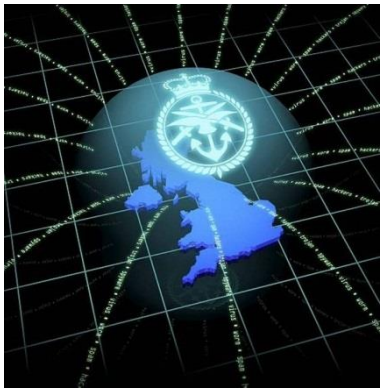
Developing an integrated approach to the analysis of MOD cyber-related risks

Colette Jeffery, James Tate - Defence Science Technology Laboratory

COST Expert Judgement Meeting - 12 to 14 October 2016

Overview

1. Dstl and risk research
2. Customer requirement
3. Overview of risk management process
4. Risk assessment methodology review
5. Evidence assessment
6. Future work
7. Conclusions



Dstl

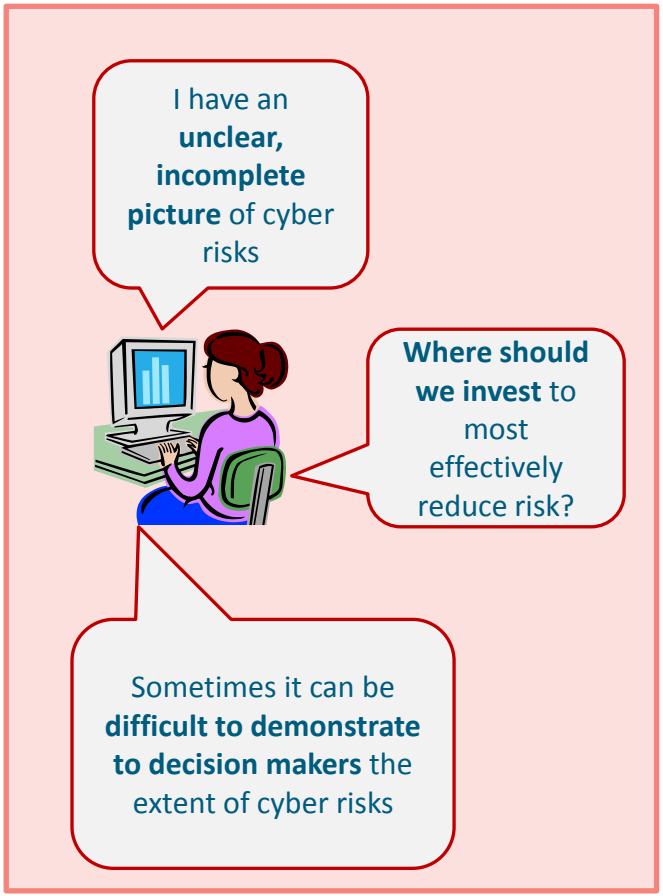
- Dstl is part of the Ministry of Defence (MoD)
- It provides sensitive and specialist services, advice, analysis and assurance to customers across government
- **The Cyber Enterprise Risk project was requested by Cyber Joint User (within Joint Forces Command)**

Customer Requirement

To develop an evidence-based approach that:

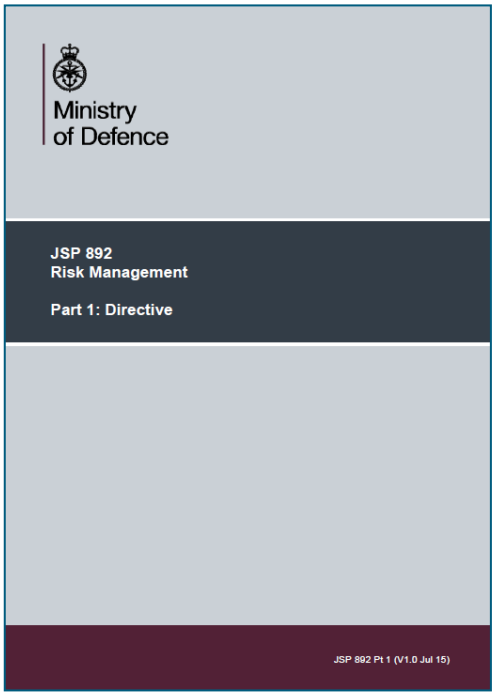
- informs Capability Planning on the likely risk from cyber threats
- advises on the level of investment required to reduce this risk to an acceptable level

