

People view risk differently – team members, board members, ministers, stakeholders and the public. That's a fact of life and we need to become comfortable as policy makers and delivery managers in this environment. On occasions, we need to be able to tap into these diverse views (as part of our evidence-gathering) and represent them to Ministers. On other occasions, particularly for SROs, bringing in an external colleague to do a sanity check on what you're trying to do in your project - 'as if they were taking over the project from tomorrow morning' – can be extremely useful.



Joint Service Publication (JSP) 892 – Risk Management

Risk is inherently part of everything we do.

The objective of risk management is to harness our collective knowledge of risk and to **formalise, where it makes sense to**, our approach to analysing and managing the **more significant uncertainties** we face that could affect the achievement of our objectives and delivery of our outputs.

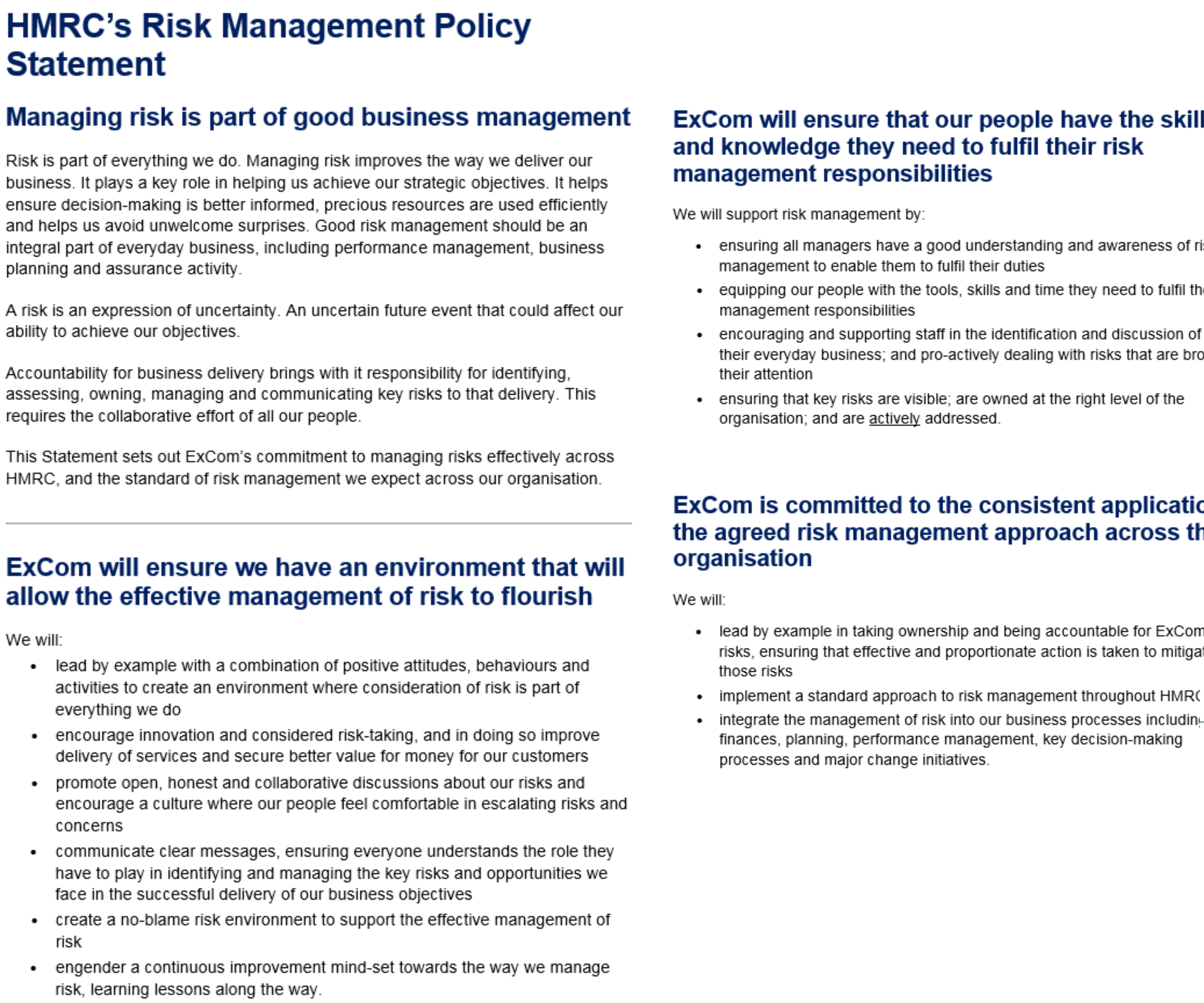
Risk management is **not about avoiding risk or being risk averse**, nor should it be performed simply as a **'tick box' compliance** activity.

Effective risk management allows us to understand and **optimise** the **benefits** and **value** we can generate from **calculated risk taking** as well as helping us to avoid unwanted surprises.

This policy sets out the principles … allowing **informed decisions** to be made by the right people at the right time.

This policy will evolve as our needs and abilities develop over time.

This helps because…	… it clearly and succinctly articulates the organisation's approach to, and expected value from, effective risk management. This, in turn, helps to manage stakeholder expectations.
Used by	MOD
Applies to the following types of risk	• Internal • External • Strategic • Major Project
Relates to the following element of risk management	Building blocks



HMRC's Risk Management Policy Statement

Managing risk is part of good business management

Risk is part of everything we do. Managing risk improves the way we deliver our business. It plays a key role in helping us achieve our strategic objectives. It helps ensure decision-making is better informed, precious resources are used efficiently and helps us avoid unwelcome surprises. Good risk management should be an integral part of everyday business, including performance management, business planning and assurance activity.

A risk is an expression of uncertainty. An uncertain future event that could affect our ability to achieve our objectives.

Accountability for business delivery brings with it responsibility for identifying, assessing, owning, managing and communicating key risks to that delivery. This requires the collaborative effort of all our people.

This Statement sets out ExCom's commitment to managing risks effectively across HMRC, and the standard of risk management we expect across our organisation.

ExCom will ensure we have an environment that will allow the effective management of risk to flourish

We will:

- lead by example with a combination of positive attitudes, behaviours and activities to create an environment where consideration of risk is part of everything we do
- encourage innovation and considered risk-taking, and in doing so improve delivery of services and secure better value for money for our customers
- promote open, honest and collaborative discussions about our risks and encourage a culture where our people feel comfortable in escalating risks and concerns
- communicate clear messages, ensuring everyone understands the role they have to play in identifying and managing the key risks and opportunities we face in the successful delivery of our business objectives
- create a no-blame risk environment to support the effective management of risk
- engender a continuous improvement mind-set towards the way we manage risk, learning lessons along the way.

ExCom will ensure that our people have the skills and knowledge they need to fulfil their risk management responsibilities

We will support risk management by:

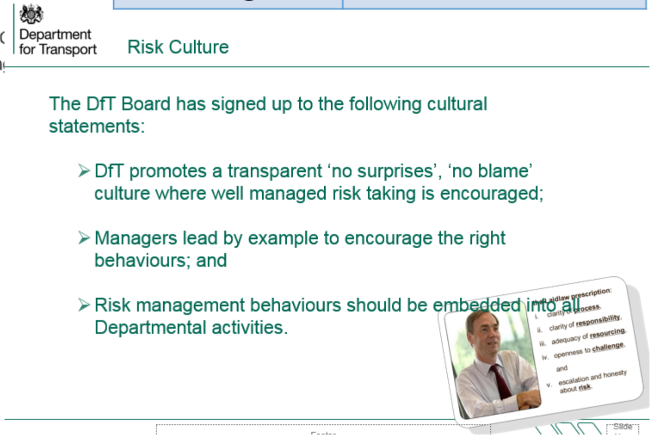
- ensuring all managers have a good understanding and awareness of risk management to enable them to fulfil their duties
- equipping our people with the tools, skills and time they need to fulfil their risk management responsibilities
- encouraging and supporting staff in the identification and discussion of risk in their everyday business; and pro-actively dealing with risks that are brought to their attention
- ensuring that key risks are visible; are owned at the right level of the organisation; and are actively addressed.

ExCom is committed to the consistent application of the agreed risk management approach across the organisation

We will:

- lead by example in taking ownership and being accountable for ExCom-level risks, ensuring that effective and proportionate action is taken to mitigate those risks
- implement a standard approach to risk management throughout HMR
- integrate the management of risk into our business processes includin finances, planning, performance management, key decision-making processes and major change initiatives.

This helps because…	… it demonstrates the explicit commitment to effective risk management from the top of the organisation to the rest of the organisation. This helps set the right tone and increases the likelihood that the management of risk will be given appropriate consideration
Used by	DfT & HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Building Blocks



Department for Transport

Risk Culture

The DfT Board has signed up to the following cultural statements:

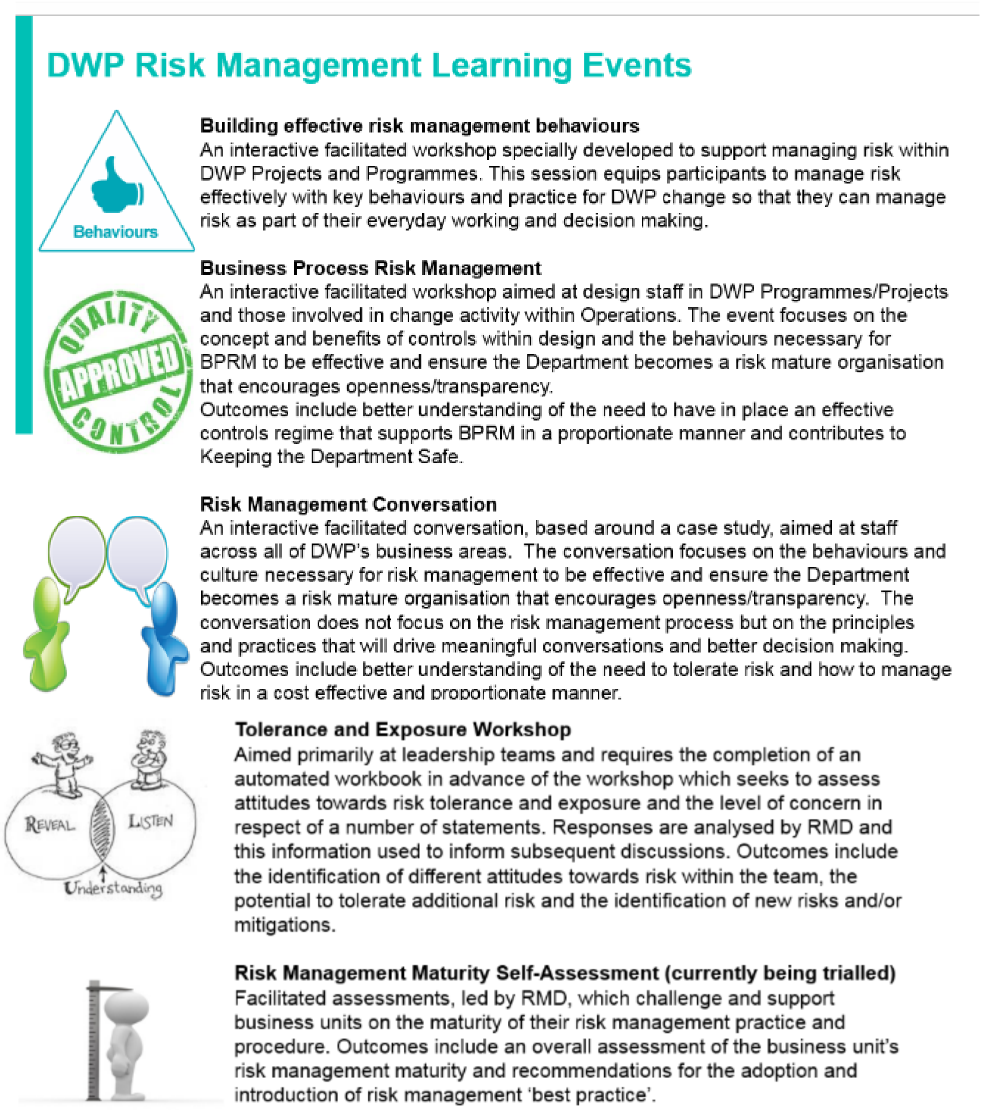
- DfT promotes a transparent 'no surprises', 'no blame' culture where well managed risk taking is encouraged;
- Managers lead by example to encourage the right behaviours; and
- Risk management behaviours should be embedded into all Departmental activities.

