IDENTIFYING RISKS

INTRODUCTION

Risks that are not identified are not likely to be managed

The types of risks that impact organizations vary depending on such factors, such as: region, industry, and level of globalization

- Banks → credit and market risk
- Insurance companies → actuarial risk
- Business firms → reputation and legal risks

Risk management is not intended to be risk elimination.

Risk identification → identifying the threats and vulnerabilities

INTRODUCTION

Identification of risk can be separated into two distinct phases:

1. **Initial risk identification**

   For an organization which has not previously identified its risks in a structured way, or for new organization, or for a new project or activity within an organization

2. **Continuous risk identification**

   Identification of new risks which did not previously arise, changes in existing risks, or risks which did exist ceasing to be relevant to the organization

DETERMINING RISKS

1. **Risks can only be assessed and prioritized in relation to objectives**

   Organization cannot involve risks related to individual objectives

2. **A risk may be relevant to more than one of the organization's objectives, but the potential impact may vary in relation to different objectives**

   Best way of addressing a risk may be different in relation to different objectives

3. **In stating risks, avoid stating impacts which do not impact on objectives**

   A statement of a risk should encompass the cause of the impact, and the impact to the objective

STEPS IN IDENTIFYING RISKS

1. **Identify threats**

   A threat is any circumstance or event with the potential to cause a loss → "any activity that represents a possible danger"

   Loss or danger is directly related to one of the following:

   - Loss of confidentiality – someone sees your password
   - Loss of integrity – an email message is modified, a virus infects a file, someone make unauthorized changes to a website
   - Loss of availability – an email server is down and no one has email access, a file server is down so data files aren't available

STEPS IN IDENTIFYING RISKS

1. Identify threats

Threat identification → a process of creating a list of threats

It involves all possible threats to an organization.

Threats can be categorized into:

1. External or internal
2. Natural or man-made
3. Intentional or accidental

One method to identify threats → brainstorming session

- Participants throw out anything that pops into their heads
- All ideas are written without any evaluation

STEPS IN IDENTIFYING RISKS

2. **Identify vulnerability**

   A vulnerability is a weakness → when a threat occurs, if there is a vulnerability, the weakness is apparent

   Sources to identify vulnerability:

   1. Audits
   2. Certification and accreditation records
   3. System logs
   4. Prior events
   5. Trouble reports
   6. Incident response teams