To provide articulation of Cyber Risk at Defence Board level in a meaningful and consistent form with other Risks reported



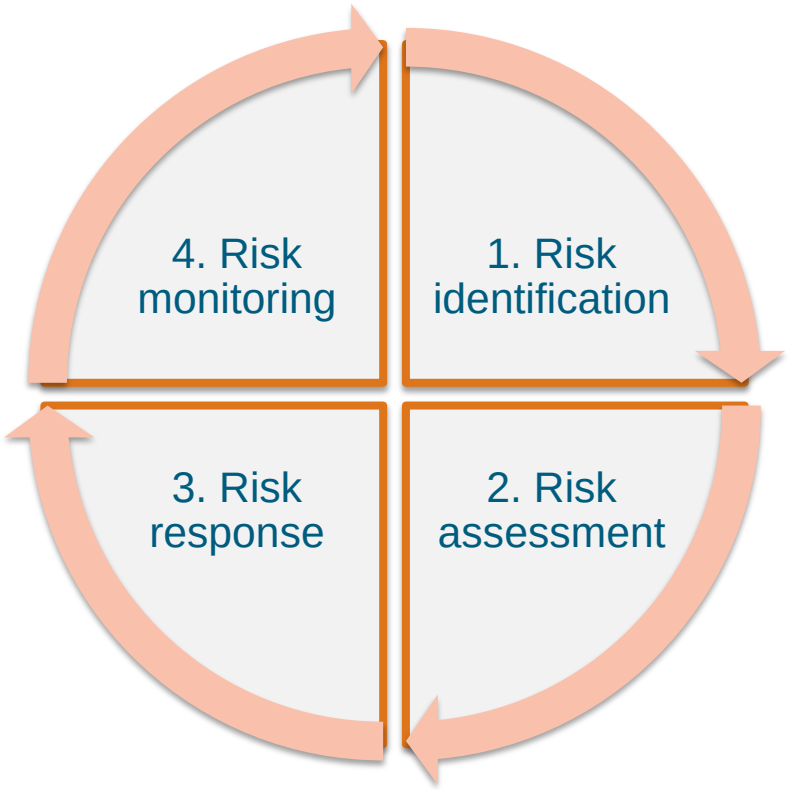
Dstl Input

- A **process** which captures and assesses strategic-level cyber-related risks; informing Defence Board risk management
- Generated a **standardised approach to assess the impact and likelihood** of these risks using mandated policy on Risk Management
- Authored a **Statement of Requirement** to inform the development of a pan-MOD cyber risk management tool



