

CE29x Team-Project Challenge

Risk Management

Professor Anthony Vickers

Room: INW.3.17

e-mail: vicka

with acknowledgements to Michael Fairbank, Keith Primrose and Adaptavist

Partly based on material from: Frode L. Ødegård, Ødegård Labs Inc.

Definition

Risk Management:

“Is a formal process in which risk factors are systematically identified, assessed, and mitigated.”

What is a risk?

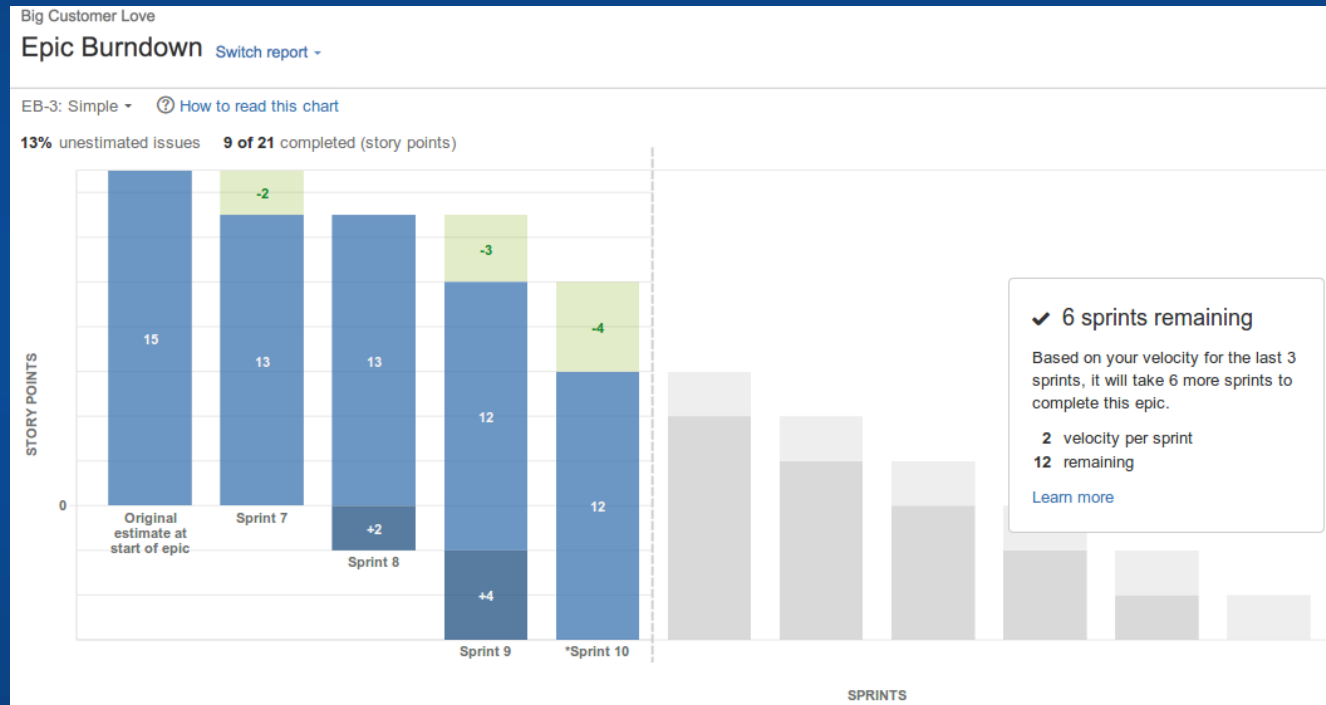
Risk: An uncertain event or set of events that if they were to occur, would have either a positive or negative impact on the project.

- Threats
- Opportunities

Q: Can you give examples of each of the above?

What Risks affect your group project?

What risks are associated with this diagram?



Why do projects go wrong - I?

Process reasons:

- * Inadequate understanding of customer needs
- * Poor requirements documents / management
- * Poor or no architecture/design
- * Build first and ask questions later
- * Poorly understood legacy design/components
- * No peer reviews to catch problems early
- * Ineffective testing - misses serious defects (e.g. caused by
Programmers vouching for their own work quality)

Why do projects go wrong - 2?