The Laidlaw prescription:

i. clarity of process,
ii. clarity of responsibility,
iii. adequacy of resourcing,
iv. openness to challenge, and
v. escalation and honesty about risk.

Building risk management capability

These help because…	… they use a workshop approach to build the capability and confidence of staff in managing risks more effectively. The different packages have been developed to serve different learning needs.
Used by	DWP
Applies to the following types of risk	• Internal • External • Strategic • Major Project
Relates to the following element of risk management	Building blocks


Behaviours
QUALITY APPROVED CONTROL
REVEAL
LISTEN
Understanding

DWP Risk Management Learning Events

Building effective risk management behaviours
An interactive facilitated workshop specially developed to support managing risk within DWP Projects and Programmes. This session equips participants to manage risk effectively with key behaviours and practice for DWP change so that they can manage risk as part of their everyday working and decision making.

Business Process Risk Management
An interactive facilitated workshop aimed at design staff in DWP Programmes/Projects and those involved in change activity within Operations. The event focuses on the concept and benefits of controls within design and the behaviours necessary for BPRM to be effective and ensure the Department becomes a risk mature organisation that encourages openness/transparency.
Outcomes include better understanding of the need to have in place an effective controls regime that supports BPRM in a proportionate manner and contributes to Keeping the Department Safe.

Risk Management Conversation
An interactive facilitated conversation, based around a case study, aimed at staff across all of DWP's business areas. The conversation focuses on the behaviours and culture necessary for risk management to be effective and ensure the Department becomes a risk mature organisation that encourages openness/transparency. The conversation does not focus on the risk management process but on the principles and practices that will drive meaningful conversations and better decision making.
Outcomes include better understanding of the need to tolerate risk and how to manage risk in a cost effective and proportionate manner.

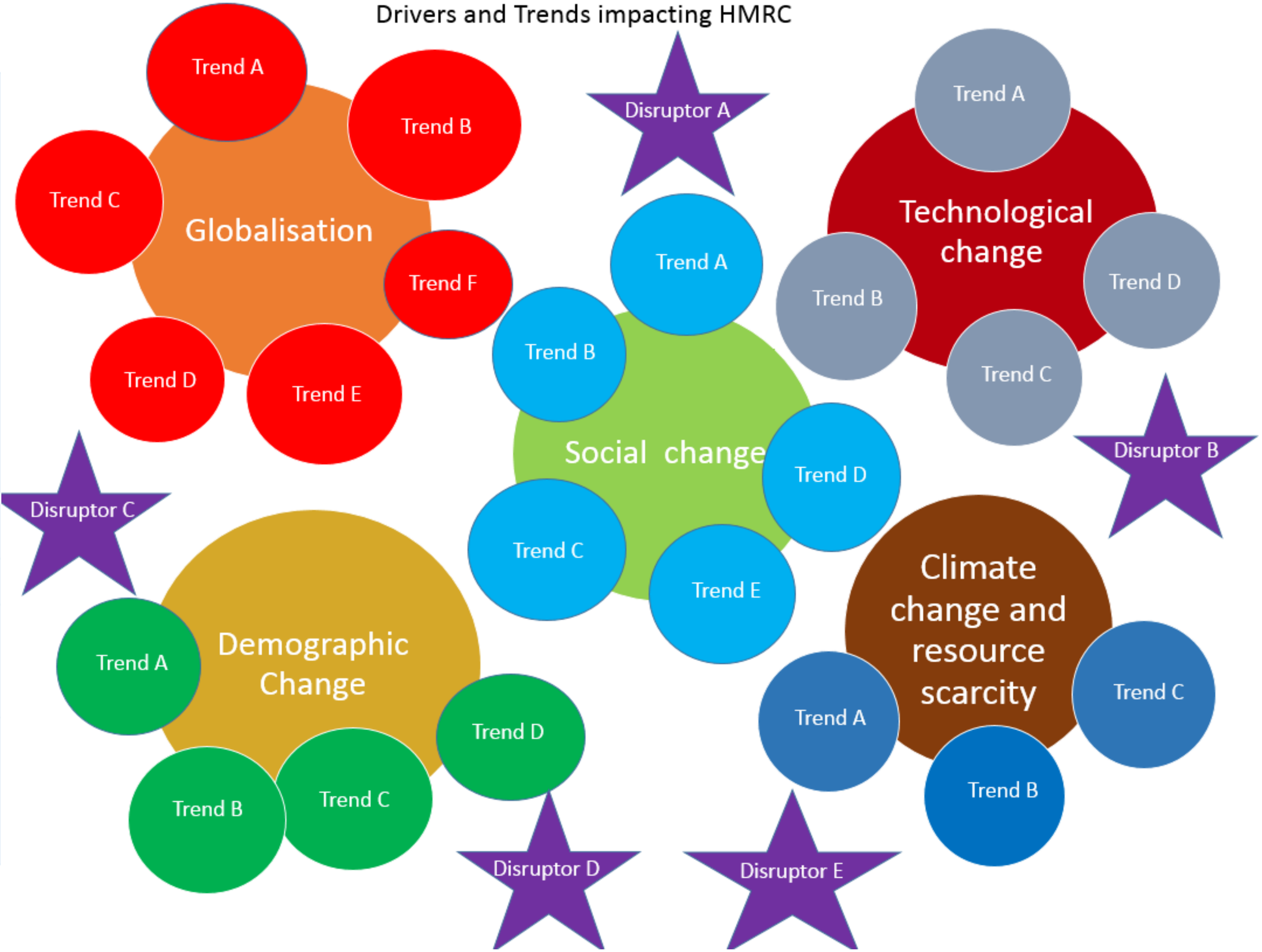
Tolerance and Exposure Workshop
Aimed primarily at leadership teams and requires the completion of an automated workbook in advance of the workshop which seeks to assess attitudes towards risk tolerance and exposure and the level of concern in respect of a number of statements. Responses are analysed by RMD and this information used to inform subsequent discussions. Outcomes include the identification of different attitudes towards risk within the team, the potential to tolerate additional risk and the identification of new risks and/or mitigations.

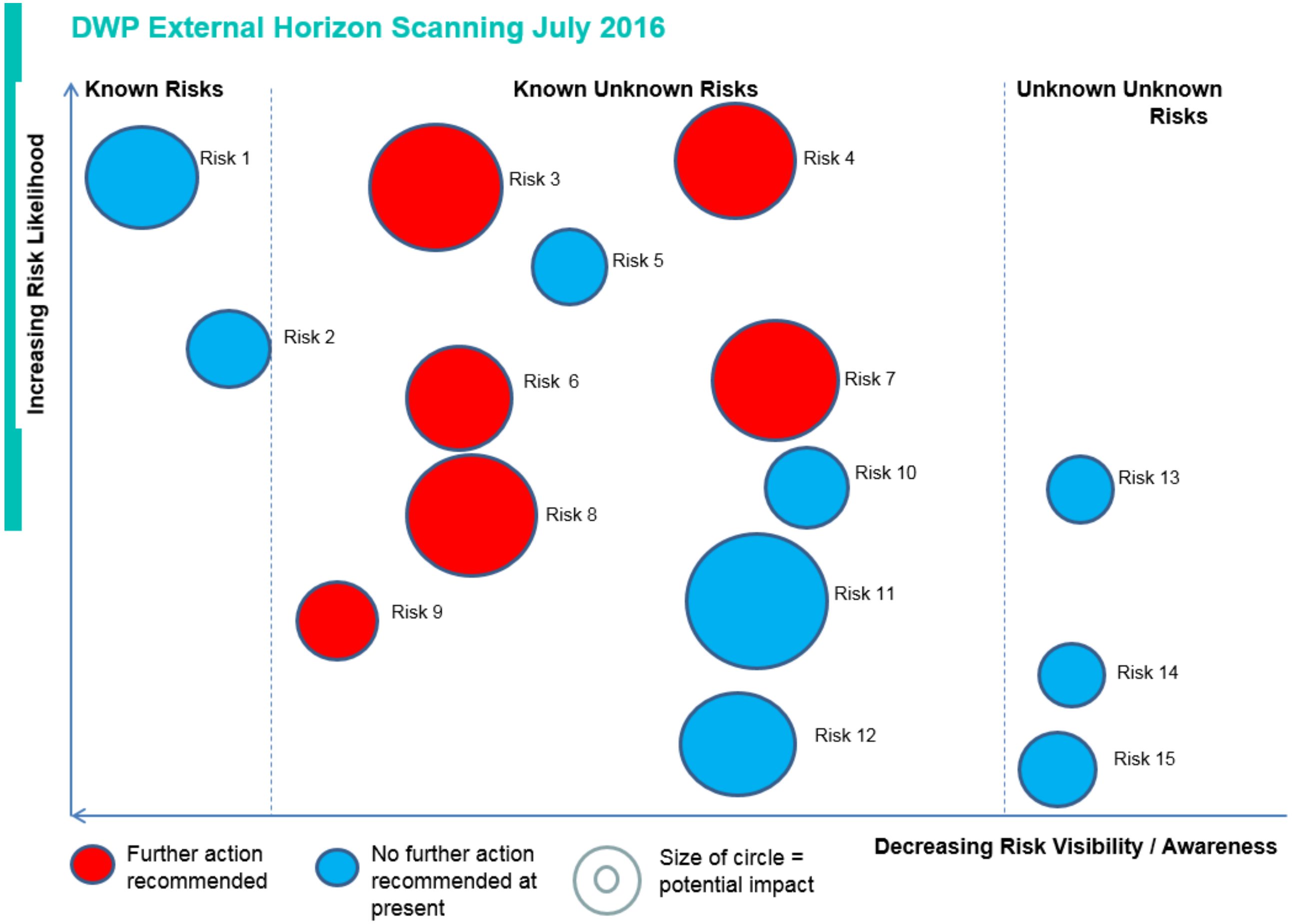
Risk Management Maturity Self-Assessment (currently being trialled)
Facilitated assessments, led by RMD, which challenge and support business units on the maturity of their risk management practice and procedure. Outcomes include an overall assessment of the business unit's risk management maturity and recommendations for the adoption and introduction of risk management 'best practice'.

Scanning the horizon

This helps because…	… it identifies key trends and drivers in the organisation's environment that present both opportunities for, and risks to, the achievement of the organisation's objectives. It can therefore support risk identification exercises and strategic planning
Used by	HMRC
Applies to the following types of risk	• External • Strategic
Relates to the following element of risk management	Periodic activities

Drivers and Trends impacting HMRC





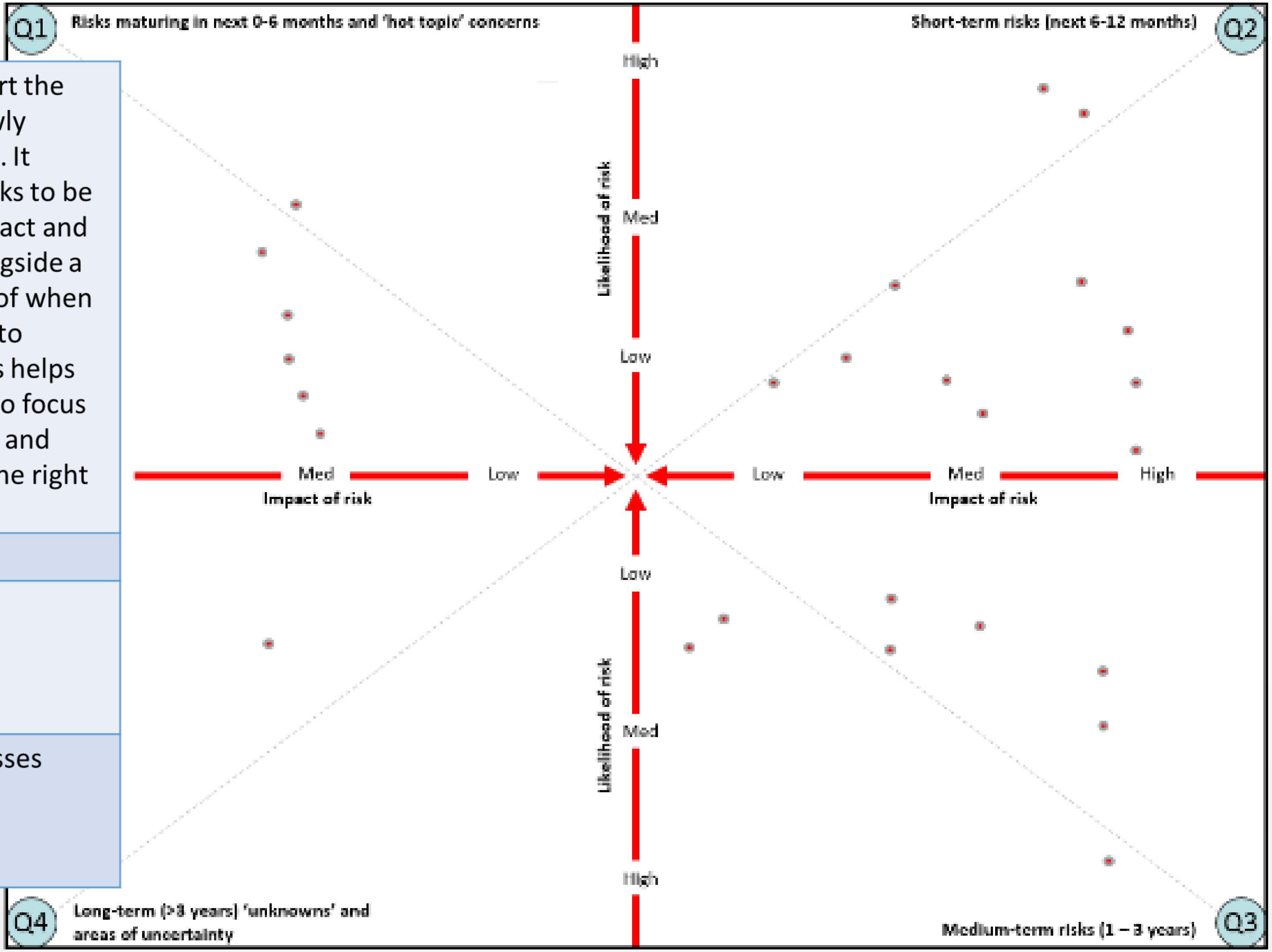
These help because…	… one shows risks identified through horizon scanning, their potential impact on the organisation and highlighting the risks where further action is recommended. The other shows, very simply, how horizon scanning information can inform decision-making by highlighting the possible consequences of those risks materialising
Used by	DWP & MOD
Applies to the following types of risk	• External • Strategic
Relates to the following element of risk management	Periodic activities

