Enterprise Risk Management:
Risk Appetite Framework

Steve Treece, NHS Digital
IRM Health and Care SIG
27 June 2019

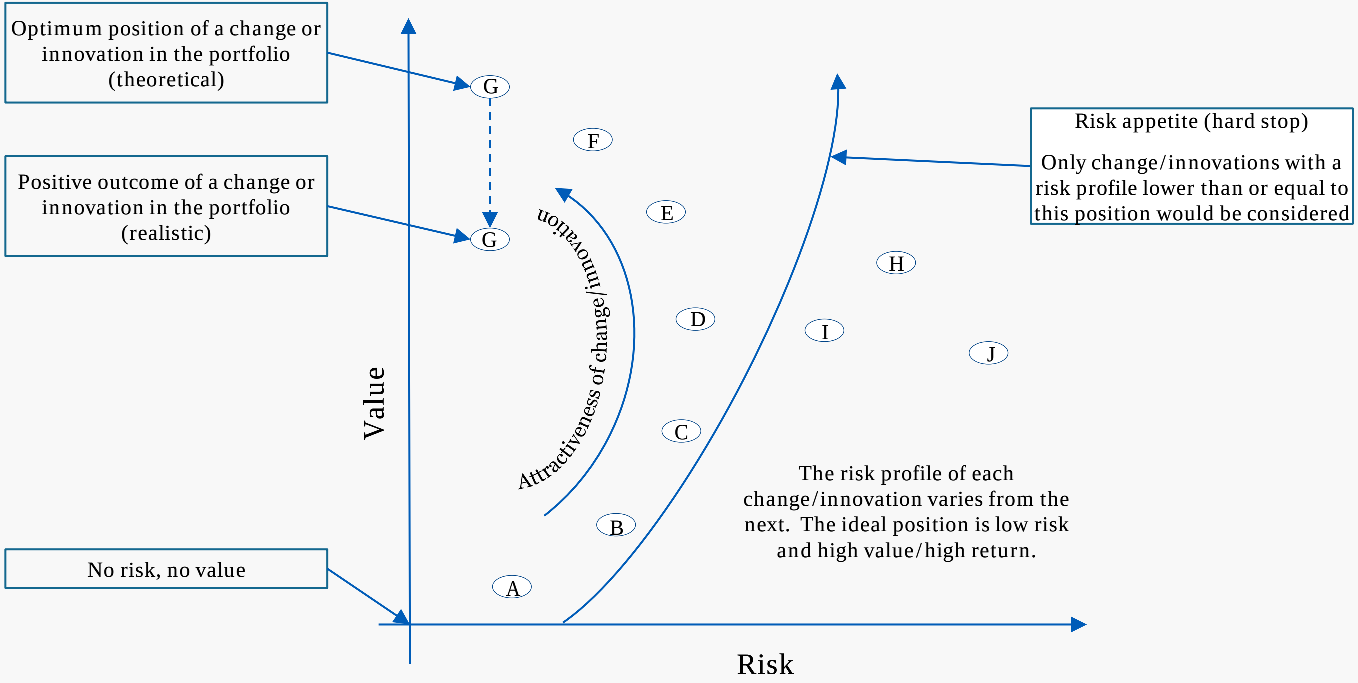
Key Issues

- 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 KRIs 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)