Product / Resource reasons:

- * Resource constraints / inadequate funding
- * Inexperienced or incapable personnel
- * Lack of domain expertise
- * Complex design
- * Poorly defined interfaces
- * Lack of appropriate tools

Why do projects go wrong - 3?

External risks:

- * TalkTalk customer database hacked in 2015
 - * 157000 customer records lost, including passwords, email address, possibly more
 - * TalkTalk received record fine £400,000 at the time
- * Regulations change – e.g. GDPR, Brexit
- * Denial of Service attacks are common
- * Patent trolls attack your new startup

Anatomy of a risk

- * Once a risk is identified, you need to consider:
 - * Probability of the occurrence of the risk
 - * The consequences - i.e. the size of the loss

Risk Exposure: Quantification

Risk Exposure = Probability x Consequence

Calculating Risk Exposure

Factor	Probability	Cost	Risk Exposure
Late delivery from vendor	0.25	28 days	7 days
Integration delay	0.6	15 days	9 days
Additional component testing needed, as there are 5% more components than first estimated	0.9	20 days	18 days
Test team report they may have to delay their work by 1 month	0.5	30 days	15 days
Total Risk Exposure	?	?	?

NB – You can't simply add these together, it depends on any relationships / dependencies between them

E.g. Additional component testing would be linked to the risk of requiring extra components that need developing.

Why quantify risk

- * Allows solution ideas to be evaluated more critically
- * Allows feedback on impact of risks we anticipated
- * Allows us to allocate resources to deal with risks
- * Allows us to determine whether a risk is acceptable

Recording a risk into Jira

Create risk issue like any normal issue.

Give it a:
Summary
Description
Likelihood and
Impact

The screenshot shows a Jira issue creation form. At the top, the 'Issue Type' is set to 'Risk'. Below this, the 'Summary' field contains the text 'Rollout of new operating system could cause existing code to break'. The 'Description' field is a rich text editor with a toolbar showing options for bold, italic, underline, text color, background color, link, unlink, list, and more. The description text reads: 'The company is scheduled to install windows 11 to all client machines in February. This might break the current code which was only written and tested for windows 10.' At the bottom, the 'Likelihood' is set to 'Likely' and the 'Impact' is set to 'Major'.

Issue Type* Risk

Summary* Rollout of new operating system could cause existing code to break

Description

Style **B** *I* U A [^]

The company is scheduled to install windows 11 to all client machines in February.
This might break the current code which was only written and tested for windows 10.

Visual Text

Likelihood Likely

Impact Major

Recording a risk into Jira

Issue Type* Risk

Summary* Rollout of new operating system could cause existing code to break

Description

Likelihood

- None
- None
- Rare
- Unlikely
- Possible
- Likely
- Certain

Impact

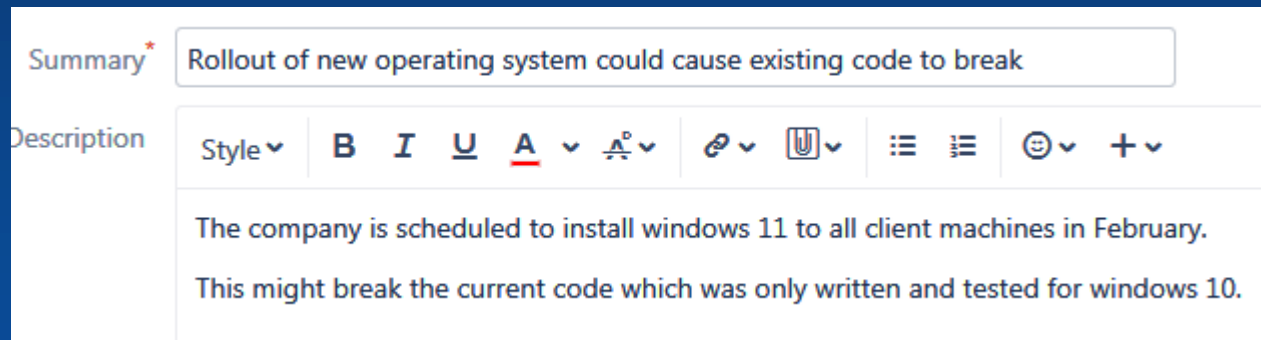
- None
- None
- Insignificant
- Minor
- Moderate
- Major
- Catastrophic