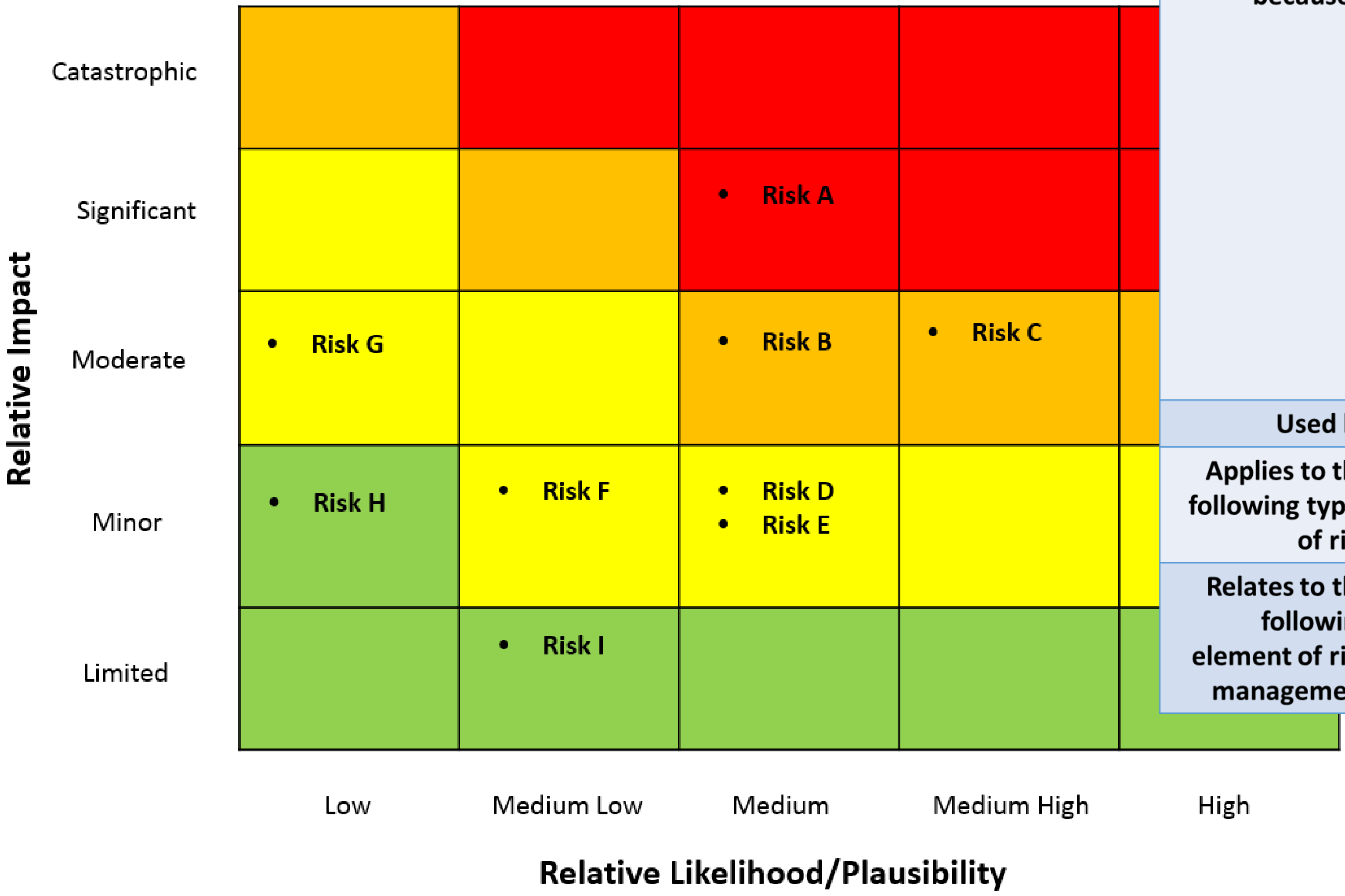
MOD Horizon Scanning

Event	Possible Consequences

Capturing risks

This helps because…	… it can support the capture of newly identified risks. It enables the risks to be plotted by impact and likelihood alongside a consideration of when they are likely to crystallise. This helps management to focus their attention and resources on the right risks.
Used by	Former BIS
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes


Q1
Risks maturing in next 0-6 months and 'hot topic' concerns
Short-term risks (next 6-12 months)
Q2
High
Med
Low
Likelihood of risk
Med
Low
Impact of risk
Low
Med
High
Impact of risk
Low
Med
High
Likelihood of risk
Q4
Long-term (>3 years) 'unknowns' and areas of uncertainty
Medium-term risks (1 – 3 years)
Q3

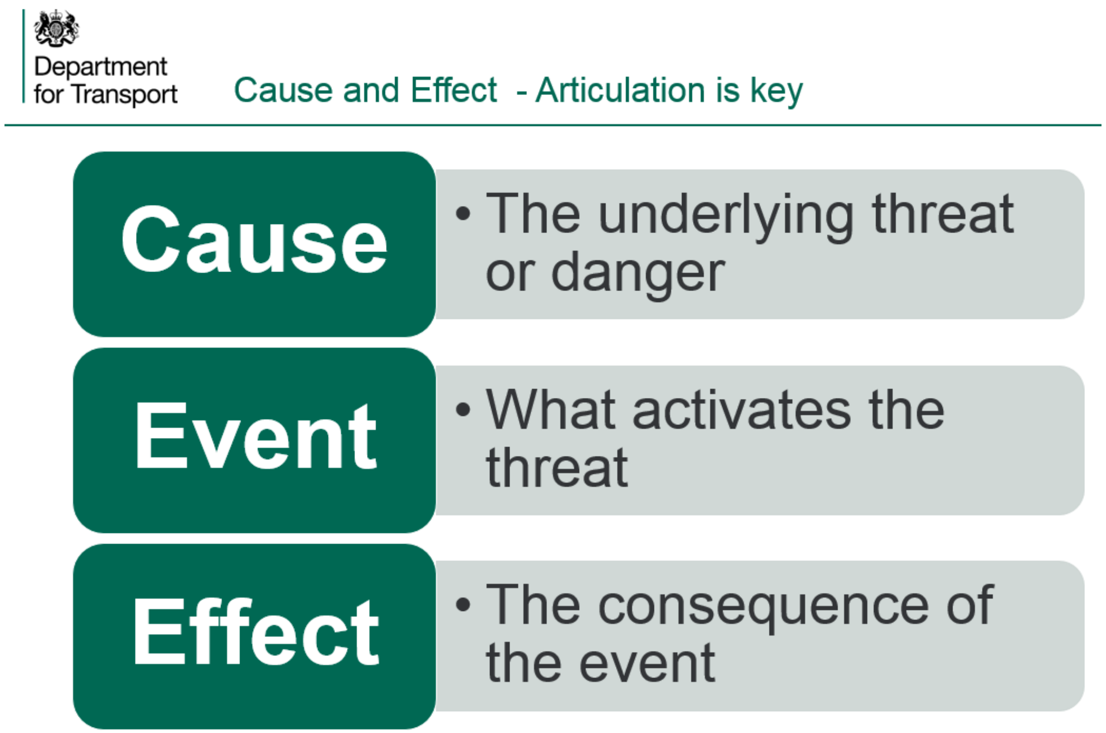


Relative Impact	Low	Medium Low	Medium	Medium High	High
Catastrophic					
Significant			• Risk A		
Moderate	• Risk G		• Risk B	• Risk C	
Minor	• Risk H	• Risk F	• Risk D • Risk E		
Limited		• Risk I			

Relative Likelihood/Plausibility

This helps because…	… it highlights National Risk Register risks considered particularly relevant to that organisation, along with their likelihood and impact. This supports risk identification exercises and can provide assurance over the completeness of those exercises
Used by	Defra
Applies to the following types of risk	External
Relates to the following element of risk management	Routine processes

Articulating risk



Department for Transport

Cause and Effect - Articulation is key

Cause
- The underlying threat or danger

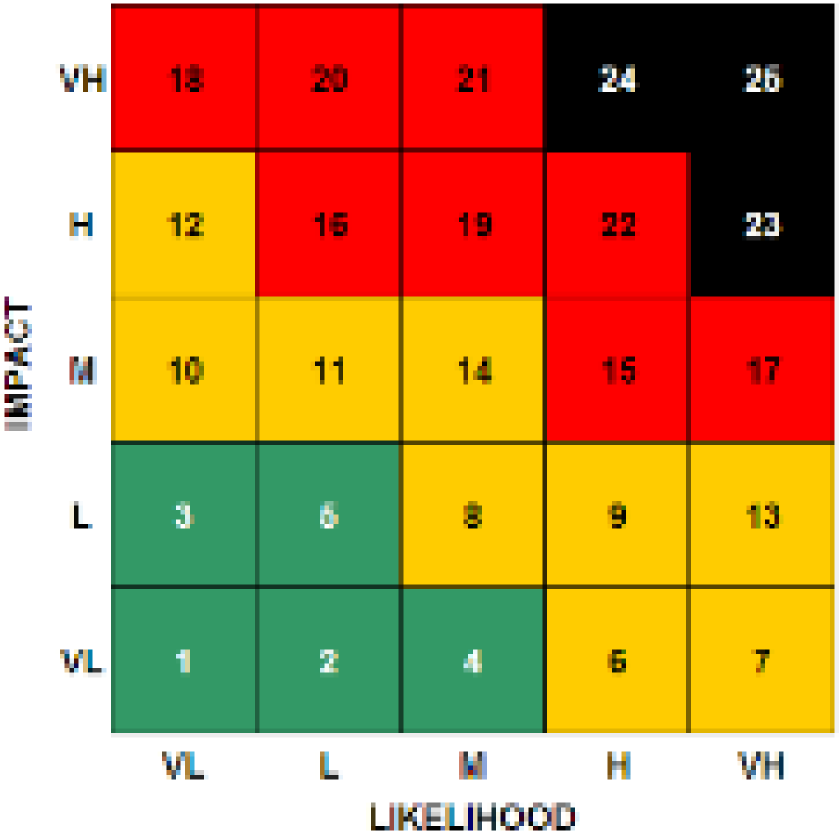
Event
- What activates the threat

Effect
- The consequence of the event

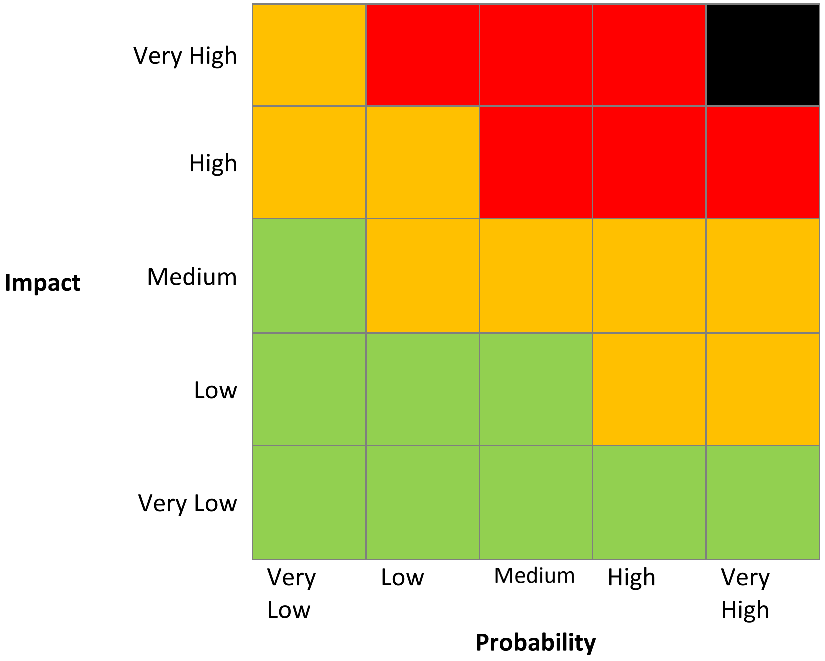
This helps because…	… it gives the risk a clear structure and enables stakeholders to understand the nature of the risk. If actions are required to mitigate the risk, this structure helps focus those actions on making the risk less likely and/or reducing the impact if it did.
Used by	DfT
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

