the Parole Board

working with others to protect the public

Parole Board for England and Wales
Risk Management Policy and Guidelines

August 2008

Contents

Chapter 1 - Introduction

What is this guide for?

This guide aim to bring together practical advice based on good risk management practice from wider government to use within the Parole Board.

……and what's in it for me, if I read it?

Reading and taking account of the messages in this document – whatever you role – **will help you do your job better**. **You will feel more in control of your job** and **you will get less nasty shocks**, with the ultimate aim being **'no surprises'** for you, and all those that rely upon you, including the public.

Who is it for?

This is for every member of staff within the Parole Board. It is as relevant to a member of the Parole Board Management Board as it is to a Head of Department or Project Head or more junior member of staff in an operational support role.

Many of us already manage risk every day, although you may not think of it in those terms. Risk affects everybody and everything we do- we should therefore **THINK RISK!**

What is 'risk'?

This guide uses the Office of Government Commerce (OGC) definition, which defines **'risk'** as **'uncertainty of outcome, whether positive opportunity or negative threat'.**

This guidance focuses especially on negative threats, which, potentially, could have a disastrous impact on public protection and the public's confidence in our ability to deliver.

What is risk management?

Risk management is a process to control the level of risk and to reduce its effects. In managing risk, the Parole Board seeks to minimise, though not necessarily eliminate, threats and maximise opportunities.

Successful risk management involves:

- Identifying and assessing threats to the achievement of objectives
- Taking action to anticipate or manage them;
- Monitoring them and reviewing progress in order to establish whether or not any further action may be necessary.

Why manage risk?

As stated above, it'll help you do your job better, but specifically:

- At a strategic level risk management can help ensue that our long term aims are achieved and foreseeable difficulties are presented.
- At a project level risk management can help ensure that the business benefits and objectives from a programme of change which are often made up of a series of steps are delivered.
- At an operational level risk management helps insure that disruption to day to day operations are minimised, as well as providing early warning systems when things go wrong.
- At a departmental level risk management can be a key component in ensuring consistent output by formulating plans to mitigate potential difficulties.

Chapter 2 – Our risk policy – no surprises

This statement sets out our commitment to managing risks effectively and the standard of risk management that the Parole Board expects in the Department

Our Risk Management Policy – 'no surprises'

We are determined to manage risk well in order to protect the public and secure our future. It is our intent to demonstrate an ongoing commitment to improving risk management throughout our organisation.

1. **Awareness:** ***"all our people have an awareness and understanding of the risks that affect the public, our colleagues and our business"***
   - **Risk identification** – line managers will encourage staff to identify risks so that there are no surprises. Staff will not be blamed or seen as being unduly negative for identifying risks.
   - **Accountability** – we will identify people who own the action to tackle risks.
   - **Communication** – there will be active and frequent communication between staff and with stakeholders, partners and suppliers.

2. **Competence:** ***"all our people are competent at managing risk."***
   - **Training** - our people will be equipped with the tools and skills they need to fulfil their responsibilities.
   - **Behaviour and culture** - senior management will lead change by example, ensuring that risks are identified, assessed and managed. Front line staff will be encouraged to identify risks.

3. **Management:** ***"all our activities are controlled using our risk management process and our people are empowered to tackle risks"***
   - **Risk assessment and management** - we will assess the risks and act to prevent, control or reduce them to an acceptable level. Our people will have the freedom and authority they need to take action to tackle risks. There will be contingency plans where needed.
   - **Process** – we will implement a risk management process. This will be integrated with our processes for audit and personal performance management and the processes of our stakeholders, delivery partners and suppliers.
   - **Measuring performance** – we will measure our risk exposure and reduce this over time. We will also measure and improve our risk management culture.

We encourage considered risk taking, experimentation and innovation. Our priority is to reduce those risks that impact on public protection, and to take appropriate steps to reduce our financial, operational and reputational risks.

Chapter 3 – Managing risk – the role of internal control

1. Internal control is an integral part of Risk Management

Internal control is action taken by management to ensure the achievement of business objectives. Control is a response to risk- it is intended to contain uncertain outcomes that have been identified.

Internal control at the Parole Board includes-

- The establishment of business objectives and measures (business plan objectives and key performance indicators)
- Procedures manuals (desk top instructions)
- Clear definitions of responsibilities (job descriptions)
- Performance management (PDR process)
- Financial controls over expenditure and budget (eg budget monitoring)

2. Balancing risk

It is important that any controls introduced are proportional to the risk. Apart from the most extreme undesirable outcomes, it is usually sufficient to design controls to give reasonable assurance of confining likely loss within the risk tolerance of the Parole Board. The control should offer value for money in relation to the risk that it is controlling. The purpose of a control is to contain risk rather than preclude it.