Likelihood Likely

Impact Major

Risk exposure=Likelihood×Impact

Recording a risk into Jira



The screenshot shows a Jira issue form. The 'Summary' field contains the text 'Rollout of new operating system could cause existing code to break'. The 'Description' field contains two paragraphs: 'The company is scheduled to install windows 11 to all client machines in February.' and 'This might break the current code which was only written and tested for windows 10.' The form includes a rich text editor toolbar with options for bold, italic, underline, text color, background color, link, unlink, bulleted list, numbered list, smiley, and a plus sign for more options.

Risk exposure=Likelihood×Impact

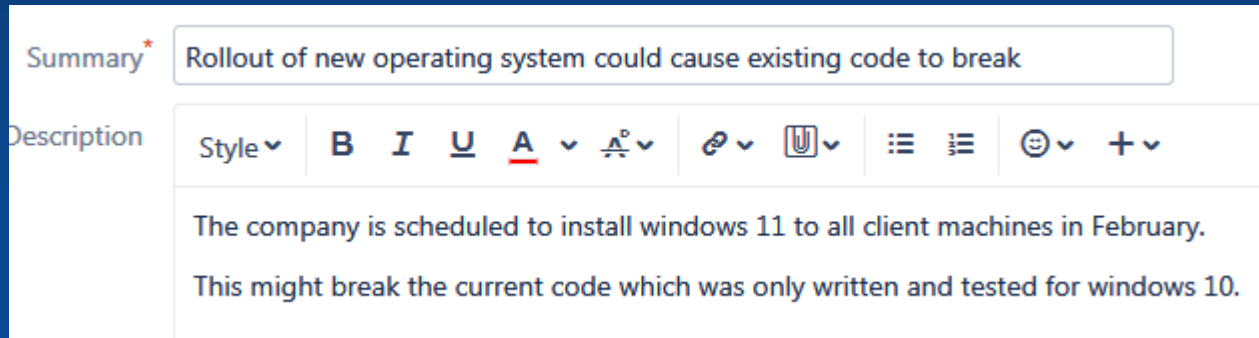
For this particular risk, how might we lower the exposure?

To lower the likelihood?

To lower the Impact?

NB – Prevention of the risk also costs resources

Recording a risk into Jira



The screenshot shows a Jira issue form. The 'Summary' field contains the text 'Rollout of new operating system could cause existing code to break'. The 'Description' field contains two paragraphs: 'The company is scheduled to install windows 11 to all client machines in February.' and 'This might break the current code which was only written and tested for windows 10.' The form includes a rich text editor with various formatting options like bold, italic, underline, and link.

Summary* Rollout of new operating system could cause existing code to break

Description

The company is scheduled to install windows 11 to all client machines in February.
This might break the current code which was only written and tested for windows 10.

Risk exposure=Likelihood×Impact

- * Add comments / enhance description to describe progress on resolving the risk.
- * Leave risk in backlog until risk is resolved.
- * When the exposure is zero, the risk can be moved to Done.
- * For some risks, total resolution never happen until project is completed.

Risk Matrix

	Impact				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	Lowest	Low	Medium	Medium	High
Unlikely	Low	Medium	Medium	High	High
Possible	Medium	Medium	High	High	Highest
Likely	Medium	High	High	Highest	Highest
Certain	High	High	Highest	Highest	Highest