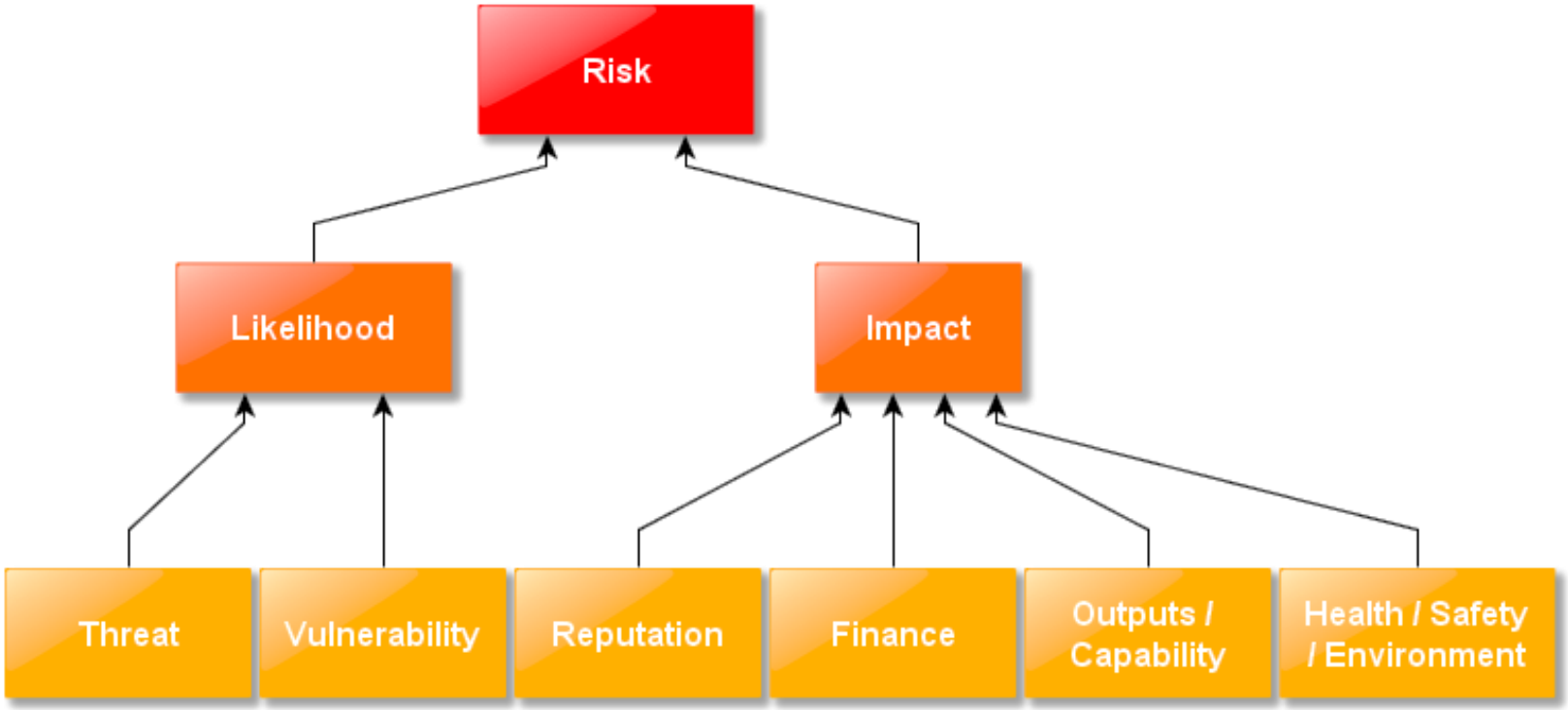
Joint Service Publication (JSP) 892 on Risk Management

Risk Management Process



1. Risk identification: Through Dstl technical assessments
2. Risk assessment: Follows MOD policy (JSP 892); involves expert elicitation workshops and analysis
3. Risk response: Conducted by the Risk Owners to determine which risks require new or further management action
4. Risk monitoring: Conducted by the Risk Owners / Risk Management Boards to detect changes in risk status, ensure responses are effective etc.