Assessing risk

These help because…	… they provide examples of matrices used to plot risks in terms of likelihood and impact. This also helps management prioritise and focus their attention on the biggest risks.
Used by	DfT & HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes



IMPACT	VL	L	M	H	VH
VH	🟥 18	🟥 20	🟥 21	⬛ 24	⬛ 25
H	🟨 12	🟥 16	🟥 19	🟥 22	⬛ 23
M	🟨 10	🟨 11	🟨 14	🟥 15	🟥 17
L	🟩 3	🟩 5	🟨 8	🟨 9	🟨 13
VL	🟩 1	🟩 2	🟩 4	🟨 6	🟨 7



Impact	Very Low	Low	Medium	High	Very High
Very High	🟧	🟥	🟥	🟥	⬛
High	🟧	🟧	🟥	🟥	🟥
Medium	🟩	🟧	🟧	🟧	🟧
Low	🟩	🟩	🟩	🟧	🟧
Very Low	🟩	🟩	🟩	🟩	🟩

Likelihood Assessment Scores

Score	Very Likely (5)	Likely (4)	Possible (3)	Unlikely (2)	Very Unlikely (1)
Probability	75+%	50-74%	30-49%	5-29%	<5%

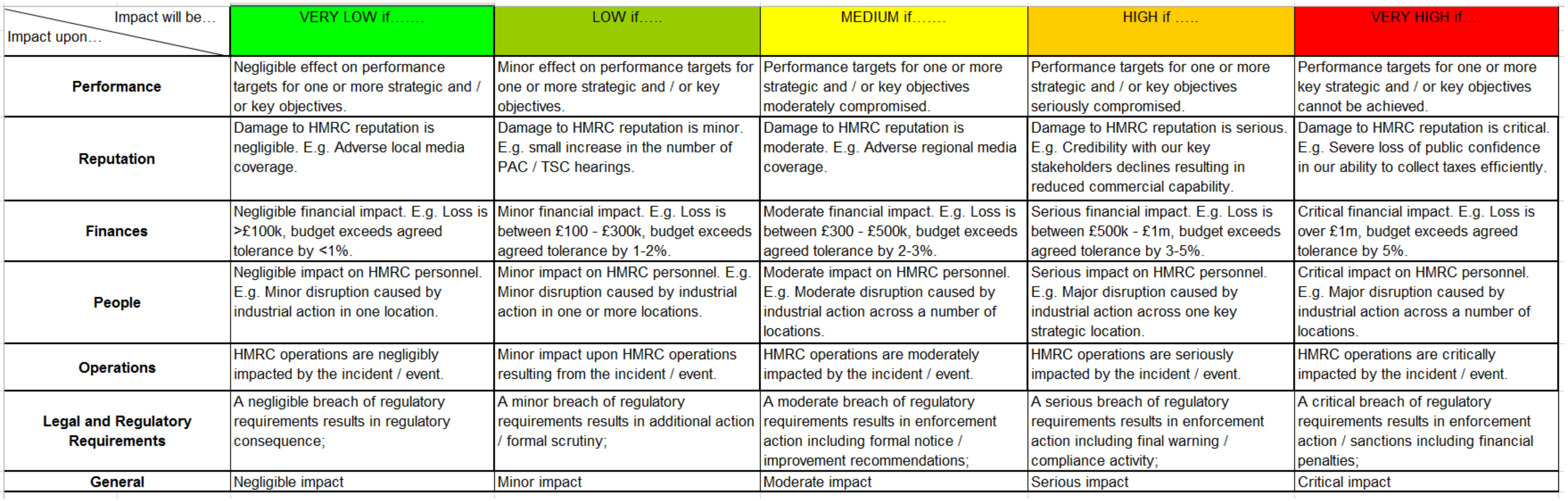
Impact Assessment Scores – where a risk has more than one impact the impact score is that of the highest scoring impact.

	Very High/Severe (5)	High/Major (4)	Medium/Moderate (3)	Low/Minor (2)	Very Low/Insignificant (1)
Transport Disruption	Serious (unwanted or unplanned) disruption to transport networks. One single national or London network element, ie: major airport/airline, major SRN route, main rail line, major container port, shut down 1+ days Multiple network elements in one local district shut down for 1+ days	One single national or London network element, ie: major airport/airline, major SRN route, main rail line, major container port, shut down for 3+ hours Multiple network elements in one local district shut down for 3+ hours	Minor unplanned disruption to national or London network.		
Service Delivery	Serious unplanned disruption to delivery of public service(s) A front line service suspended for 1+ days Failure to meet several key customer facing targets Loss of (or security breach to) 0.5% of customer data	Reasonably serious unplanned disruption to delivery of any public service(s) A front line service suspended for up to 1 day. Failure to meet a key customer facing target. Loss or breach of security in relation to <0.5% individual customer records	Any unplanned disruption to delivery of any public service Failure to meet any customer facing targets		
Project/Objective Delivery	A key departmental, Government, or customer-facing commitment will be delayed by greater than one year or never delivered A tier 1 strategic project will delayed by greater than one year or never delivered A customer facing KPI will be missed continuously over a period greater than one year Failure to deliver either domestic or European legislative requirement	A key initiative, a business plan commitment, a Government manifesto commitment or Prime Ministerial pledge or tier 1 project will be delayed by up to one year A customer facing KPI will be missed A tier 2 strategic project will be delayed by greater than one year or never delivered	A tier 1 project will be delayed by up to 2 months. A tier 2 project will be delayed by up to 1 year	An internal milestone will be delayed by greater than one year or never delivered An internal KPI will be missed continuously over a period greater than one year	Ar by
Financial	Financial impact of greater than £100 million Greater than 10% of Agency budget.	Financial impact of between £15-£100 million between 7% and 10% of Agency budget (in current spend review period)	Financial impact of between £5-£15 million between 5% and 7% of Agency budget (in current spend review period)	Financial impact of between £1-£5 million between 3% and 5% of Agency budget (in current spend review period)	les
Reputation	Sustained or widespread criticism of the Department, and / or the Secretary of State being pressed to make a statement to Parliament Sustained front page/headline national public criticism of transport policy or the Department lasting at least a week (not including targeted campaigns on specific issues). Events requiring significant time (e.g. more than 6 months) to restore relationships with other Departments or key stakeholders	Some national public or media criticism lasting at least a week (not including targeted campaigns on specific issues) Events requiring medium length of time (e.g. 4-6 months) to restore relationships with other Departments or key stakeholders	Widespread local/regional public and/or specialist criticism (not including targeted campaigns on specific issues) Events requiring at least some significant time (e.g. 3-4 months) to restore relationships with other Departments or key stakeholders	2-3 months to restore relationships with other Departments or key stakeholders	

This helps because…	… it allows the user to quantify both the likelihood and the impact of a risk. This in turn enables the user to plot the risk with some confidence on a risk matrix (see previous page).
Used by	DfT
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

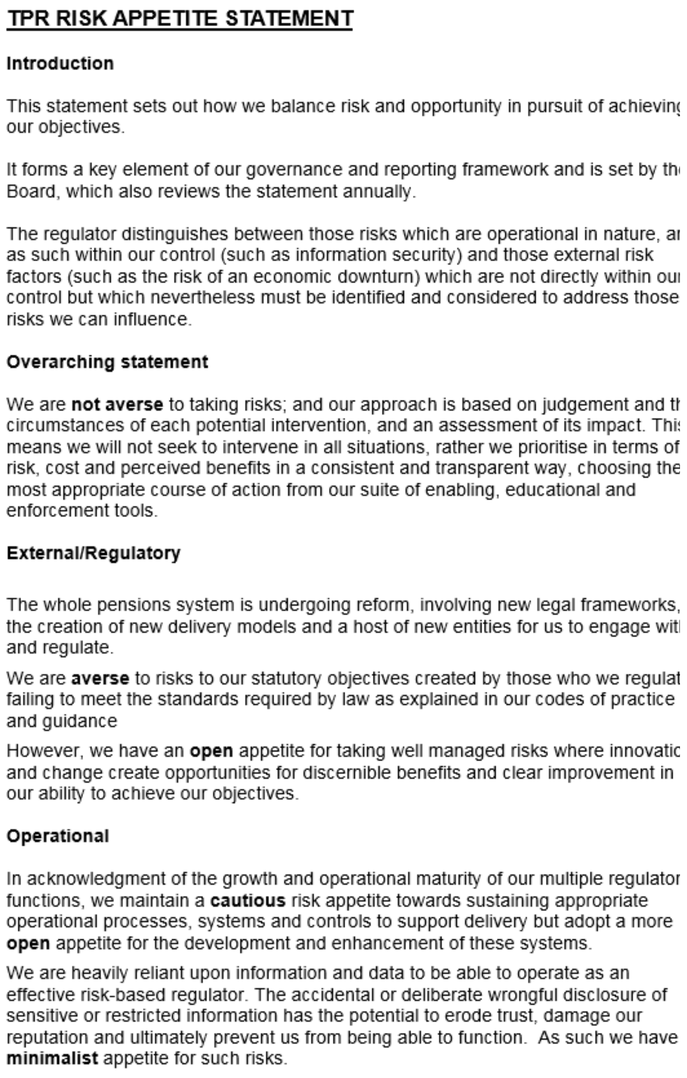
These help because…	… they, again, allow the user to quantify both the likelihood and the impact of a risk. This would be used in conjunction with a risk matrix.
Used by	HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

Probability	Percentage	Criteria
Very high	>80%	Almost certain to occur
High	60 – 80%	More likely to occur than not
Medium	40 – 60%	Fairly likely to occur
Low	20 – 40%	Unlikely but not unforeseeable
Very low	0 – 20%	Unlikely to occur



Impact will be… Impact upon…	VERY LOW if…….	LOW if…..	MEDIUM if…….	HIGH if …..	VERY HIGH if….
Performance	Negligible effect on performance targets for one or more strategic and / or key objectives.	Minor effect on performance targets for one or more strategic and / or key objectives.	Performance targets for one or more strategic and / or key objectives moderately compromised.	Performance targets for one or more strategic and / or key objectives seriously compromised.	Performance targets for one or more key strategic and / or key objectives cannot be achieved.
Reputation	Damage to HMRC reputation is negligible. E.g. Adverse local media coverage.	Damage to HMRC reputation is minor. E.g. small increase in the number of PAC / TSC hearings.	Damage to HMRC reputation is moderate. E.g. Adverse regional media coverage.	Damage to HMRC reputation is serious. E.g. Credibility with our key stakeholders declines resulting in reduced commercial capability.	Damage to HMRC reputation is critical. E.g. Severe loss of public confidence in our ability to collect taxes efficiently.
Finances	Negligible financial impact. E.g. Loss is >£100k, budget exceeds agreed tolerance by <1%.	Minor financial impact. E.g. Loss is between £100 - £300k, budget exceeds agreed tolerance by 1-2%.	Moderate financial impact. E.g. Loss is between £300 - £500k, budget exceeds agreed tolerance by 2-3%.	Serious financial impact. E.g. Loss is between £500k - £1m, budget exceeds agreed tolerance by 3-5%.	Critical financial impact. E.g. Loss is over £1m, budget exceeds agreed tolerance by 5%.
People	Negligible impact on HMRC personnel. E.g. Minor disruption caused by industrial action in one location.	Minor impact on HMRC personnel. E.g. Minor disruption caused by industrial action in one or more locations.	Moderate impact on HMRC personnel. E.g. Moderate disruption caused by industrial action across a number of locations.	Serious impact on HMRC personnel. E.g. Major disruption caused by industrial action across one key strategic location.	Critical impact on HMRC personnel. E.g. Major disruption caused by industrial action across a number of locations.
Operations	HMRC operations are negligibly impacted by the incident / event.	Minor impact upon HMRC operations resulting from the incident / event.	HMRC operations are moderately impacted by the incident / event.	HMRC operations are seriously impacted by the incident / event.	HMRC operations are critically impacted by the incident / event.
Legal and Regulatory Requirements	A negligible breach of regulatory requirements results in regulatory consequence;	A minor breach of regulatory requirements results in additional action / formal scrutiny;	A moderate breach of regulatory requirements results in enforcement action including formal notice / improvement recommendations;	A serious breach of regulatory requirements results in enforcement action including final warning / compliance activity;	A critical breach of regulatory requirements results in enforcement action / sanctions including financial penalties;
General	Negligible impact	Minor impact	Moderate impact	Serious impact	Critical impact

Establishing risk appetite



TPR RISK APPETITE STATEMENT

Introduction

This statement sets out how we balance risk and opportunity in pursuit of achievin our objectives.