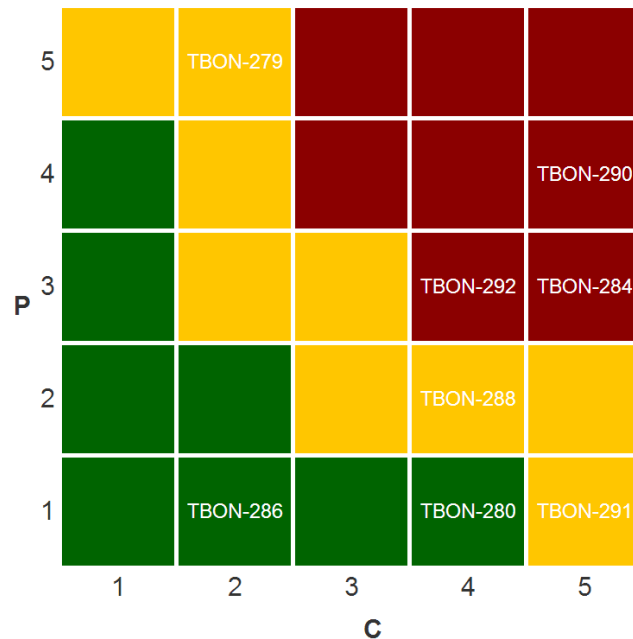
* The qualitative exposure of a particular risk can be viewed on this matrix.

Q: According to this matrix, what is the exposure of a risk with “Likelihood: Possible” and “Impact: Major”?

Recording a risk into Jira

Some plugins (paid for) give an overview of all current outstanding risks:

Updated: 23/dec/13 10:26 AM (TBON-292) | Issues:8 | Red issues:3 | Yellow issues:3 | Green issues:2

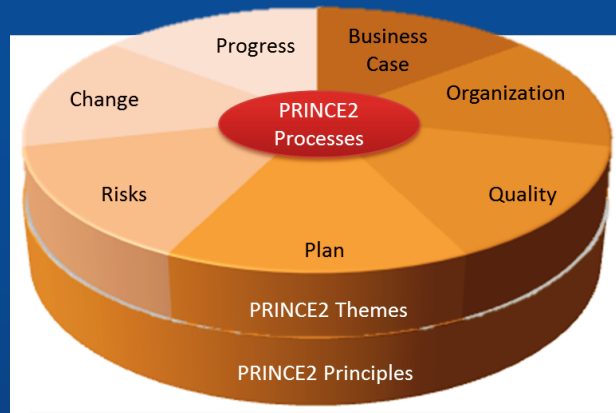


Q: Which Issue has the highest exposure here?

Formal Risk Management

Formal Risk Management

- * **PRINCE2** (**PR**ojects **IN** Controlled **E**nvironments) is a project management methodology which includes standards for best practice in project management topics, including risk.



Formal Risk Management

- * The UK Government's Central Computer & Telecommunications Agency (CCTA) promoted a number of mandatory methodologies such as PROMPT, PRINCE and CRAMM.
- * CRAMM stands for the CCTA Risk Assessment Management Method.
- * The CCTA was part of the Office of Government Commerce, now closed. Is there any current UK Government oversight?