Modified JSP Measure of Risk



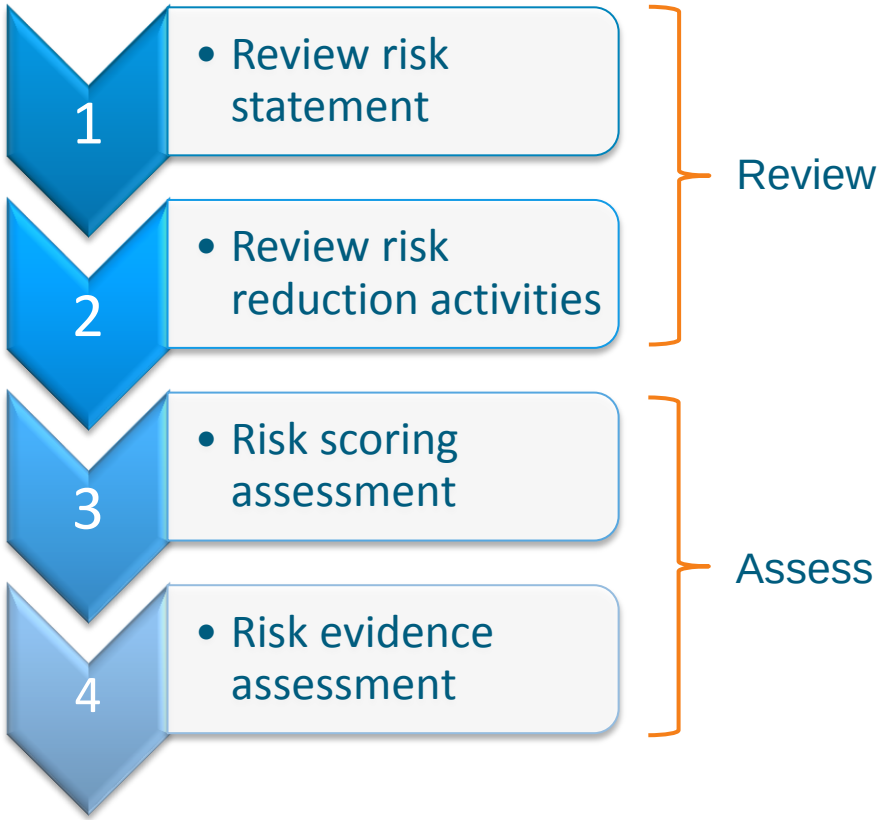
Risk Assessment Workshops

Workshops aim to review and score the risks such that they may be presented to decision makers.

Attended by Subject Matter Experts (SMEs) and a facilitator. SMEs use a mixture of their tacit knowledge and available evidence to score the risks:

- Provide a three point estimate for risk impact
- Provide a single score for vulnerability

Final scoring reached by group consensus



Key Questions

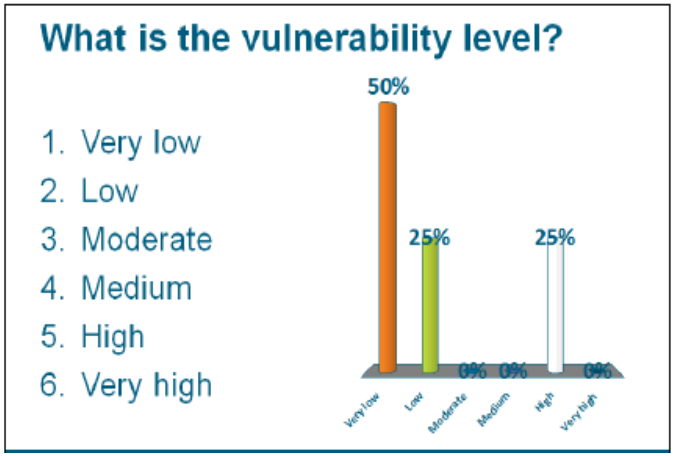
1. How could we improve the elicitation process in the risk assessment workshops?

2. How can we help decision makers to understand the level of confidence they should place in the risk scores?

1 Impact Elicitation Techniques: Electronic Voting

What is the **vulnerability** level for Risk A?

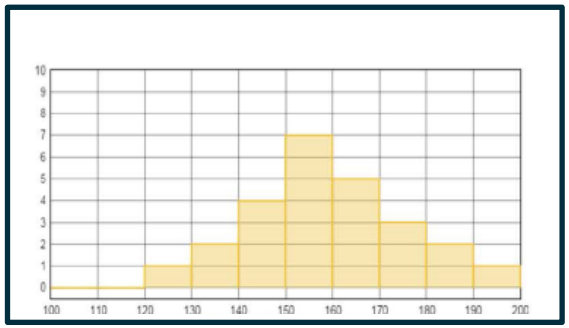
Person A = 1 (Very low)



Fictitious Data

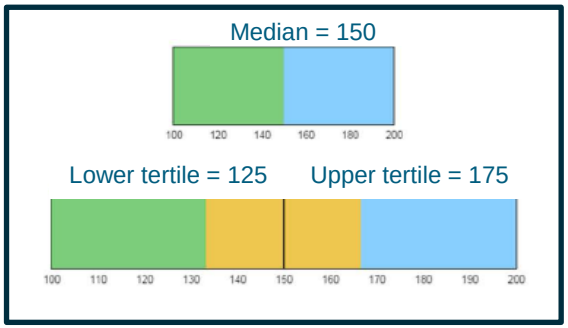
1 Impact Elicitation Techniques: MATCH

A web based version of the Sheffield University Elicitation Framework (SHELF) R script