It is better to have five controls that you can monitor effectively than 8 controls of which three are operating effectively.

3. Type of control

Controls can address the likelihood of a risk occurring, or reduce the impact. Selecting the right controls depends on the nature of the risk.

Top tip - Identifying risk is only part of the risk management process- you also need to think about putting controls in place to counter and manage key risks.

Chapter 4 – How to Manage Risk

Basic Principles

It is Parole Board policy to implement a risk management process, which ensures that risks are identified, assessed, controlled, and, when necessary, escalated.

All staff have a responsibility to manage risk – things that could go wrong could affect the public or your colleagues. But, if you are the Head of a Department, are responsible for a project or are responsible for any operational activity, you should do the following as part of your job:

- Identify risks to the protection of the public, finance, delivery of objectives and reputation – drawing on the knowledge of front line staff;
- Assess the scale of individual risks looking at the likelihood that they will happen, and the size of the impact if they do;
- Identify the actions needed to reduce the risk and the mitigation action owners;
- Record this on a risk register;
- Check frequently (monthly) on progress;
- Apply healthy critical challenge – but do not blame people for identifying and highlighting risks or considering that they are being unduly negative in doing so.
- Have a mechanism to escalate the most severe risks and use it!

What is mandatory?

All staff, regardless of where they work in the Parole Board are required to adhere to the Risk Management Policy in the preceding section and to follow the **basic principles** of the 'best practice' risk management listed above.

Note - All reporting of risks on the Corporate Risk Register and Departmental and project risks registers *must* be on the standard Parole Board risk register template. This is to ensure that, wherever risks originate, there is consistency in how risks are reported at the top level.

The Parole Board Risk Management Framework

Step 1 Clarify Objectives

- Strategic direction
- Understanding the organisation
- Risk management scope

Step 2 Identify Risks

- What can happen?
- What can go wrong?
- How and why can it happen?

Step 3 Assess Risks

- Acknowledge existing controls
- Determine likelihood / impact
- Evaluate Risk Scores

Step 4 Address Risks

- Treat
- Tolerate
- Transfer
- Terminate

Step 5 Review and Report Risk

- Corporate
- Delivery plans
- Projects and programmes
- Unit reporting

Step 1: Clarify Objectives

For the first step of the risk management process you'll need to think clearly about what it is you are expected to achieve:

- What are you (we) trying to achieve?
- By when? and
- Who is accountable for delivery?

This includes:

- Identifying and clarifying the Parole Board Strategic Objectives that are relevant to your organisation – if you forget this step you will have a risk register that is not relevant to your work and cannot be used as an effective tool[1];
- Understanding your organisation, its activities, responsibilities and its capabilities, as well as its goals and objectives and the plans that are in place to achieve them;
- Identifying links with internal and external stakeholders;[2]
- Identifying other external factors that might affect the organisation;
- Establishing the roles and responsibilities for risk management in your organisation.

Key Outcome - You are clear about what you and your organisation is expected to achieve – the key first step before you identify any risks.

Step 2: Identify Risks

Firstly, you need to identify the risks:

- Do you know what all of the risks to the delivery of your objectives or work are, especially those that impact on public protection?
- Who does?
- Who else might know?

If you can, you need to gather these people together and hold a meeting or run a risk identification workshop.

At this stage, the following key questions should be asked:

- What could happen?
- What can go wrong?
- How and why can this happen
- What do we depend upon for our continued success?

Remember that absence of evidence of a risk does not mean absence of a risk! If you are not sure whether you have full information on a

[1] This stage is often forgotten and the effectiveness of risk registers is affected as a result.

[2] Stakeholder is defined in this guide as a person or group who has an interest in or is affected by the work that you are doing.

potential serious risk arising in your area of responsibility, you should check whether more information is needed.

Defining Risks

You must define your risks or you won't be able to manage them! Defining risks is a common problem and is an exercise that people can find difficult.

It is critical that risks are clearly articulated. If they are not then it is difficult to put in place effective mitigating actions and contingency plans. It is very easy, as you begin to identify risks, to record them in a generic or summarised way. For example- "IT failure" or "Lack of resources". However, in this way valuable thinking about the precise cause, effect and scope of the risk may be lost-leaving you with a list of risks which may mean different things to different people. It helps if risks are articulated in the following format:

"Something may happen (cause), which may lead to something else happening (the effect), where the impact would be something (preferably quantifiable) adverse."