No risk, no value

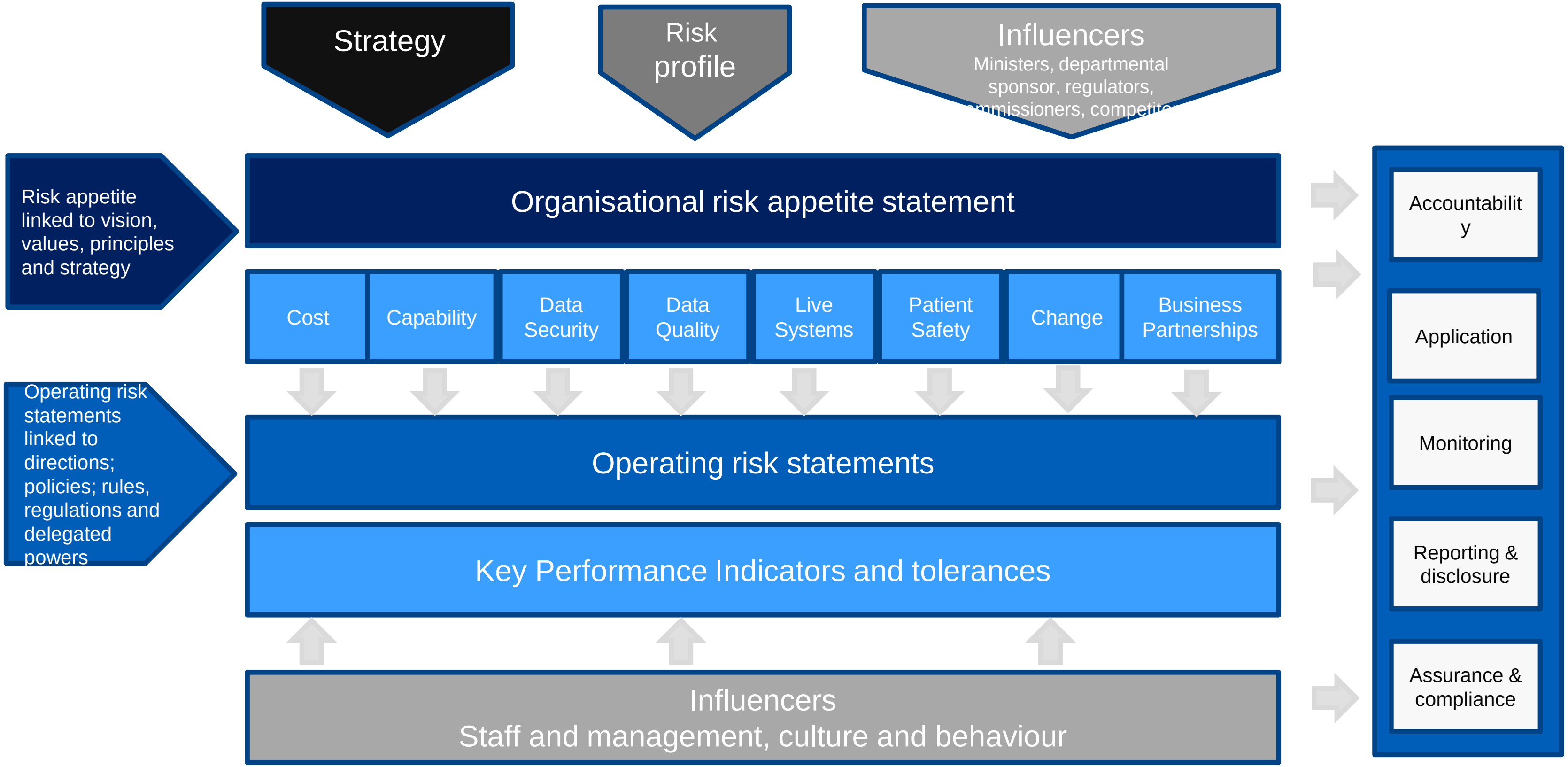
Risk appetite (hard stop)

Only change/innovations with a risk profile lower than or equal to this position would be considered

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



Strategy

Risk profile

Influencers
Ministers, departmental sponsor, regulators, mmissioners, competito

Risk appetite linked to vision, values, principles and strategy

Organisational risk appetite statement

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

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

Operating risk statements

Key Performance Indicators and tolerances

Influencers
Staff and management, culture and behaviour

Accountability

Application

Monitoring

Reporting & disclosure

Assurance & compliance

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?

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

Key Risk Indicators

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

The Basis of Risk Escalation

Risk Scoring Matrix

Impact	Very High	5	16	20	22	24	25
	High	4	11	14	18	21	23
	Medium	3	9	10	12	17	19
	Low	2	6	7	8	13	15
	Very Low	1	1	2	3	4	5
	Score		**1**	**2**	**3**	**4**	**5**
			Rare < 10%	Unlikely 11-33%	Possible 34-67%	Likely 68-89%	Almost Certain 90-100%

Likelihood

- 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