STEPS IN IDENTIFYING RISKS

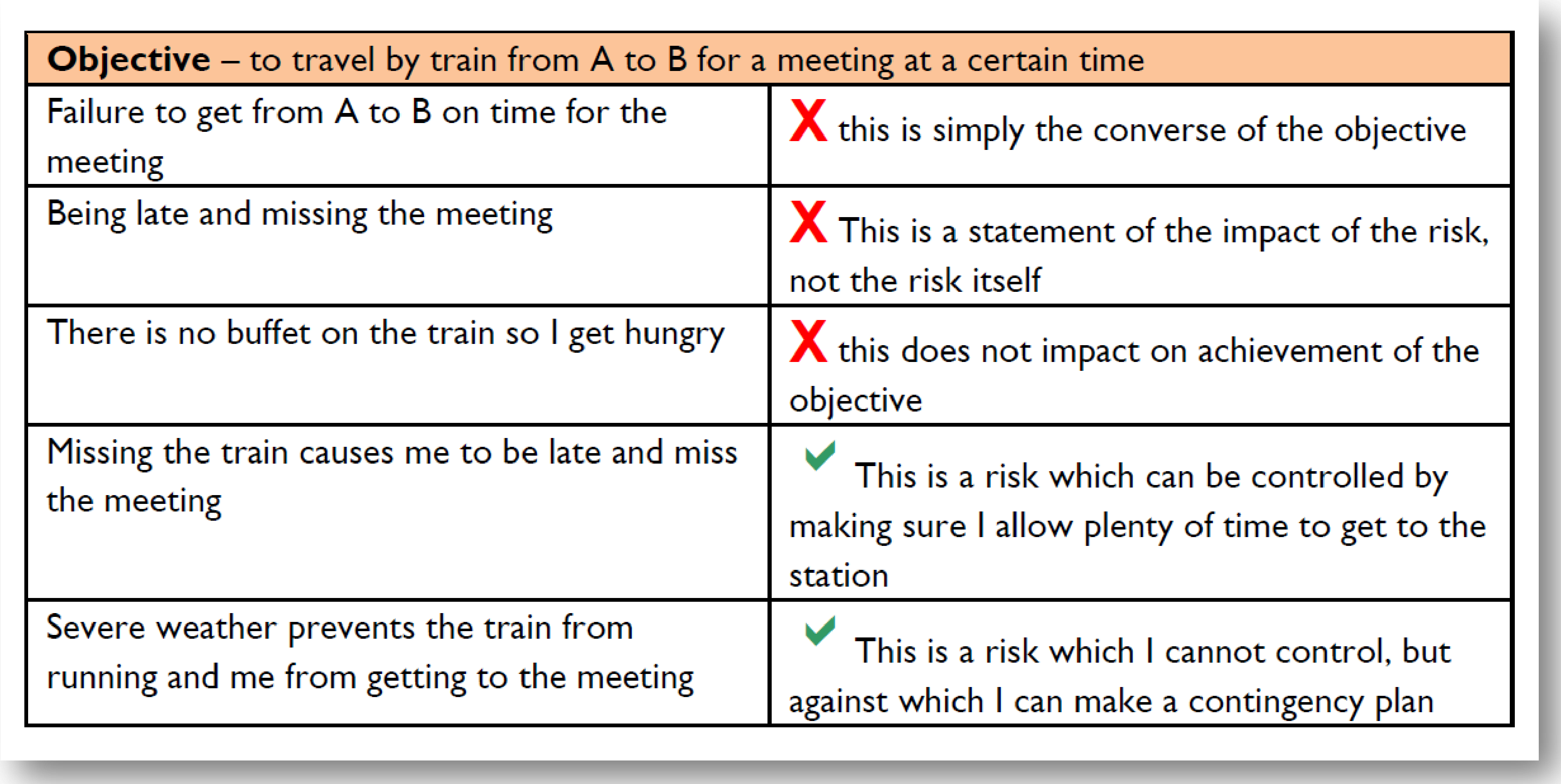
3. Estimate the likelihood of threat exploiting a vulnerability

To determine the likelihood of a risk → threats are matched to existing vulnerability

How to pair threat with vulnerabilities

1. Risk = Threat x Vulnerability
2. Total risk = Threat x Vulnerability x Asset Value

EXAMPLE OF IDENTIFYING RISK



Objective – to travel by train from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	✗ this is simply the converse of the objective
Being late and missing the meeting	✗ This is a statement of the impact of the risk, not the risk itself
There is no buffet on the train so I get hungry	✗ this does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	✓ This is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	✓ This is a risk which I cannot control, but against which I can make a contingency plan