The risk management process

1. Risk identification

- * Identify project, product and business risks

2. Risk analysis

- * Assess the likelihood and consequences of these risks

3. Risk planning

- * Draw up plans to avoid or minimise the effects

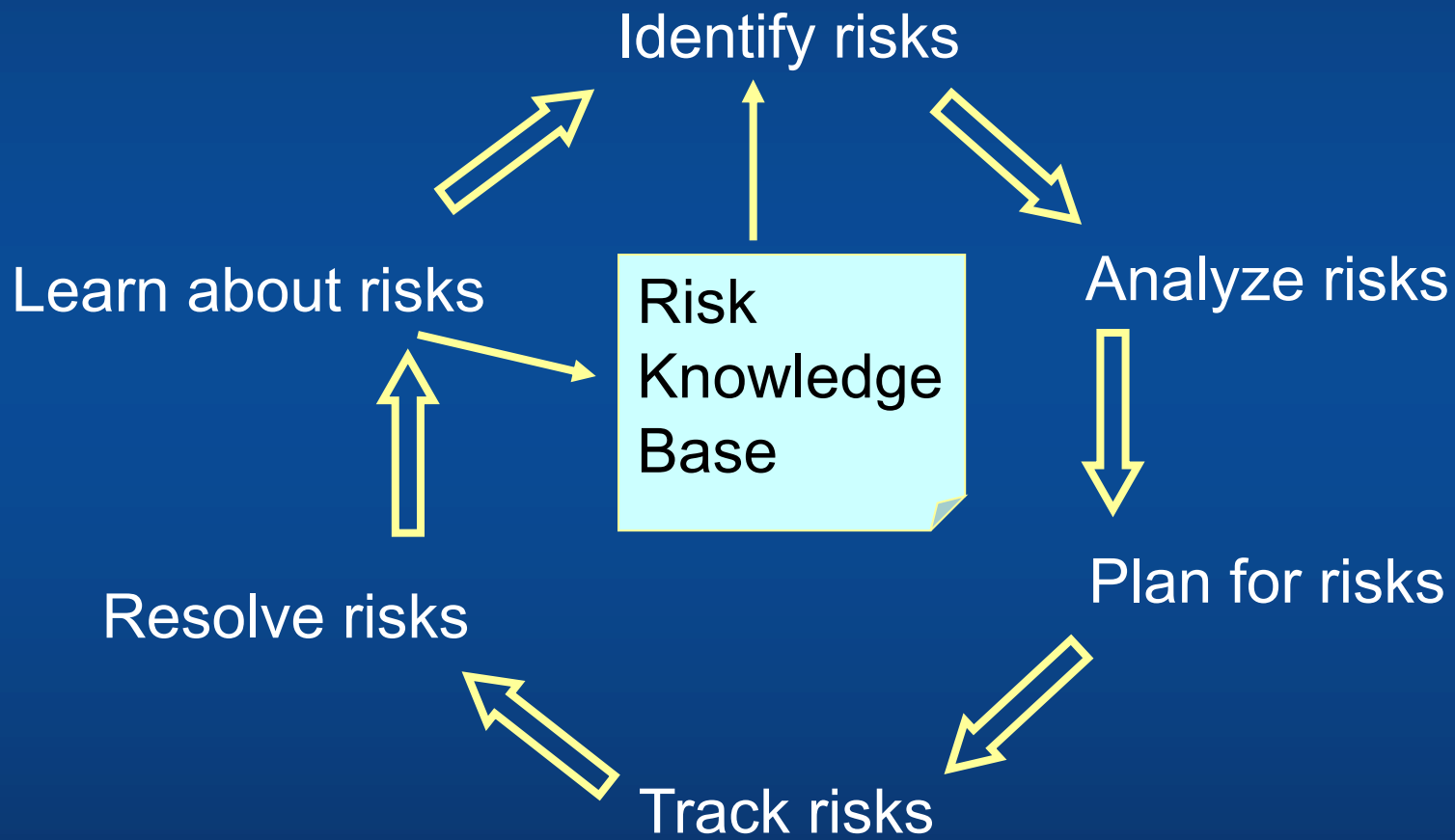
4. Risk monitoring

- * Monitor the risks throughout the project
- * Communicate status to stakeholders

5. Resolution

- * Implement the contingency plans

Risk management process



I. Risk identification

- * Technology risks
- * People risks
- * Organisational risks
- * Requirements risks
- * Estimation risks

Q: Suggest some examples of each of these (e.g. for your CE29x group project)

Identification: Communication

Notify all affected stakeholders:



- * Customers
- * Project / Program Manager
- * Team Members
- * Management
- * Marketing
- * Sales
- * Customer Support
- * Finance
- * Quality Assurance
- * ...

Identification: Documentation

Each risk you identify can require documenting separately:

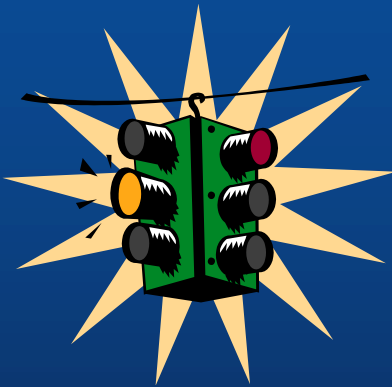
Header	Project	<i>Name of project</i>
Assessment	Date	<i>Date of entry</i>
Action Plan	Risk name	<i>Name of risk</i>
Tracking	Risk category	<i>Type of risk</i>
Resolution	Probability	<i>Likelihood of occurrence</i>
	Consequence	<i>Severity of impact</i>
	Originator	<i>Who reported this risk</i>
	Phase/activity	<i>Where in process</i>
	WBS Element	<i>WBS relationship</i>