It forms a key element of our governance and reporting framework and is set by th Board, which also reviews the statement annually.

The regulator distinguishes between those risks which are operational in nature, a as such within our control (such as information security) and those external risk factors (such as the risk of an economic downturn) which are not directly within ou control but which nevertheless must be identified and considered to address those risks we can influence.

Overarching statement

We are **not averse** to taking risks; and our approach is based on judgement and t circumstances of each potential intervention, and an assessment of its impact. Thi means we will not seek to intervene in all situations, rather we prioritise in terms of risk, cost and perceived benefits in a consistent and transparent way, choosing the most appropriate course of action from our suite of enabling, educational and enforcement tools.

External/Regulatory

The whole pensions system is undergoing reform, involving new legal frameworks, the creation of new delivery models and a host of new entities for us to engage wit and regulate.

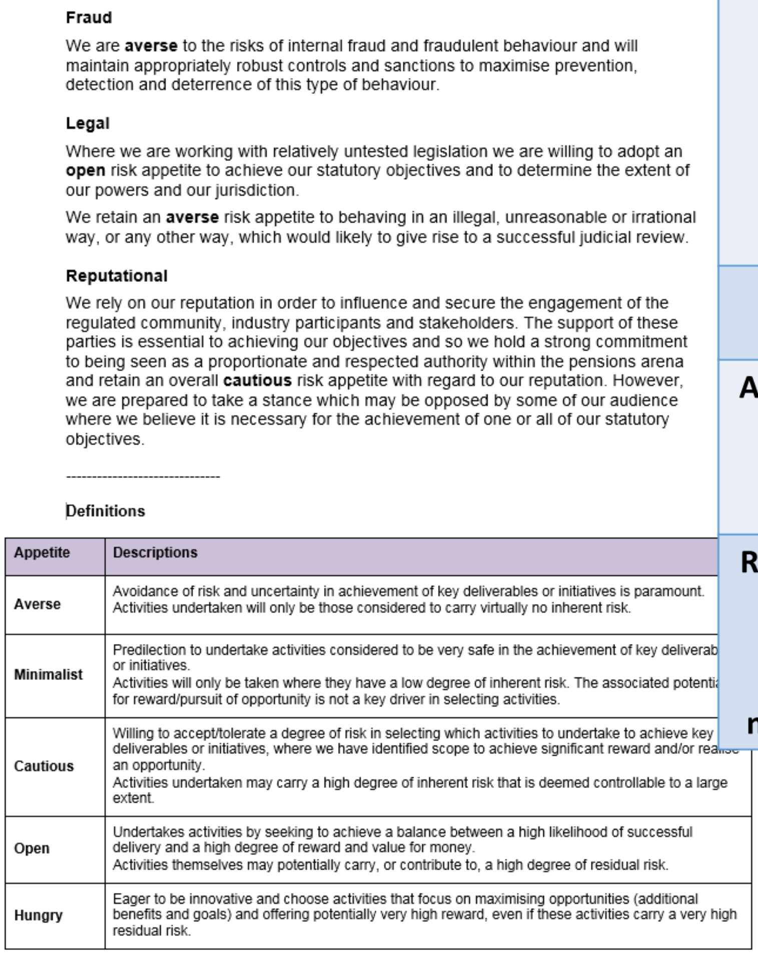
We are **averse** to risks to our statutory objectives created by those who we regula failing to meet the standards required by law as explained in our codes of practice and guidance

However, we have an **open** appetite for taking well managed risks where innovati and change create opportunities for discernible benefits and clear improvement in our ability to achieve our objectives.

Operational

In acknowledgment of the growth and operational maturity of our multiple regulato functions, we maintain a **cautious** risk appetite towards sustaining appropriate operational processes, systems and controls to support delivery but adopt a more **open** appetite for the development and enhancement of these systems.

We are heavily reliant upon information and data to be able to operate as an effective risk-based regulator. The accidental or deliberate wrongful disclosure of sensitive or restricted information has the potential to erode trust, damage our reputation and ultimately prevent us from being able to function. As such we have **minimalist** appetite for such risks.



Fraud

We are **averse** to the risks of internal fraud and fraudulent behaviour and will maintain appropriately robust controls and sanctions to maximise prevention, detection and deterrence of this type of behaviour.

Legal

Where we are working with relatively untested legislation we are willing to adopt an **open** risk appetite to achieve our statutory objectives and to determine the extent of our powers and our jurisdiction.

We retain an **averse** risk appetite to behaving in an illegal, unreasonable or irrational way, or any other way, which would likely to give rise to a successful judicial review.

Reputational

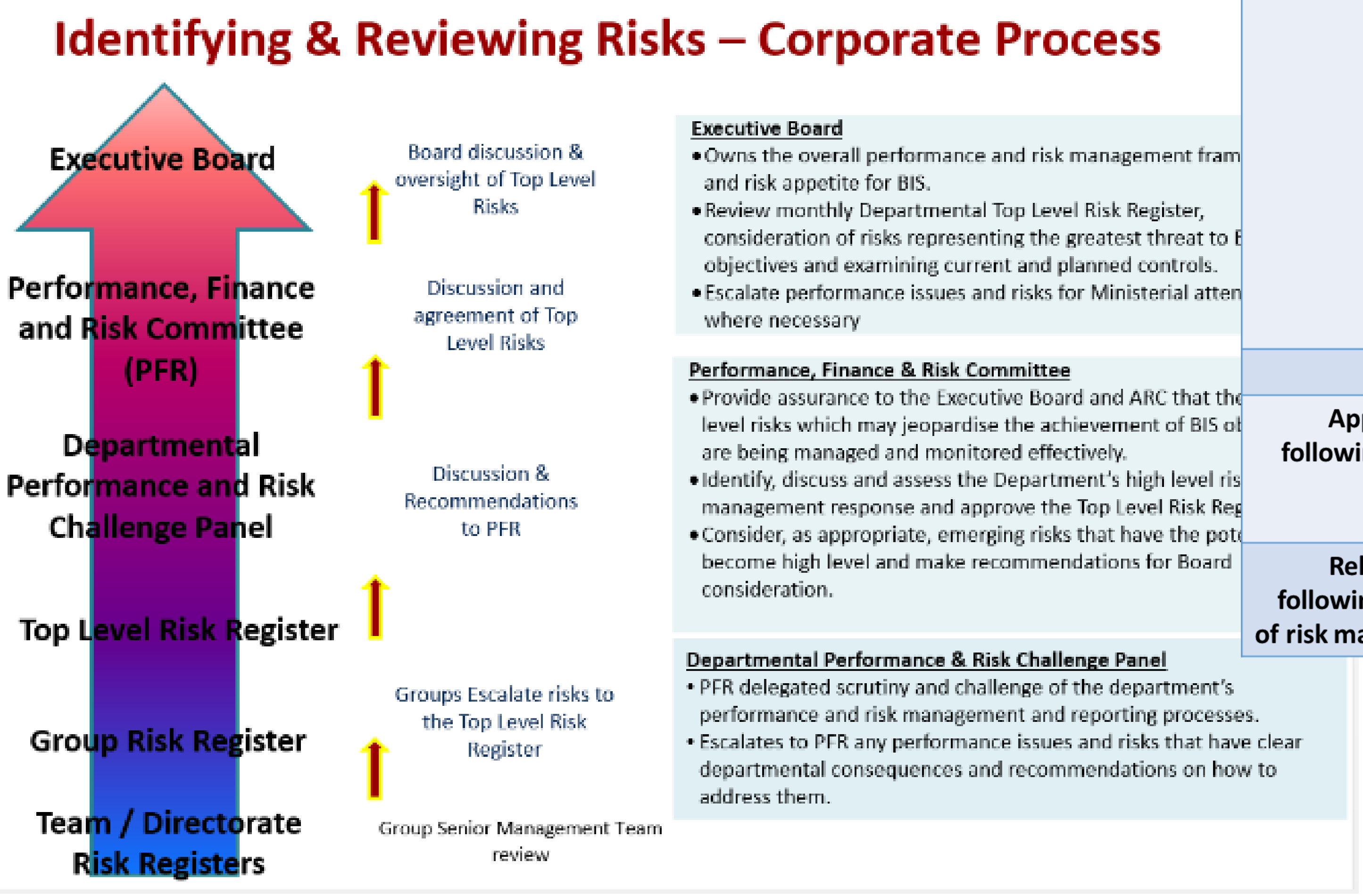
We rely on our reputation in order to influence and secure the engagement of the regulated community, industry participants and stakeholders. The support of these parties is essential to achieving our objectives and so we hold a strong commitment to being seen as a proportionate and respected authority within the pensions arena and retain an overall **cautious** risk appetite with regard to our reputation. However, we are prepared to take a stance which may be opposed by some of our audience where we believe it is necessary for the achievement of one or all of our statutory objectives.

Definitions

Appetite	Descriptions
Averse	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is paramount. Activities undertaken will only be those considered to carry virtually no inherent risk.
Minimalist	Predilection to undertake activities considered to be very safe in the achievement of key deliverab or initiatives. Activities will only be taken where they have a low degree of inherent risk. The associated potenti for reward/pursuit of opportunity is not a key driver in selecting activities.
Cautious	Willing to accept/tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant reward and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
Open	Undertakes activities by seeking to achieve a balance between a high likelihood of successful delivery and a high degree of reward and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.
Hungry	Eager to be innovative and choose activities that focus on maximising opportunities (additional benefits and goals) and offering potentially very high reward, even if these activities carry a very high residual risk.

This helps because…	… it defines and articulates the organisation's appetite for different types of risk. This in turn helps support management in making risk-based decisions
Used by	The Pensions Regulator
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

Reviewing risks



Identifying & Reviewing Risks – Corporate Process

Executive Board
Performance, Finance and Risk Committee (PFR)
Departmental Performance and Risk Challenge Panel
Top Level Risk Register
Group Risk Register
Team / Directorate Risk Registers
Board discussion & oversight of Top Level Risks
Discussion and agreement of Top Level Risks
Discussion & Recommendations to PFR
Groups Escalate risks to the Top Level Risk Register
Group Senior Management Team review

Executive Board

- Owns the overall performance and risk management fram and risk appetite for BIS.
- Review monthly Departmental Top Level Risk Register, consideration of risks representing the greatest threat to B objectives and examining current and planned controls.
- Escalate performance issues and risks for Ministerial atten where necessary

Performance, Finance & Risk Committee

- Provide assurance to the Executive Board and ARC that the level risks which may jeopardise the achievement of BIS ob are being managed and monitored effectively.
- Identify, discuss and assess the Department's high level ris management response and approve the Top Level Risk Reg
- Consider, as appropriate, emerging risks that have the pote become high level and make recommendations for Board consideration.