APPROACH TO IDENTIFY RISKS

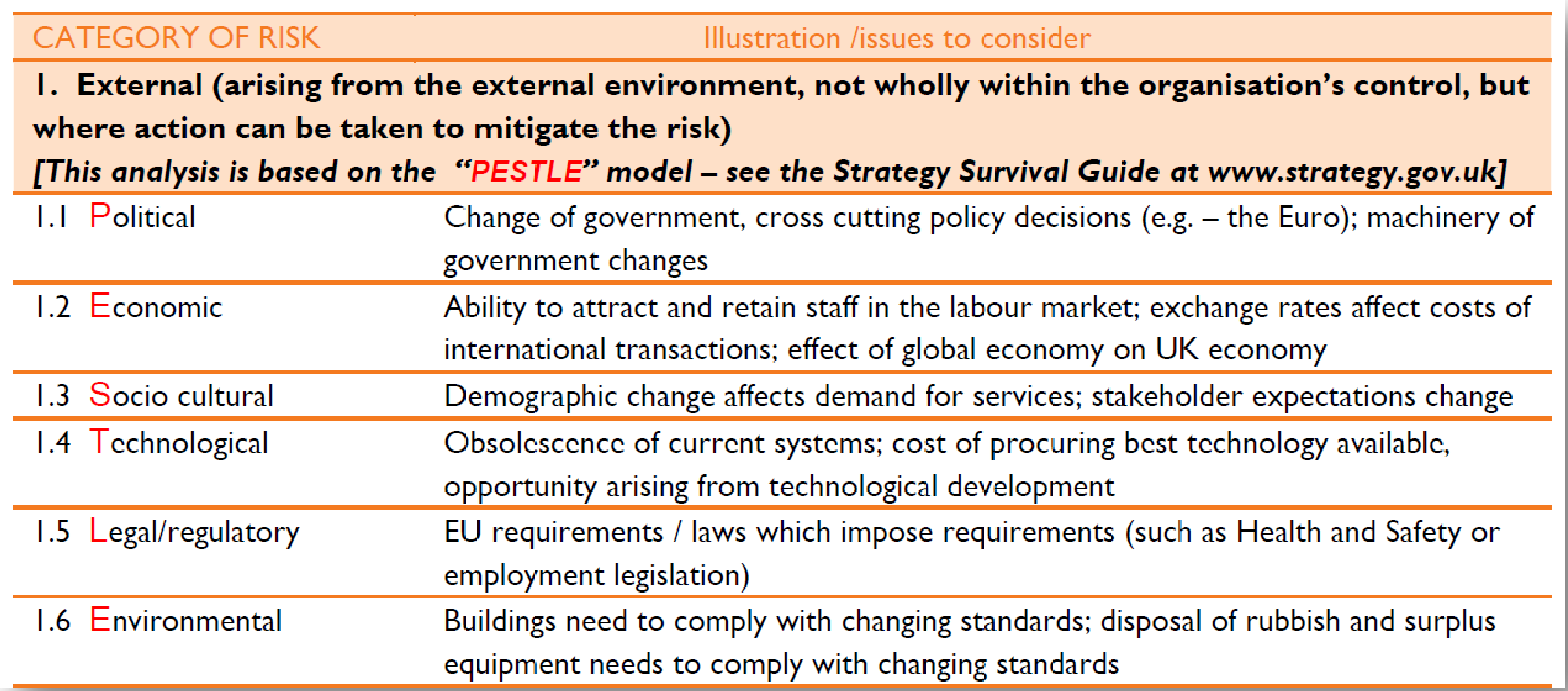
1. **Commissioning a risk review**
   - Establish a designated team (either in-house or contracted in)
   - Consider all the operations and activities of the organization in relation to its objectives
   - Conduct a series of interviews with key staff at all level of the organization to build risk profile
   - Identify the associated risks