NB: This is repeated for every identified risk

Adapted from *Managing Risk: Methods for Systems Development* by Elaine M. Hall, Addison-Wesley 1998

2. Risk analysis

- * Assess seriousness of each risk from previous Risk Exposure calculation
- * Risk effects might be catastrophic, serious, tolerable or insignificant
- * Some organisations use a traffic light coding:



Red:	Major risk – must be addressed
Amber:	Minor risk – should be addressed
Green:	Negligible risk – fix if time allows

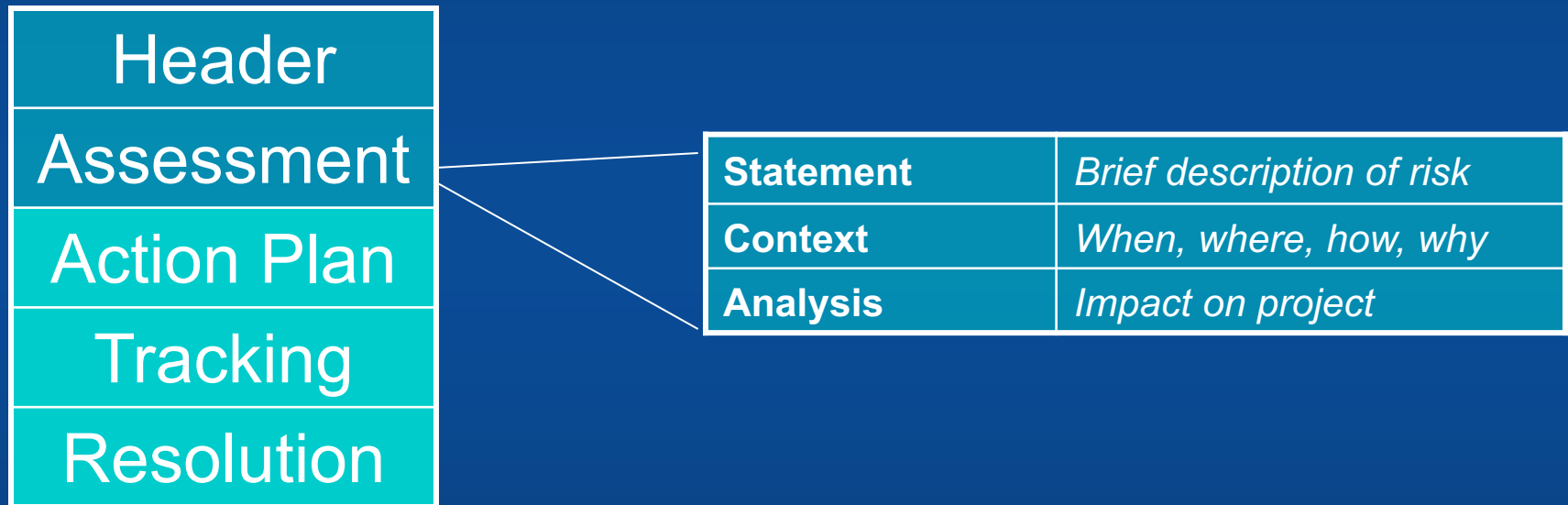
Analysis of risks: Questions

- * How severe is the consequence?
- * How likely is the occurrence?
- * Is the risk exposure acceptable?
- * How soon must the risk be dealt with?
- * What is causing the risk?
- * Are there similarities between risks?
- * Are there dependency relationships?