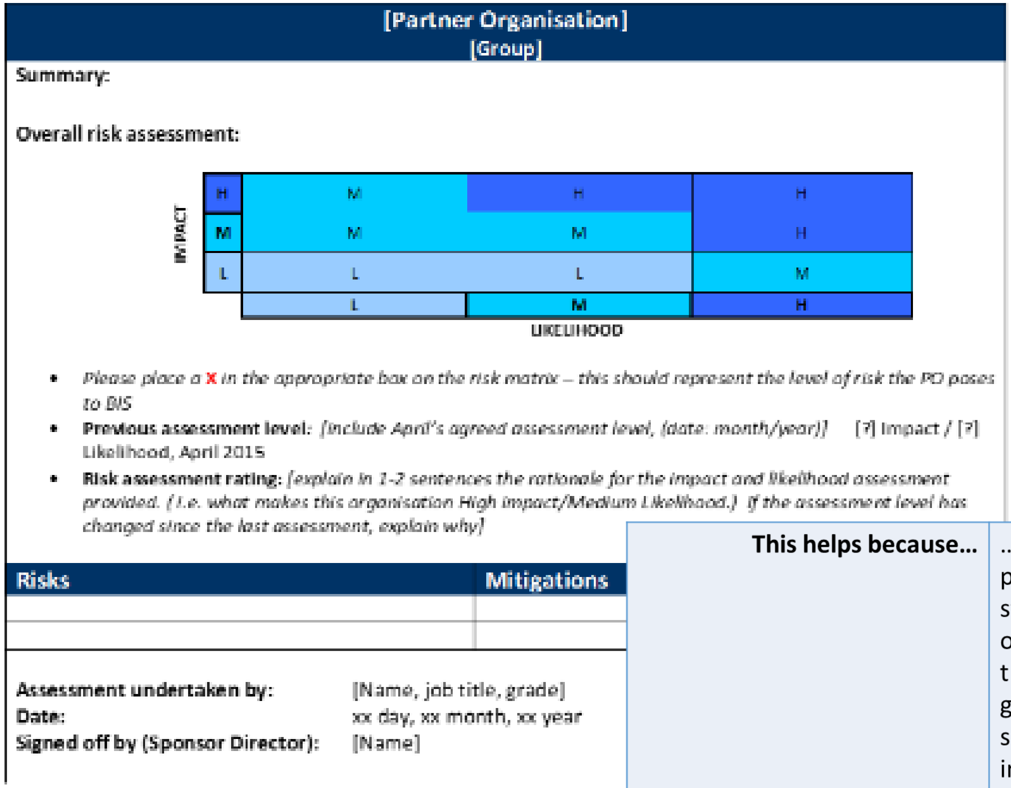
Departmental Performance & Risk Challenge Panel

- PFR delegated scrutiny and challenge of the department's performance and risk management and reporting processes.
- Escalates to PFR any performance issues and risks that have clear departmental consequences and recommendations on how to address them.

This helps because…	… it shows how risk information can flow upwards through an organisation. It also shows how that risk information is reviewed and challenged along the way. This helps support oversight of the way risks are being managed and helps ensure the risk information is robust by the time it gets to the top of the organisation.
Used by	Former BIS
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

Partner Organisation Risk Assessments

- Partner Organisation Sponsor Teams provide a Assurance Assessment on a quarterly basis
- If significant risks or issues arise in the interim period Sponsor Teams will submit a by-exception Assurance Assessment.
- Once a year in April these are produced jointly be the sponsor team and Partner Organisation.
- This includes comment on the state of relationship between the Department and Partner Organisation and agreement on the top risks.



[Partner Organisation]
[Group]

Summary:

Overall risk assessment:

IMPACT			
H	M	H	H
M	M	M	H
L	L	L	M
	L	M	H
	LIKELIHOOD		

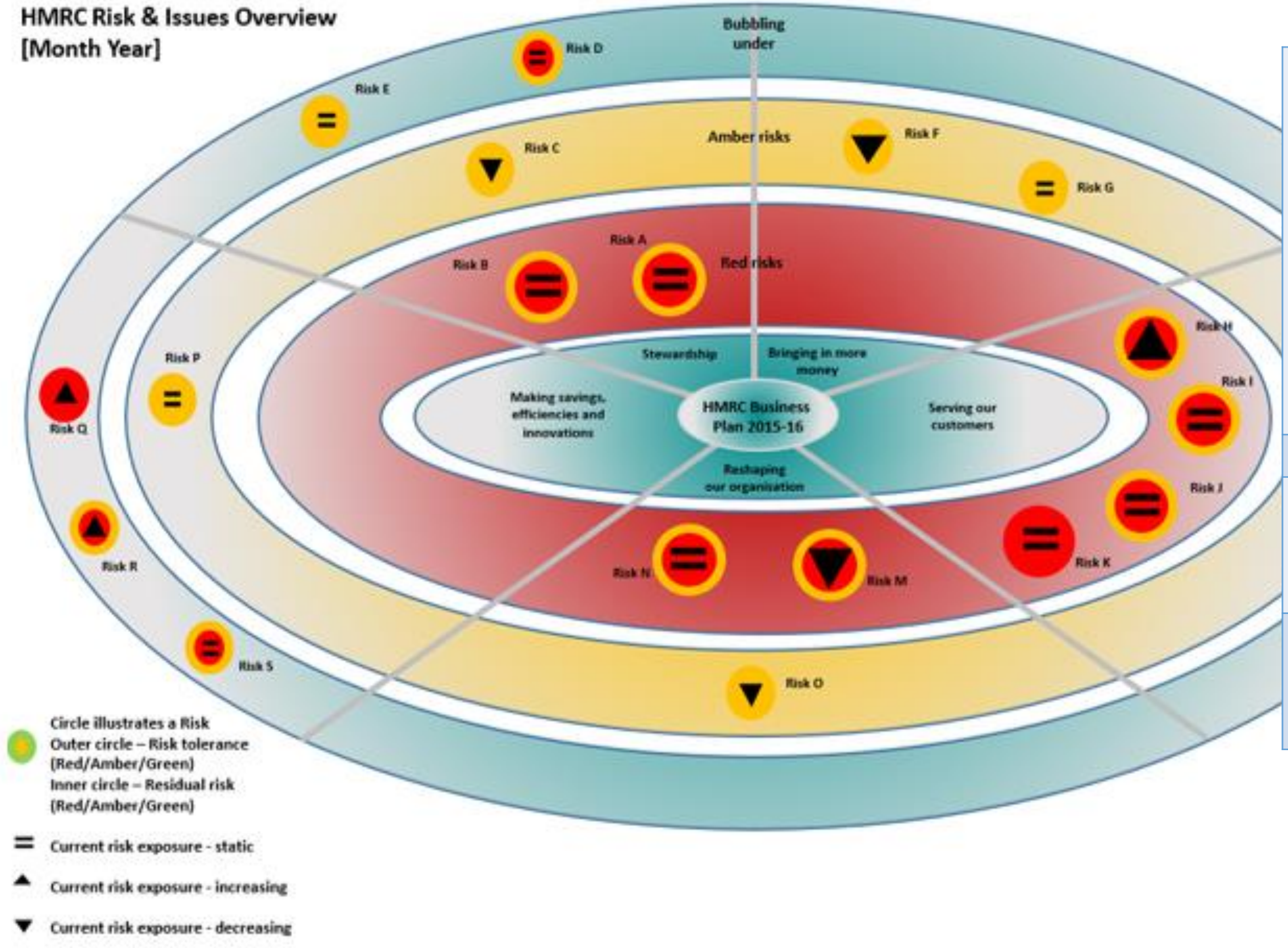
- *Please place a* **X** *in the appropriate box on the risk matrix – this should represent the level of risk the PO poses to BIS*
- **Previous assessment level:** *[include April's agreed assessment level, (date: month/year)]* [?] Impact / [?] Likelihood, April 2015
- **Risk assessment rating:** *[explain in 1-2 sentences the rationale for the impact and likelihood assessment provided. (i.e. what makes this organisation High impact/Medium Likelihood.) If the assessment level has changed since the last assessment, explain why]*

Risks	Mitigations

Assessment undertaken by: [Name, job title, grade]
Date: xx day, xx month, xx year
Signed off by (Sponsor Director): [Name]

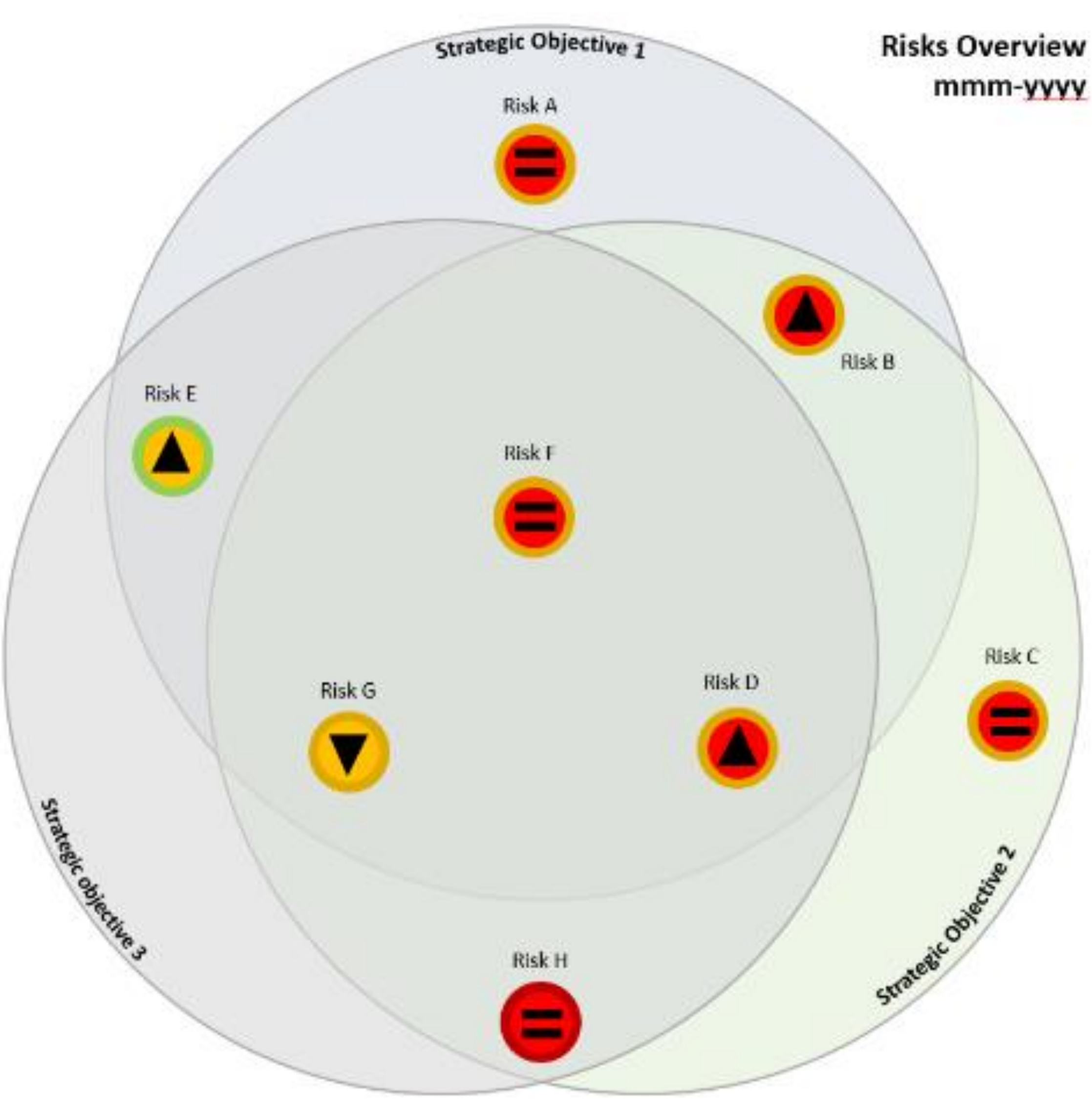
This helps because…	… it enables an organisation to periodically obtain information, in a structured form, from partner organisations on their top risks and how they are being managed. This in turn gives the organisation assurance over any shared dependencies / interdependencies.
Used by	Former BIS
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