APPROACH TO IDENTIFY RISKS

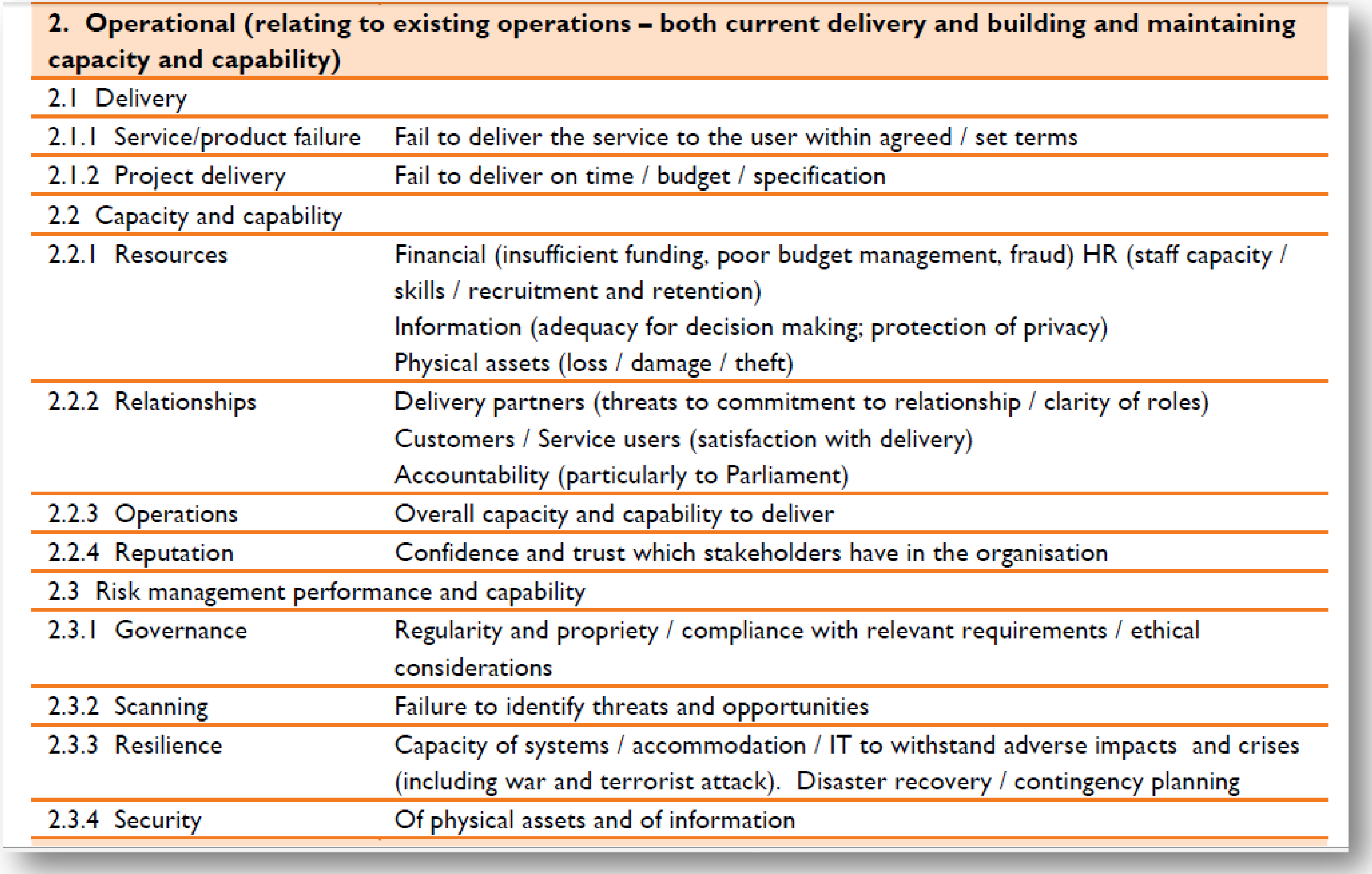
2. **Risk self-assessment**

    - Each level and part of the organization is invited to review its activities and to contribute its diagnosis of the risks
    - This could be done through a documentation approach (using a set of questionnaires)
    - But, it is often more effective through a facilitated workshop approach → a better ownership of risk management tends to be established when the owners identify the risks they face