Analysis of risks: Activities

- * Grouping
 - * Eliminate redundant risks
 - * Combine related risks
 - * Link dependent risks
- * Determining risk drivers
 - * Underlying factors that affect severity of consequence
 - * May affect estimation of probability, consequence, risk exposure
 - * Increases understanding of how risks can be mitigated
- * Ranking
 - * Order of likelihood, consequence, exposure, time frame
- * Determining root causes (sources of risk)
 - * Old-fashioned root cause analysis
 - * What events are capable of causing the risk to occur?
 - * Identify common root causes

Analysis: Documentation



Snapshot from a Risk Management database (kindly given by Capita)

Risk Reference	Date Raised	Risk title	Risk Description & Impact	Next Review Date	Risk Probability	Risk Impact	Gross Risk Rating	Risk response	Mitigating actions including dates	Risk Status	Date closed
Cdiv R403	06/08/2015	Code Management	Risk that code is not retrofitted for every release (all development teams). Impact would be that the code being tested would not be on latest code release and therefore causes regression meaning additional time & cost.	29 May 16	3	3	9	Avoid	17/08 - review with development teams & publish delivery schedule 06/10 - Approach for code management distributed, awaiting agreement risk now mitigated by new code approach. 9/11: GY to review with suppliers 14/12 - AE to chase RB for governance proposal 15/02: Continue to monitor bundles from suppliers 04/04: Continue to Monitor	Open	
Cdiv R417	07/10/2015	Infrastructure	there is a risk that the rollout of windows 7 laptops to the programme team results in a delay to development and testing which could lead to increasing costs and timelines	29 May 16	3	4	12	Accept	07/10 - in the event that first recipients cannot access required systems, we will request delay to programme rollout 19/10: users will be keeping their existing laptops therefore reducing impact of down time 9/11: new laptops for majority of team not expected until 2016 18/01: Continue to monitor 04/04: Further laptops being rolled out to the team over the next 2 weeks, monitor impact 18/04: Risk reduced 05/05: Continue to monitor	Open	
Cdiv R418	16/10/2015	Test Environments	There is a risk that we are unable to refresh the contract engine test databases in preparation for Policy Enquiry UAT which could increase the number of queries being raised through testing due to out of date data.	.	3	3	9	Avoid	Life - Activities in place to provide connectivity to test environment DB2T which is currently not being used by any other projects. IBM - Establishing point of contact for the refreshing of the 01AM environment. Also liaising with Bristol CDC team to understand impact to inflight and plan projects. 19/10: work under way to establish connectivity to DB2T target date for completion 23rd Oct. Trying to establish point of contact to refresh IBM environments 9/11: process now in place for refresh of IBM databases and DB2T environment created and tested. Close.	Closed	09/11/2015
Cdiv R419	19/10/2015	Resources	There is a risk that the decision to send onshore developers offshore will result in increased defects and extend timeline and cost of project	.	3	4	12	Reduce	19/10: to implement regular communication checkpoints and review of defect levels 23/11 - not seeing any impact following this decision, continue to monitor 14/12 - No issues since developers moved offshore, close	Closed	14/01/2016
Cdiv R438	02/02/2016	Manage Customer Details Timeline	There is a risk that the level of outstanding consolidated view defects will impact delivery timeline for Manage Customer Details resulting in increased costs and reduced benefits		3	3	9	Avoid	02/02: AE to look at financial impact of retaining resource to assist defect fixing 15/02: Consolidated view targeted for production this week, close upon implementation 29/02: Close	Closed	29/02/2016

Risk Description & Impact

Risk that code is not retrofitted for every release (all development teams), Impact would be that the code being tested would not be on latest code release and therefore causes regression meaning additional time & cost.

there is a risk that the rollout of windows 7 laptops to the programme team results in a delay to development and testing which could lead to increasing costs and timelines

There is a risk that we are unable to refresh the contract engine test databases in preparation for Policy Enquiry UAT which could increase the number of queries being raised through testing due to out of date data.

There is a risk that the decision to send onshore developers offshore will result in increased defects and extend timeline and cost of project

There is a risk that the level of outstanding consolidated view defects will impact delivery timeline for Manage Customer Details resulting in increased costs and reduced benefits

* So why do Capita
bother keeping this log?

