Enterprise Risk Management: Risk Appetite Framework
Key Issues

• Can we develop a model for Health and Care, recognising that a lot of what we do has inherent risk?
• Approach must be specific to organisation: aligned with strategy/mission/vision
• Who are the key stakeholders?
• What metrics can we use to measure appetite and give early warning of potential operation outside of appetite?
• Consider appetite in relation to:
  – Controls/assurance want to apply
  – Level of investment willing to make to reduce risk (deployment of resources)
  – Balance between risk and opportunity: low risk appetite and desire to achieve benefits/improvement
  – Risk proximity
• Consider data available to develop dashboards
Some Principles

• Clarify what we are defining appetite against
• Define key questions:
  – Where do you think you should take more risk?
  – Where do you feel uncomfortable with the level of risk being taken?
  – What are your tolerances?
  – What is your appetite for spend?
• Align and educate stakeholders
• Pick specific small set of risks to start with – stakeholders from specific areas concerned
• Link risk appetite metrics to how organisation measures success (e.g. develop KRI as flip side of KPIs)
• Collective review to ratify and consider areas of trade off and organisational appetite
• Executive buy-in
• Socialise and operationalise
We may vary the Risk Appetite for different parts of the organisation

Optimum position of a change or innovation in the portfolio (theoretical)

Positive outcome of a change or innovation in the portfolio (realistic)

Risk appetite (hard stop)
Only change/innovations with a risk profile lower than or equal to this position would be considered

No risk, no value

The risk profile of each change/innovation varies from the next. The ideal position is low risk and high value/high return.

Ability to take faster decisions with greater confidence
Strategy and Risk Appetite

Risk appetite linked to vision, values, principles and strategy

Operating risk statements linked to directions; policies; rules; regulations and delegated powers

Organisational risk appetite statement

- Cost
- Capability
- Data Security
- Data Quality
- Live Systems
- Patient Safety
- Change
- Business Partnerships

Influencers
- Ministers, departmental sponsor, regulators, commissioners, competitors

Operating risk statements

Key Performance Indicators and tolerances

Influencers
- Staff and management, culture and behaviour

Strategy

Risk profile

Influencers

Cost

Capability

Data Security

Data Quality

Live Systems

Patient Safety

Change

Business Partnerships

Accountability

Application

Monitoring

Reporting & disclosure

Assurance & compliance

Strategy and Risk Appetite
Application of Risk Appetite

- Risk Appetite will be defined in terms of our most significant risks; and applied on a case by case basis, supported by defined metrics to provide Key Risk Indicators and escalation criteria.
- We will consider situations where we feel we should take more risk and where we feel uncomfortable with the current level of risk exposure.
- We will also consider accumulations of risks, so we understand how much (cumulative) risk we can tolerate and survive.
- Detailed application will consist of:
  - Target appetite for each strategic risk with supporting metrics/Key Risk Indicators: to set escalation criteria.
  - Framework for risk escalation: including to consider when we should operate outside of appetite* (e.g. in trade-off/prioritisation etc. decisions).
  - Structure for Risk, Incident and Near-Miss reporting: are we operating within appetite; and (if “non-compliance” is organisation wide) whether we need to recalibrate risk appetite.
  - Consideration of how much (cumulative) risk we can tolerate and survive.

* When seeking permission to take a risk outside of appetite the request should define the potential consequences in terms of acting/not acting, in particular:
  - Positive/negative impacts – especially in areas of low risk appetite, where we would wish to avoid any adverse impact e.g. patient safety; protection of personal sensitive data (“golden rules”);
  - Benefits/opportunities that would be obtained/missed;
  - How identified risks and issues will be managed; and
  - Risk based go/no go thresholds.
**Risk Appetite: a Template?**

Assumed Level of Risk Appetite: Minimalist (Amber/Green)
Current Strategic Risk Target (Post Mitigated) Rating: Amber – indicates level of Risk Tolerance?

<table>
<thead>
<tr>
<th>Definitions</th>
<th>Averse</th>
<th>Minimalist</th>
<th>Cautious</th>
<th>Open</th>
<th>Hungry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoidance of risk and uncertainty is a key</td>
<td></td>
<td>Preference for ultra-safe</td>
<td>Preference for safe delivery</td>
<td>Willing to consider all potential delivery</td>
<td>Eager to be innovative and to choose options offering potentially</td>
</tr>
<tr>
<td>Organisational objective.</td>
<td></td>
<td>business delivery options that</td>
<td>options that have a low</td>
<td>options and choose the one that is most</td>
<td>higher business rewards (despite greater inherent risk).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>have a low degree of inherent</td>
<td>degree of inherent risk and</td>
<td>likely to result in successful delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>risk and only have a potential</td>
<td>may only have limited</td>
<td>while also providing an acceptable level of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>for limited reward.</td>
<td>potential for reward.</td>
<td>reward (and value for money etc.).</td>
<td></td>
</tr>
</tbody>
</table>

| Risk Impacts Metric Scale                        |        |                                 |                              |                                                |                                                                        |
## Key Risk Indicators

<table>
<thead>
<tr>
<th>Risk dimension</th>
<th>Types of indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>• Number of risk events</td>
</tr>
<tr>
<td></td>
<td>• Average time between incidents</td>
</tr>
<tr>
<td></td>
<td>• Missed programme etc. milestones/KPI targets</td>
</tr>
<tr>
<td>Severity</td>
<td>• Current RAG rating accumulated</td>
</tr>
<tr>
<td></td>
<td>• Total Duration of incidents</td>
</tr>
<tr>
<td></td>
<td>• Cost of service disruption</td>
</tr>
<tr>
<td>Impact</td>
<td>• Personal data compromised</td>
</tr>
<tr>
<td></td>
<td>• Penalties</td>
</tr>
<tr>
<td></td>
<td>• Service disruption</td>
</tr>
</tbody>
</table>


The Basis of Risk Escalation

Risk Scoring Matrix

- The risk scoring matrix is the basis of our risk reporting and escalation framework.
- It follows an HM Treasury model and is based on a formula which gives more emphasis to high impact risks.
- Additional factors to RAG ratings should be taken into account when making a decision as to whether to escalate a risk, including:
  - Key Risk Indicator trigger reached;
  - Risk Proximity / Critical Date;
  - Operating outside of Risk Appetite / defined Tolerances;
  - Late / Incomplete Mitigation Action(s); and
  - Key Control Gaps/Weaknesses.
Risk Appetite Aide Memoire

Things to consider

• Risk appetite: the amount of (residual) risk exposure we are prepared to accept to achieve our (long term) objectives.

• Risk tolerance: the boundaries for tolerable risk taking; cumulatively the limit of loss we can absorb and remain a sustainable organisation.

• Risk control: level of control and assurance we wish to have in place to take a risk (related to severity of risk exposure; circumstances where we wish to operate outside of appetite; or novelty of activity).

• Risk Appetite articulation:
  – “We will only take a risk in this area in these circumstances……
  – within the boundaries of…and …..
  – and if we have a level of control/mitigation that includes…..
  – with appropriate assurance on control/mitigation effectiveness, which gives us an acceptable level of confidence.”

• Control Appetite. Set in the context of risk profiles and tolerances (defined in RPAs cyber risk profiles, information asset criticality etc.):
  – High Inherent risk
  – Medium Inherent risk
  – Minimal Inherent risk