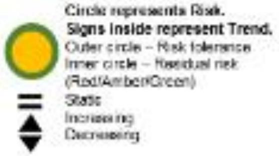
Reporting on risks - in summary

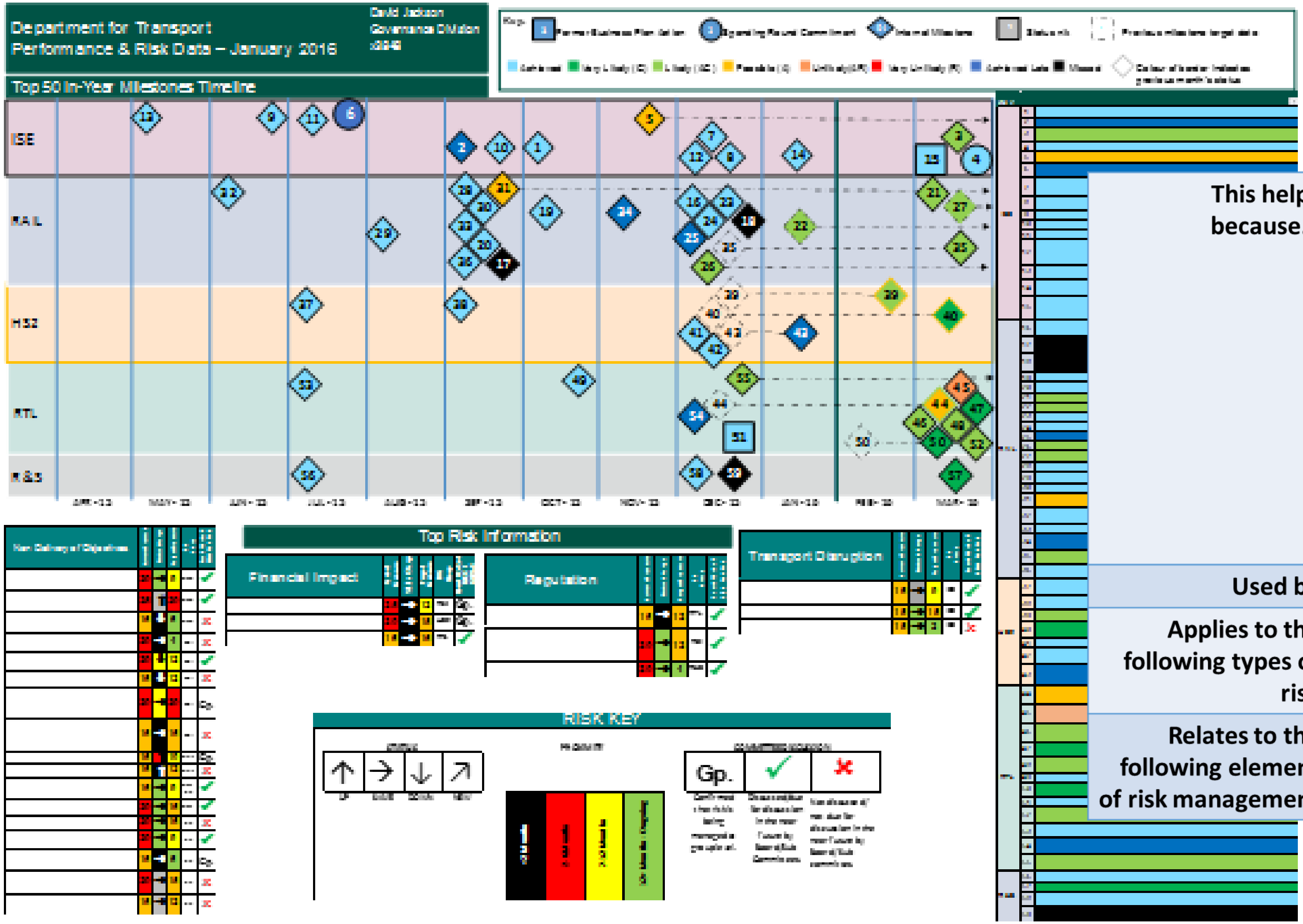

HMRC Risk & Issues Overview
[Month Year]
Bubbling under
Risk D
Risk E
Amber risks
Risk F
Risk C
Risk G
Risk A
Risk B
Red risks
Risk H
Risk I
Risk P
Risk Q
Stewardship
Bringing in more money
Making savings, efficiencies and innovations
HMRC Business Plan 2015-16
Serving our customers
Reshaping our organisation
Risk J
Risk K
Risk N
Risk M
Risk R
Risk S
Risk O
Circle illustrates a Risk
Outer circle – Risk tolerance (Red/Amber/Green)
Inner circle – Residual risk (Red/Amber/Green)
= Current risk exposure - static
▲ Current risk exposure - increasing
▼ Current risk exposure - decreasing

This helps because…	… it shows a summary level of detail for a number of risks in a very visual way. It links those risks clearly to business priorities, which helps management understand which of those priorities is most at risk. Management can then prioritise their attention on the right risks.
Used by	HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

This helps because…	… it shows a summary level of detail for a number of risks. This Venn diagram approach is useful if the risks relate to the achievement of more than one strategic objective/business priority. This, in turn, helps management prioritise their attention on the right risks.
Used by	HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes




Circle represents Risk.
Signs inside represent Trend.
Outer circle – Risk tolerance
Inner circle – Residual risk
(Red/Amber/Green)
Static
Increasing
Decreasing



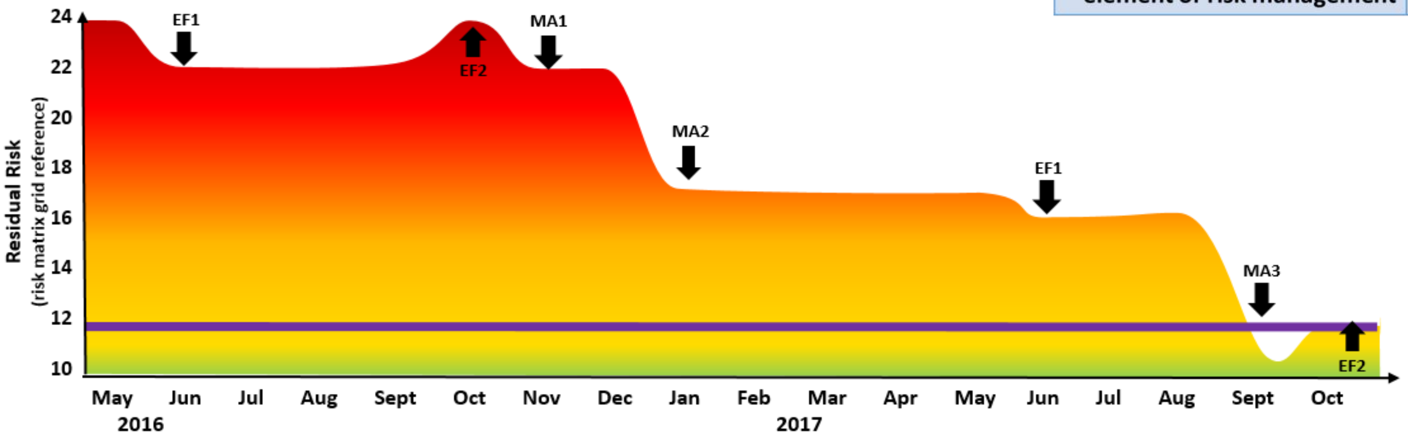
This helps because…	… it shows, in summary form, the top risks associated with programme delivery. This helps management focus on the right areas by breaking down elements such as progress against milestones, delivery of objectives, alongside financial and reputational impacts.
Used by	DfT
Applies to the following types of risk	Project
Relates to the following element of risk management	Routine processes

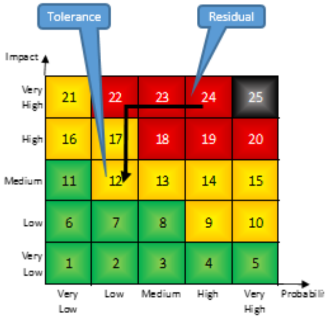
Managing and reporting on risk - specific risks

This helps because…	… it provides a visual representation of risk exposure over time. This supports active management of the risk by helping decision-makers understand whether planned actions will be sufficient to bring the risk within tolerance and by when.
Used by	Various Government bodies
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

Risk flightpath

There is a risk that [...]
Risk sponsor: A N Other





Graph key:
MA – Management Actions
EF - External Factors /potential for negative publicity
▬ - Risk Tolerance

Key Management Actions

MA1: [Action designed to reduce the probability of the risk occurring.] [Action owner]

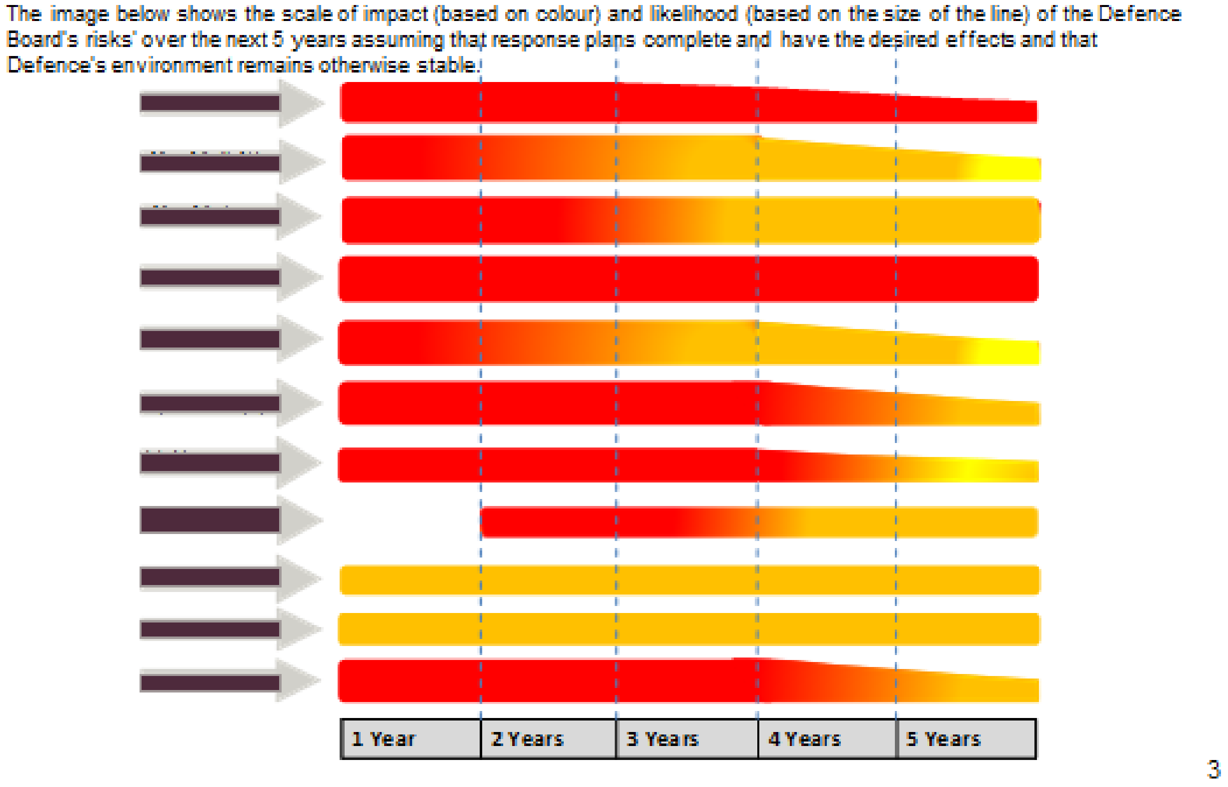
MA2: [Action designed to reduce the impact of the risk occurring.] [Action owner]

MA3: [Action designed to reduce the probability and impact of the risk occurring.] [Action owner]