Top tip – A good check, to find out whether you have defined your risk clearly enough is to ask yourself this question – Will I know when this risk has happened? If the answer is no, you should revisit the risk you have identified and reconsider what causes them and what impact they will have if they occur.

Look at the following hypothetical examples:

"Backlog of criminal record notifications may include convictions for serious offences which have not been entered on the PNC (cause) resulting in possible failure to carry out effective CRB checks in these cases (effect) where the impact would be increased risk to the public."

"Resources for an IT project may not have the required technical skills (cause) resulting in additional work to acquire resource (effect) where the impact would be a delay or a significant increase in costs."

This can also be more easily expressed as: **CAUSE – EFFECT – IMPACT**

Getting this right pays real dividends later as you can directly match counter measures to the potential threat. More often than not, it's the cause you need to counter.

Risk Ownership

Risk is not something that is managed by an 'expert'. Having identified and defined your risks, it is essential that someone 'owns' them. This is not the same as being responsible for carrying out any mitigation actions which may be needed to control the risk. However, without a named individual taking overall responsibility, it is unlikely that risk management actions will be followed through.

For that reason this person should:

- Where possible, be someone who has the ability to influence the outcome of the event one way or another; and
- Certainly be the primary person who is accountable for delivery in the area where the risk would have an impact.

In reality, the individuals selected would be accountable for any risks threatening the business, whether explicitly named or not. 'Ownership' of the risk within the context of a risk management framework simply clarifies and formalises their responsibilities.

Remember!

Risk owner – The person who is accountable and answerable, should the risk materialise.

Action Owner – The person responsible for one or more of the mitigating actions (as there may be several). The action owner may well be one of several reporting to the owner of the risk. It is also possible that the risk owner undertakes one, more or all of the mitigating actions.

Key Outputs - You should have a list of all the key risks that threaten achievement of Parole Board objectives. Stakeholders and workshop participants should be satisfied that the list covers all types of risk and that it does reflect reality.

- **All risks should have individual, named owners who are aware of their responsibilities;**
- **They should be defined clearly and made time specific whenever this is appropriate**

Step 3: Assess the risk

The main reason for assessing risks is to distinguish between the key risks that require comprehensive action to manage them, and other risks which can be more easily contained.

Once you have identified the risks you will need to:

a) Acknowledge your existing controls

This involves identifying any existing management systems and procedures to control risk and assessing their strengths and weaknesses. Simply put, you need to make a judgement about the effectiveness of existing controls to manage the risks you face. Make sure that any information you are relying on to assess the risks is up-to-date and valid.

b) Determine likelihood and impact

The likelihood and impact of an event occurring is always a question of judgement, but you can make use of past records, relevant experience, expert judgements and any relevant published documents to help you make this as informed as possible. Remember to take account of existing controls, which could reduce the level of risk.

Top tip - The risk rating shown should be after the effect of your mitigating actions.

The Parole Board uses the five-point scale when assigning a rating to both the likelihood and impact of individual risks (Very high, high, medium, low, and very low).

Impact

Q. How severe would its impact be on public protection, the finances of your organisation, reputation of the department or the delivery and achievement of objectives?

Impact is the outcome of an event expressed positively or negatively, qualitatively or quantitatively, being a loss, injury, disadvantage or gain. Remember – there are likely to be a range of outcomes for this event.

Impact	Score	Description
Extreme	5	Critical impact on your objectives and performance and could seriously affect reputation. Could be long term and very difficult to recover with high costs
Major	4	Major impact on your objectives and performance. Could be expensive to recover and affect reputation. Could have medium to long term

		effect.
Moderate	3	Significant impact on your operational performance and quality. Could have medium term effect and be potentially expensive to recover.
Minor	2	Minor delays and impact on your services. Short to medium term effect.
Insignificant	1	Minor impact on your services. Quickly and easily remedied.

Likelihood

Q. How likely is it that this risk will occur?

Likelihood is used as a qualitative description of likelihood or frequency. The following likelihood ratings are used by the Parole Board.

Likelihood	Score	Description
Almost certain	5	>80% Almost certain to occur
Likely	4	51-80% More likely to occur than not
Credible	3	21-50%. Fairly likely to occur
Unlikely	2	6-20% Unlikely but possible
Rare	1	0-5% Extremely unlikely

How to score impact using the matrices
You should score your risk against whichever description most closely matches the potential impact of your risk. If, for example, the potential impact of your risk matched a unit level one it should continue to be managed at that level, if however, its impact profile now matched that of a description on the higher, directorate, group or corporate register, perhaps as a result of policy changes, you should propose that this risk be escalated to the higher level, via your director.