3. Risk planning

- * Consider each risk and develop a strategy to manage that risk
- * Avoidance strategies
 - * The probability that the risk will arise is reduced
- * Minimisation strategies
 - * The impact of the risk on the project or product will be reduced
- * Contingency plans
 - * If the risk arises, contingency plans are plans to deal with that risk

Planning: Resolution Strategies

- * Risk Avoidance
 - * Prevent the risk from occurring, reduce probability to zero
- * Risk Protection
 - * Reduce the probability and/or consequence of the risk before it happens
- * Risk Reduction
 - * Reduce the probability and/or consequence of the risk after it happens
- * Risk Research
 - * Obtain more information to eliminate or reduce uncertainty
- * Risk Reserves
 - * Use previously allocated schedule or budget slack
- * Risk Transfer
 - * Rearrange things to shift risk elsewhere (to another group, for example)

Q: Is this last strategy an acceptable practice?

Planning: Activities

- * Specify scenarios
 - * How would we be able to tell it is really happening?
- * Define quantified threshold for early warning
 - * What to monitor, when we consider the risk to be happening
- * Select resolution approach
 - * What has the best Return on Investment?
- * Specify risk action plan
 - * Document decisions

4. Risk Monitoring / Tracking

- * Monitor risk scenarios
 - * Watch for signs of a risk scenario occurring
- * Compare indicators to trigger conditions
 - * Watch indicator metrics – do they meet trigger conditions?
(E.g. triggers whenever we get more than 2 days behind schedule on the Gantt chart)
- * Notify stakeholders
 - * Let stakeholders know the risk is happening; execute action plan
- * Collect statistics
 - * Useful for next project you manage
 - * Update a risk database (these list what has gone wrong in previous IT projects; e.g. see “PERIL database”)

Planning/Tracking: Documentation

Header	
Assessment	Scenario
Action Plan	Indicator
Tracking	Trigger condition
Resolution	Checkpoint
	Resolution strategy
	Action plan

<i>What would happen?</i>
<i>Metric to be monitored</i>
<i>Value indicating risk scenario</i>
<i>When/where to check metric</i>
<i>How we will handle the risk</i>
<i>Concrete action plan</i>

Adapted from *Managing Risk: Methods for Software Systems Development* by Elaine M. Hall, Addison-Wesley 1998

5. Resolution

- * Execute action plan
 - * Improvise, adapt, overcome
- * Provide continuous updates
 - * Let stakeholders know your progress in resolving the risk
- * Collect statistics
 - * Update risk database with solution

Resolution: Documentation

Header
Assessment
Action Plan
Tracking
Resolution

Design Engineer	<i>Signature</i>
Quality Engineer	<i>Signature</i>
Project Manager	<i>Signature</i>
Marketing Manager	<i>Signature</i>

6. Learning from risks

* Post mortem:

- * What were the unanticipated risks?
- * What was the actual severity of consequence?
- * What resolution strategies worked well / not so well?
- * What types of risks could we
 - * prevent or transfer?
 - * protect ourselves from or reduce?
 - * handle only by allocating reserves?

* Action:

- * What are the preventative measures we can take in the future?
- * Are there significant vendor / partner performance problems?
- * What can we share with other project teams?

PRINCE2 Risk Log

* Try to complete the PRINCE2 Risk Log for the following risks that might affect your group project:

1. Underestimation of task durations, causing late delivery
2. People risk: 2 team members are sick / refuse to turn up in the final 2 weeks of delivery.
3. Technology risk: Any of your choice, e.g. cseegit server fails
4. A requirements risk: Your user-requirements do not pin down the exact requirements, and the customer refuses to accept your final product.

Summary

- * Risks to project exist and can be disruptive
- * Formal methods exists for assessing, documenting and mitigating these risks.
- * As a project manager or team member, you should be aware of these methods and issues

Further Reading

- * PRINCE2:

- * Risk Log Template document on Moodle

- * PRINCE2 course on Moodle (LinkedIn Learning)

- * Fundamentals of Project Management : Managing Risk in Projects, by D. Hillson and D. Dalcher

Further Reading

- * Quiz: Risk Management – just 5 simple questions
- * Quiz: Critical Path Analysis 2 – slightly harder
- * Next lecture: Communications followed by a guest presenter giving you their insight into project management in their company