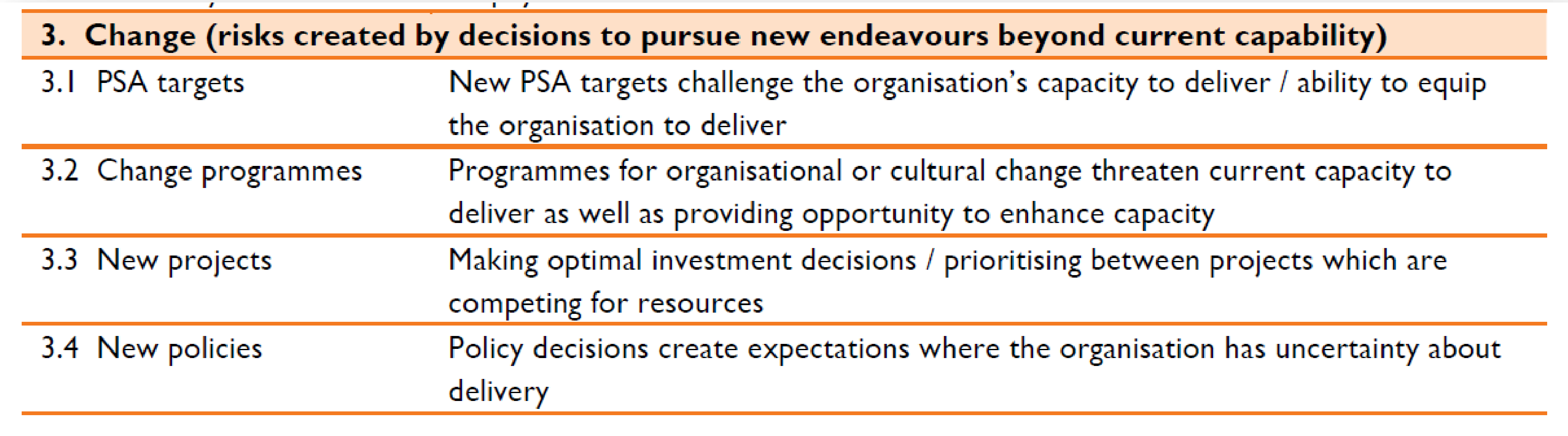
EXAMPLES OF RISK IDENTIFICATION



CATEGORY OF RISK	Illustration /issues to consider
1. External (arising from the external environment, not wholly within the organisation's control, but where action can be taken to mitigate the risk) ***[This analysis is based on the "PESTLE" model – see the Strategy Survival Guide at www.strategy.gov.uk]***	
1.1 Political	Change of government, cross cutting policy decisions (e.g. – the Euro); machinery of government changes
1.2 Economic	Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect of global economy on UK economy
1.3 Socio cultural	Demographic change affects demand for services; stakeholder expectations change
1.4 Technological	Obsolescence of current systems; cost of procuring best technology available, opportunity arising from technological development
1.5 Legal/regulatory	EU requirements / laws which impose requirements (such as Health and Safety or employment legislation)
1.6 Environmental	Buildings need to comply with changing standards; disposal of rubbish and surplus equipment needs to comply with changing standards



2. Operational (relating to existing operations – both current delivery and building and maintaining capacity and capability)	
2.1 Delivery	
2.1.1 Service/product failure	Fail to deliver the service to the user within agreed / set terms
2.1.2 Project delivery	Fail to deliver on time / budget / specification
2.2 Capacity and capability	
2.2.1 Resources	Financial (insufficient funding, poor budget management, fraud) HR (staff capacity / skills / recruitment and retention) Information (adequacy for decision making; protection of privacy) Physical assets (loss / damage / theft)
2.2.2 Relationships	Delivery partners (threats to commitment to relationship / clarity of roles) Customers / Service users (satisfaction with delivery) Accountability (particularly to Parliament)
2.2.3 Operations	Overall capacity and capability to deliver
2.2.4 Reputation	Confidence and trust which stakeholders have in the organisation
2.3 Risk management performance and capability	
2.3.1 Governance	Regularity and propriety / compliance with relevant requirements / ethical considerations
2.3.2 Scanning	Failure to identify threats and opportunities
2.3.3 Resilience	Capacity of systems / accommodation / IT to withstand adverse impacts and crises (including war and terrorist attack). Disaster recovery / contingency planning
2.3.4 Security	Of physical assets and of information