When evaluating impact, also check the scale above your own (or perhaps below). If you are looking at a risk on either the 'Projects and Programmes' or 'Unit' scale it might have a 'Corporate' dimension, so check! This will be important when deciding whether a risk needs to be escalated. You may have identified a risk that should actually be seen by your director or the HOB – **risk management can sometimes just be about sounding the alarm**. Don't worry if your director, Head of Unit or manager decides after consideration that the risk should not be escalated. **The key thing is to bring the risk to their attention, so if in doubt consult!**

c) Evaluate risk severity

The purpose of this step is to enable you to judge the degree of action that will be necessary to manage individual risks. Once you have established both the likelihood of an event and its associated impact, you then need to combine them to produce the level of risk severity.

The Parole Boards model for risk evaluation is below.

PAROLE BOARD RISK MATRIX

BUSINESS IMPACT						
Extreme	**5**	**5**	**10**	**15**	**20**	**25**
Major	**4**	**4**	**8**	**12**	**16**	**20**
Moderate	**3**	**3**	**6**	**9**	**12**	**15**
Minor	**2**	**2**	**4**	**6**	**8**	**10**
Insignificant	**1**	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Credible**	**Likely**	**Almost certain**

LIKELIHOOD

The higher the risk score the more serious the risk

Note - Evaluating risk is an iterative process. Once you plot your risks on the matrix, it could lead you to the conclusion that, for example, a particular risk seems to have too high a severity rating. In such cases you need to re-check your assumptions and look again at the likelihood and/or impact ratings.

Risk Trend

Once there is a current and previous risk assessment, a trend can be established. This will be either stable, rising or reducing and will be represented by an

appropriate arrow (up, down or horizontal). See Annexe D for an example of how this rating has been recorded.

Key Output - By the end of this step you should have a list of risks with scored levels of risk severity, a feel for which ones the threat is increasing for and an assessment of when, if any of the risks did occur, how soon they would. This information gives you an understanding of their relative priority for further action. These sequences of colours appear like a 'fruit machine' reel and give you a very visual signal or warning.

Step 4: Address the risk

Addressing the risk involves the practical steps that need to be taken to manage and control it – often to lessen the likelihood of it happening or the impact if it did, or both. Without this stage, risk management is no more than a bureaucratic or paper based process.

Not all risks can or need to be dealt with in the same way.

The Parole Board has now adapted the wording used in previous guidance to match the '4 T' (Treat, Tolerate, Transfer or Terminate) standard in the OGC Management of Risk guidance.

- **Treat** – A selective application of management action, by applying internal control to reduce either the likelihood of occurrence or the impact, or both, which is designed to contain risk to acceptable levels. For example, mitigation action, contingency planning.
- **Tolerate** – An informed decision to accept the likelihood and consequences of a particular risk. For example the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit, or, judged against your risk appetite, the risk may be manageable. If taking this course of action you would expect to have a contingency plan to handle the impact of the risk, should it occur.
- **Transfer** – Shifting the responsibility or burden for loss to another party through, for example, insurance. **Note:** This should be used with caution – in reality it is often impossible to transfer a risk effectively. For example, if the risk to the Parole Board is largely a reputational one and a contractor is only obliged to compensate us financially, the risk cannot be well-managed.
- **Terminate** – An informed decision not to become involved in a risk situation. In reality the Parole Board may not be able to avoid risks associated with its statutory functions.

In most cases, the chosen option will be the first one as other options, such as terminating the risk become unlikely as our business continues to be high profile and challenging. Innovation by its very nature involves taking risks and, as a consequence, it places greater demand on us all to ensure that those risks are well managed.

Action Progress

You will also be expected to undertake an assessment of how the action outlined in the mitigating actions box is progressing.

Contingency Plans

If you have a risk that is rated **red** in terms of its severity rating, you should always give thought to what you will do, should the risk materialise. If you have expected the risk to materialise for some time, you should have informed your line management and surprising them at the last minute is bad management. Sometimes contingency plans need only be about knowing who to contact in Press Office and/or to have briefing or a statement ready in the event of a failure or negative event. With many severe risks you will need to have put in place a full contingency plan that can counter the impact should it occur.

Good risk management is about being 'risk aware' not 'risk averse'.