Trial Roulette

Quartile



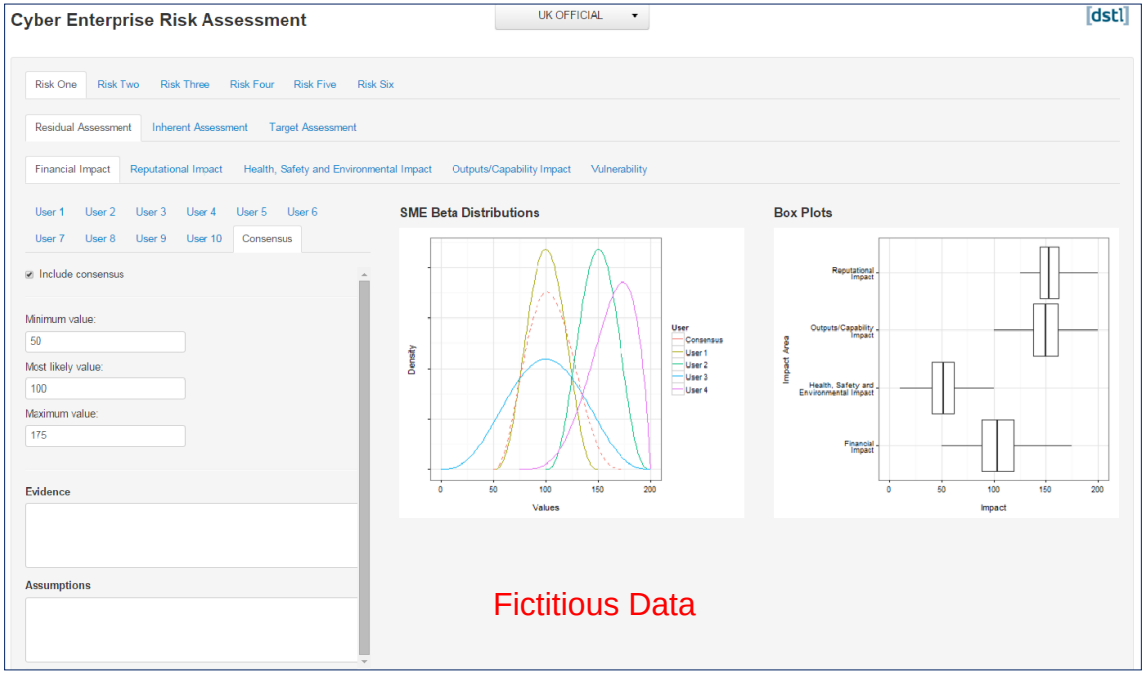
Tertile

David Morris, Jeremy Oakley, John Crowe, A web-based tool for eliciting probability distributions from experts, Environmental Modelling & Software, Volume 52, 2014

http://optics.eee.nottingham.ac.uk/match/uncertainty.php

Impact Elicitation Techniques: R Shiny Interface

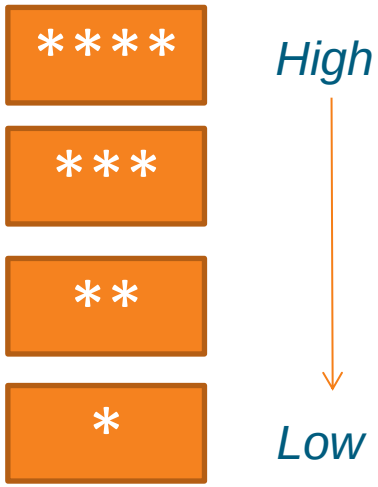
- Used to support risk workshops
- Record min, max & modal scores for each impact area
- Capture input from multiple stakeholders
- Export data for analysis in Excel