Key External Factors

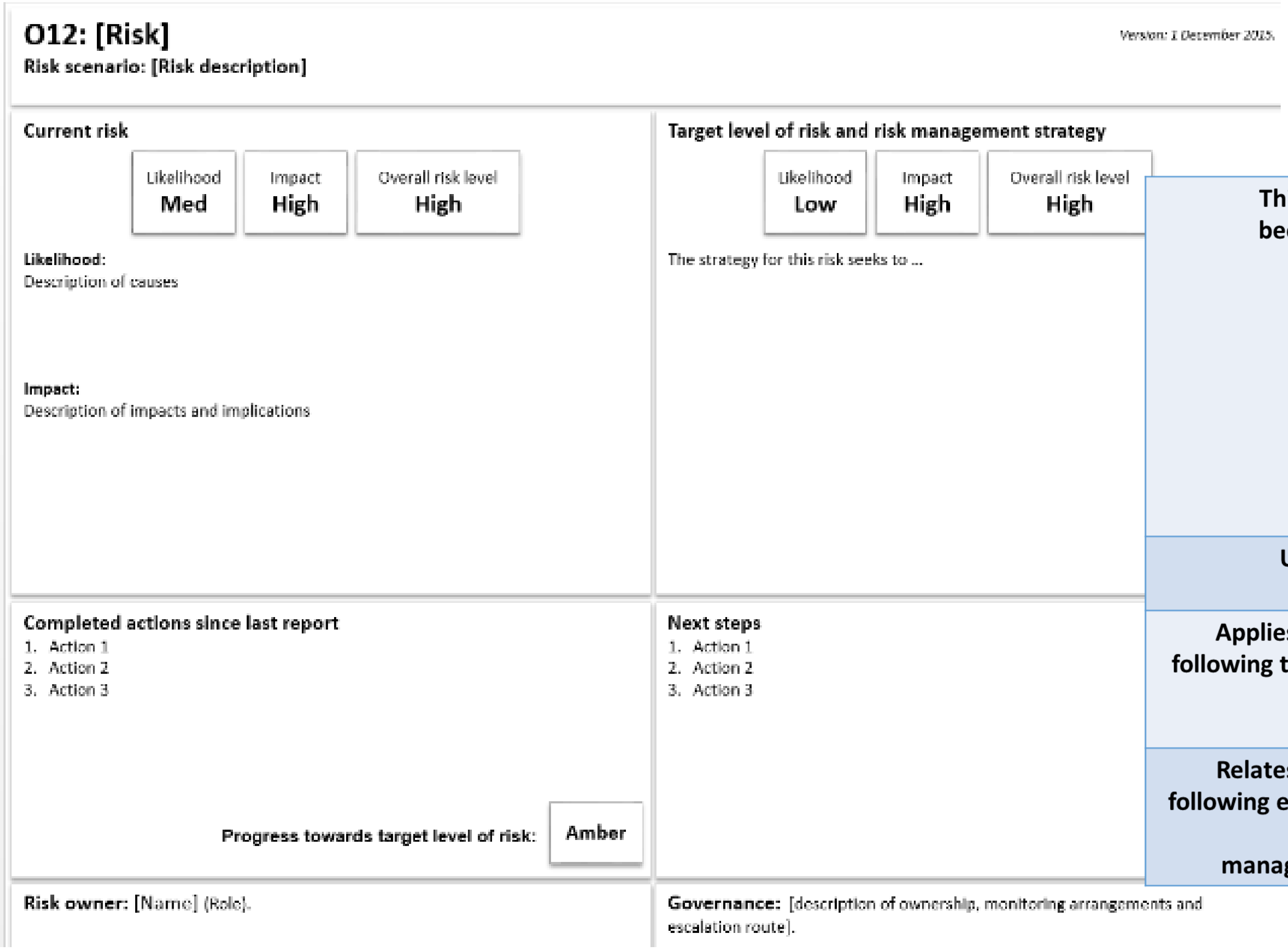
EF1: [Factor outside of management's control]

EF2: [Factor outside of management's control]



The image below shows the scale of impact (based on colour) and likelihood (based on the size of the line) of the Defence Board's risks' over the next 5 years assuming that response plans complete and have the desired effects and that Defence's environment remains otherwise stable.

This helps because…	… it shows how the scale of impact or the likelihood of the risk changes over time. This, in turn, helps to challenge horizon scanning assumptions and inform balance of investment decisions
Used by	MOD
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes



O12: [Risk]

Version: 1 December 2015.

Risk scenario: [Risk description]

Current risk

Likelihood	Impact	Overall risk level
Med	High	High

Likelihood:
Description of causes

Impact:
Description of impacts and implications

Target level of risk and risk management strategy

Likelihood	Impact	Overall risk level
Low	High	High

The strategy for this risk seeks to ...

Completed actions since last report

1. Action 1
2. Action 2
3. Action 3

Progress towards target level of risk: Amber

Next steps

1. Action 1
2. Action 2
3. Action 3

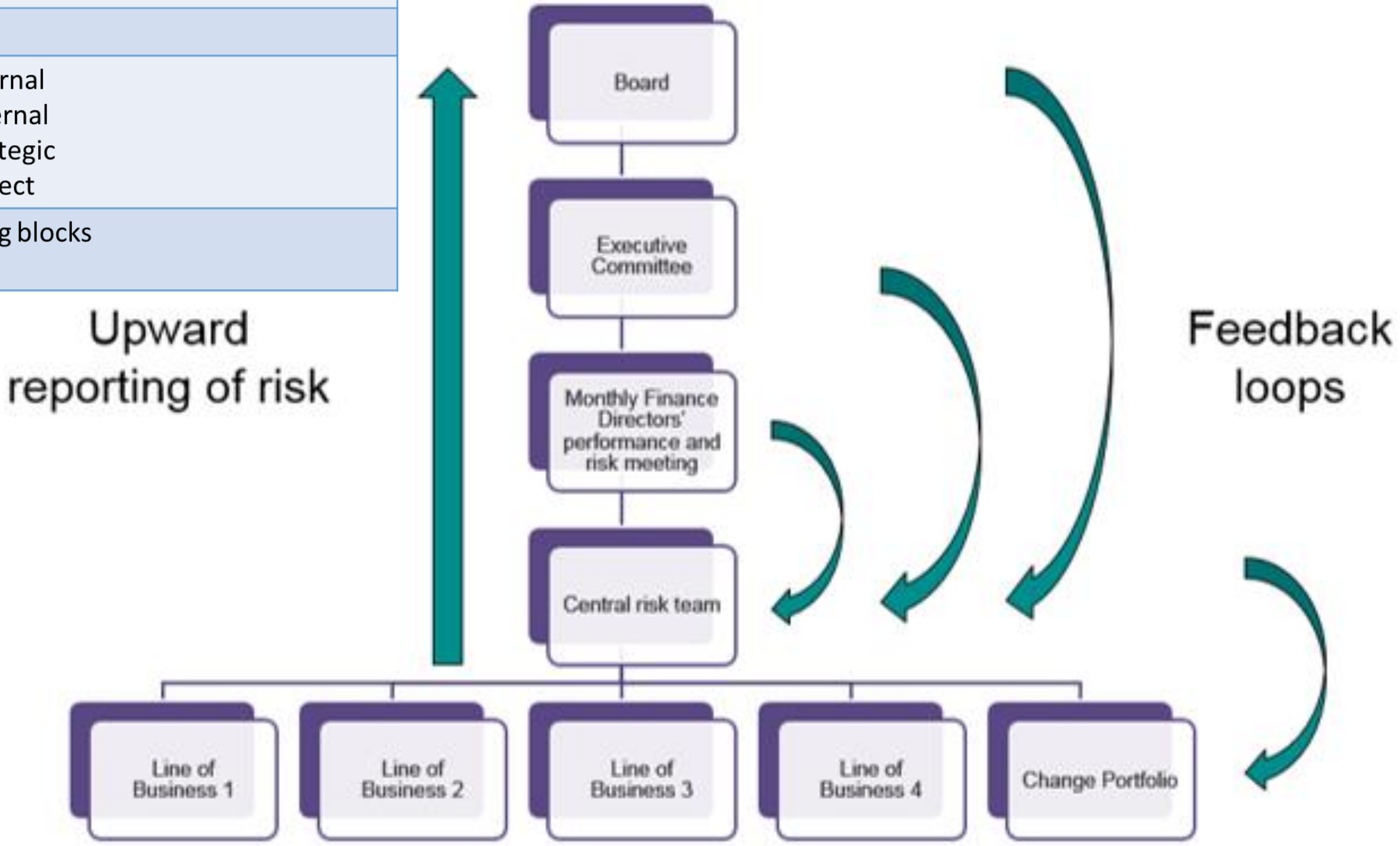
Risk owner: [Name] (Role).

Governance: [description of ownership, monitoring arrangements and escalation route].

This helps because…	… it provides in written form, on one page, what management needs to know about a specific risk. This helps decision-makers by summarising the nature of the risk, the current exposure to the risk, the target level of risk, and what is being done to get there.
Used by	Various government bodies
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Routine processes

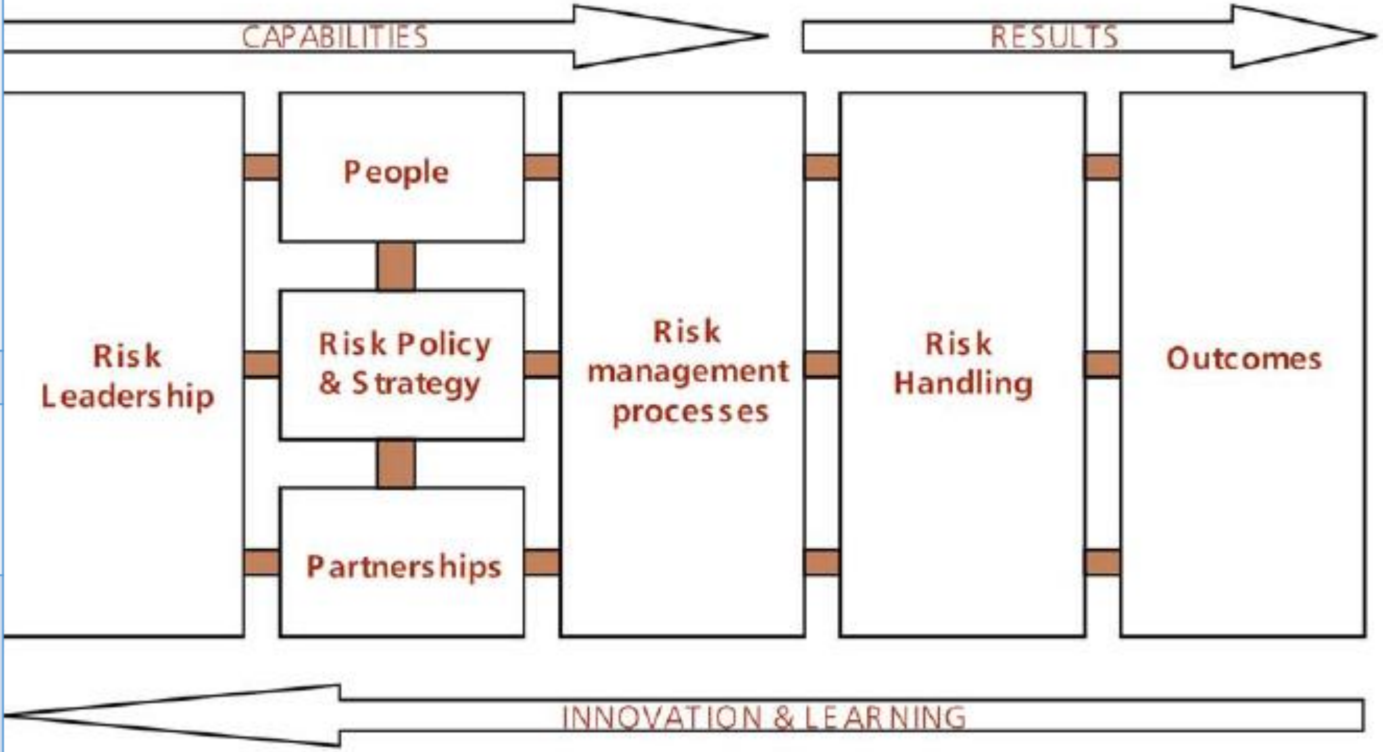
Communicating risk information

This helps because…	… it provides an example of how risk information can flow up and down an organisation. This supports management in the timely escalation and de-escalation of risks.
Used by	HMRC
Applies to the following types of risk	• Internal • External • Strategic • Project
Relates to the following element of risk management	Building blocks



Building risk maturity

This helps because…	… it uses the Risk Management Assessment Framework published by HM Treasury to distil risk management into 7 key questions. This helps management assess the organisation's relative strengths and weaknesses against the framework, and focus their subsequent improvement actions.
Used by	Various departments
Applies to the following types of risk	- Internal - External - Strategic - Project
Relates to the following element of risk management	Periodic activities



Annex D – Additional advice on risk management

The following documents should also be read and used as part of your risk management work. This framework builds on and extends the principles and concepts previously outlined in these documents.

HM Treasury’s The Orange Book
HM Treasury’s Managing Public Money (Annex 4.3)
HM Treasury’s Green Book (Annex 4)
NAO’s Managing Risks in Government
HMG’s Corporate Governance Code
HMG’s Corporate Governance Code – guidance note
FRC’s Guidance on Risk Management, Internal Control and Related Financial and Business Reporting