Key questions:

- Actions taken to manage risk may have an associated cost. When considering mitigation or contingency action, make sure that its cost is proportionate to the risk that it is controlling.
- When agreeing responses or actions to control risk, remember to consider whether the actions themselves introduce new risks or affect other people in ways which they need to be informed about.
- Always keep risks to the public uppermost in your mind. Protecting the public is what we are all here to do.

Key Output - At the end of this step you should have a clear and detailed action plan which sets out how you intend to manage your risks. Do not forget that specific actions need to be assigned to, and agreed with, specific individuals.

Step 5: Monitoring and review

Few risks will remain static. New stakeholders may affect your business and existing ones may continually change in terms of their interest and influence.

Some risks cease to exist once a key milestone has passed during the life cycle of a project.

Whatever the scenario, having identified your risks and put into place appropriate controls and action plans to manage them, it is essential that you routinely monitor their status.

The wider context

Monitoring takes place at several levels within the Parole Board:

- Group and Corporate risks are monitored monthly by the Executive Team and quarterly by the Audit and Risk Management Committee;
- Departmental risks are monitored by the Secretariat Management Committee on a quarterly basis.
- Project risk is managed by project group and reviewed by the Executive Team.

How does risk management work in your area?

Key Outcome - That management of risk becomes good management behaviour that is taken for granted, rather than something that is remembered only when it is too late.

Recording risk on a Risk Register

You will have generated a good deal of data when identifying, assessing and addressing your risks. Whilst we all want to keep the level of paperwork to a minimum, it is important that the most important risks are recorded to:

- Avoid misunderstandings later between the responsible individuals;
- Provide a clear audit trail – risk registers should be dated and an audit trail of previous risk registers should be maintained;
- Help monitor whether the risk is reducing or increasing.

Top tip: Risk registers should clearly identify risk owners.

.

Risk Register

The Parole Board using registers for

- Corporate risk
- Departmental risk
- Project risk

Note - You may have identified quite a few risks. Common sense should be used when deciding how many risks should be recorded – most people find it difficult to manage more than 10 to 15 risks. You should include those risks that are of most concern to you in terms of public protection, delivery of objectives, finance or reputation. If you have more than 15 risks, are any of these different manifestations of the same risk? You can check this by comparing mitigating actions - if they are the same, this may indicate a different facet of the same risk, eg. an operational risk may well have a reputational impact as well as an operational one.

Escalating Risk

Advice on risk escalation should be sought from the Executive Team. Risks may be both escalated and de-escalated.

Project risk

Project risk controls- think

- **Time**
- **Cost**
- **Benefit**

Annexe A – One page guide to manging risk

Step 1 Clarify Objectives

- Are you clear about what you and your organisation are expected to achieve i.e. your objectives?
- Are internal and external stakeholders identified?
- Have roles, responsibilities and objectives for risk management been established?

Step 2 Identify Risks

- Has a full, comprehensive set of threats been identified (a threat being a factor that could lead to a risk occurring)?
- Have risks been identified according to the 4 Parole Board risk classifications (Protecting the Public, Delivery, Finance, and Reputation)?
- Is the output of risk identification documented in a Risk Register (according to the standard format)?
- Is it actually a risk or an opportunity?

Risk ownership

- Have risk owners been allocated for all the various parts of the management of the risk process?
- Do the individuals who have been allocated ownership have the authority and capability to fulfill their responsibilities?
- Is ownership reassessed on a periodic basis or in the event of a change in the situation?
- Do all risks, and where appropriate, mitigation actions, have clearly identified owners? Are these owners appropriate?

Step 3 Assess Risks

- Is a consistent approach being taken to assessing potential impact, likelihood, and possible action?
- Is the level of analysis in proportion to the level of risk? Are detailed assessments being carried out on threats that are known to have little, or no, impact (or vice-versa)?
- Is there a good understanding of the relationship between the potential impact and probability of the risk occurring?

Step 4 Address Risks

- Have the risks been assessed and prioritized to see which needs tackling first?
- Has there been a clear allocation of responsibilities and ownership for actions and decisions and the required timescales for completion and review?
- Has the treatment of recommended risk counter measures been assessed in

terms of: Their costs compared with anticipated benefits of treating the risk? (Good risk management is about being 'risk aware' not 'risk averse'. Treat, tolerate, transfer or terminate? Effectiveness in containing the risk or enhancing the opportunity?

- Are risks being escalated to the appropriate level
- Is there a mechanism in place for monitoring and reporting on the effectiveness of the actions being undertaken?

Step 5 Monitoring and Review

- Are risks regularly reviewed?
- Is there confidence in the accuracy of reporting?