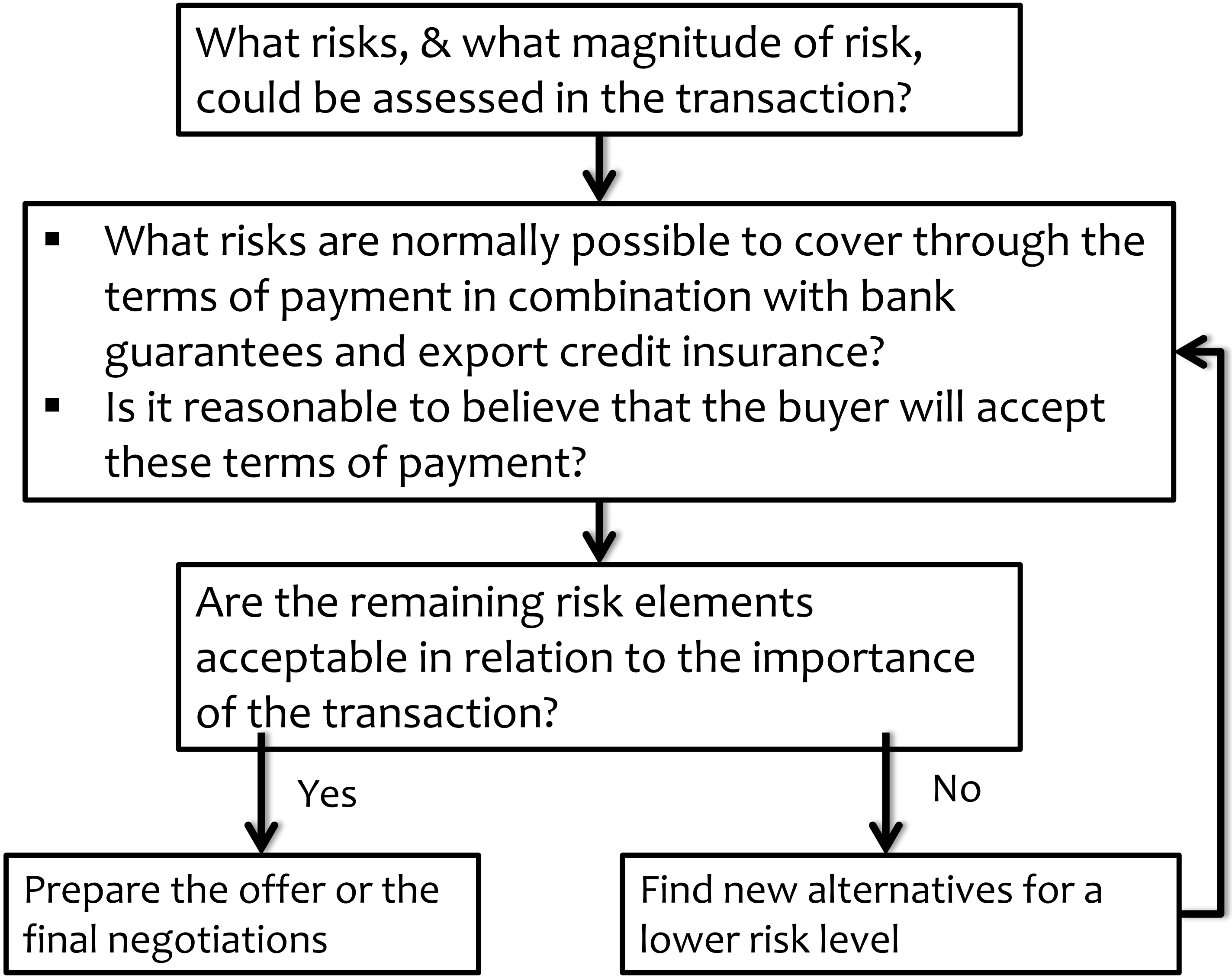
3. Change (risks created by decisions to pursue new endeavours beyond current capability)	
3.1 PSA targets	New PSA targets challenge the organisation's capacity to deliver / ability to equip the organisation to deliver
3.2 Change programmes	Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity
3.3 New projects	Making optimal investment decisions / prioritising between projects which are competing for resources
3.4 New policies	Policy decisions create expectations where the organisation has uncertainty about delivery

BASIC CONCEPTS OF RISK ASSESSMENT

Range of assessment depends on the width of transactions

Reaction towards risk depends on the degree of a subjective valuation. However, both parties who trade should have good knowledge in order to carry out a proper and meaningful risk assessment

RISK ASSESSMENT MODEL



What risks, & what magnitude of risk, could be assessed in the transaction?

- What risks are normally possible to cover through the terms of payment in combination with bank guarantees and export credit insurance?
- Is it reasonable to believe that the buyer will accept these terms of payment?

Are the remaining risk elements acceptable in relation to the importance of the transaction?

Yes

No

Prepare the offer or the final negotiations

Find new alternatives for a lower risk level