Evidence Elicitation Techniques: Star Assessment

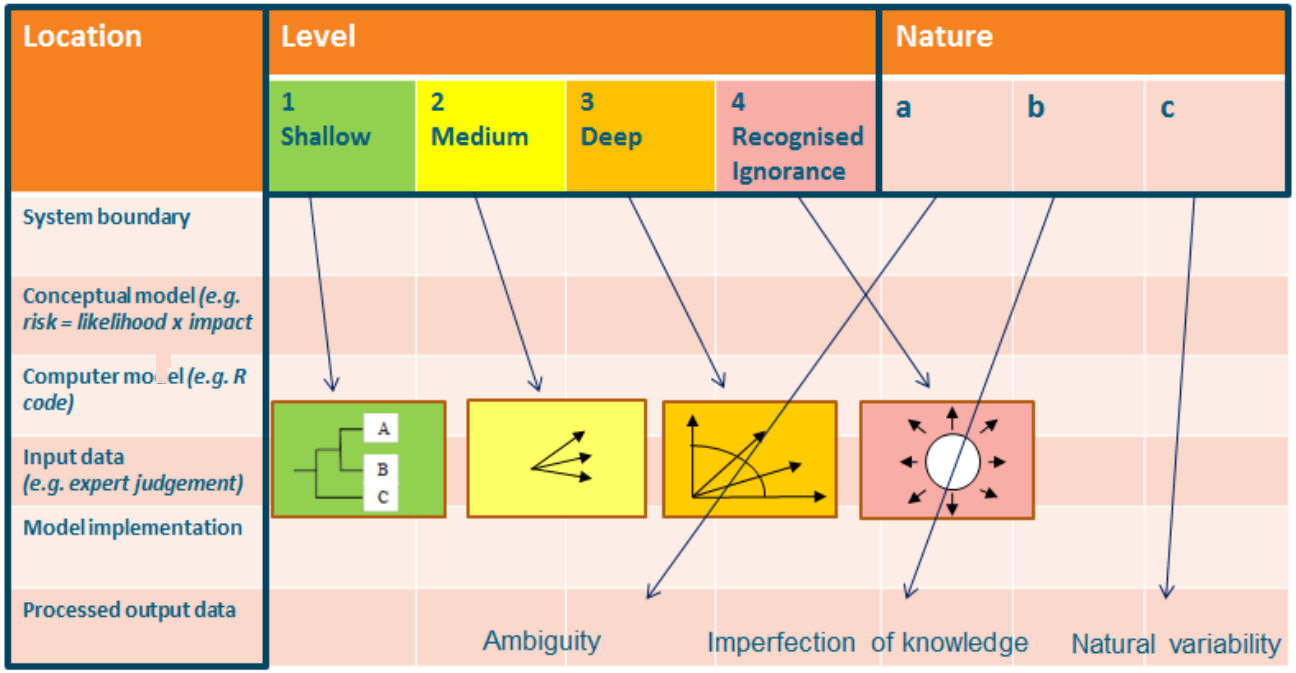
Consider:

- How well do we understand the process?
- How confident are we in the analysis?
- To what extent could new evidence change our assessment?



David Spiegelhalter, University of Cambridge, Communicating risk and uncertainty to policy-makers and the public., Calculating and Communicating Uncertainty Conference, 27-28 January 2015
http://www.southampton.ac.uk/~ccu2015/presentations/spiegelhalter.pdf

Evidence Elicitation Techniques: Walker Uncertainty Model



Jan Kwakkel, Warren Walker and Vincent Marchau, Classifying and communicating uncertainties in model-based policy analysis, Int. J. Technology, Policy and Management, Volume. 10, No. 4, 2010

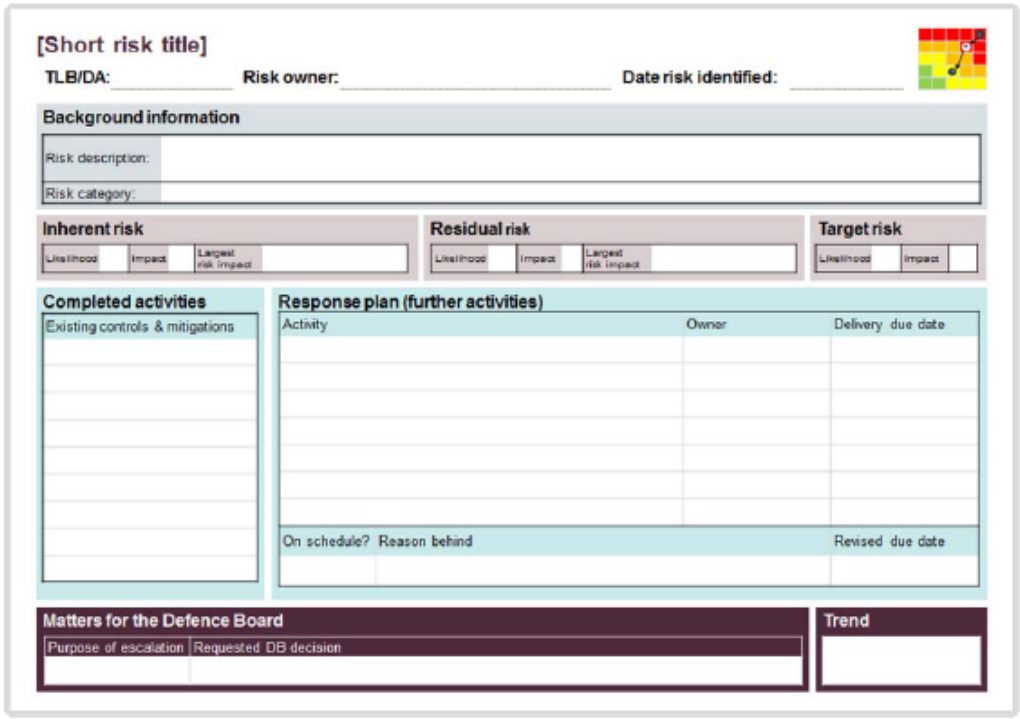
2 Evidence Elicitation Techniques: Italian Flag

- Experts select a number from 1 to 6 for each assessment they have made (impact / vulnerability)
- Easy to visually interpret

1	2	3	4	5	6
Strong supporting evidence	Weak supporting evidence	Little / no evidence either way	External events could easily change assessment	Weak conflicting evidence	Strong conflicting evidence

JSP 892 Template: CER Output

- Two-page risk summary



[Short risk title]

TLB/DA: Risk owner: Date risk identified:

Background information

Risk description:

Risk category:

Inherent risk — Likelihood | Impact | Largest risk impact

Residual risk — Likelihood | Impact | Largest risk impact

Target risk — Likelihood | Impact

Completed activities

Existing controls & mitigations

Response plan (further activities)

Activity	Owner	Delivery due date

On schedule? Reason behind Revised due date

Matters for the Defence Board

Purpose of escalation	Requested DB decision

Trend

JSP 892 – Extended Page

- Aim for consistent reporting of risk detail

- Extended to present more risk data:
  - Reasons behind risk scorings
  - Probability distribution from CER process
  - Likelihood, vulnerability and threat elements articulated explicitly
  - Evidence assessments

[Short risk title] Fictitious Data

Further information

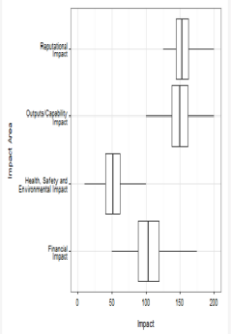
Context / Evidence

Context:
Internet connected systems are vulnerable to external intrusion through the exploitation of known vulnerabilities that have not been fixed.

Evidence:
Internal systems security audit (InfoSecAudit#001) determined internet-connected systems vulnerable to external intrusion due to lack of patching against known software vulnerabilities.

Impact	CRITICAL	
Area	Score	Reason
Financial	Major	Reasonable financial penalties levied against the organisation.
Reputation	Critical	Reputation assessed to be likely seriously damaged due to lack of adherence to industry best-practice.
Outputs / Capability	Minor	Limited damage to mission-critical systems.
HS&E		Not assessed.

Impact Probability Distributions



Vulnerability High

- Lots of vulnerabilities

Threat Source	Hackers
Network Attacks	
SIGNIFICANT	

- Lack of sufficient patch management causes internet-connected systems to be exposed to external hackers.

Evidence assessment

Impact: Reputational

Weak supporting evidence

Fictitious Data

Future work

Dstl | Requirement | Risk management | Risk assessment | Evidence assessment | **Future work**

Risk Linkages Research

Aim

- To investigate the **relationships between risk data** (Risks, Activities, Evidence) to develop MODs understanding of its ‘risk picture’

Key Research Questions to Investigate

- What are the key cyber risk response activities?
- Which activities currently underpin our residual risks?
- What level of evidence (confidence, provenance etc.) do we have to support each risk and activity?
- How, and to what extent, do the planned activities enable the residual risk positions to move toward the target risk positions, and over what time periods?
- What would a data schema for cyber risk management look like?

External Research Proposal

Aim

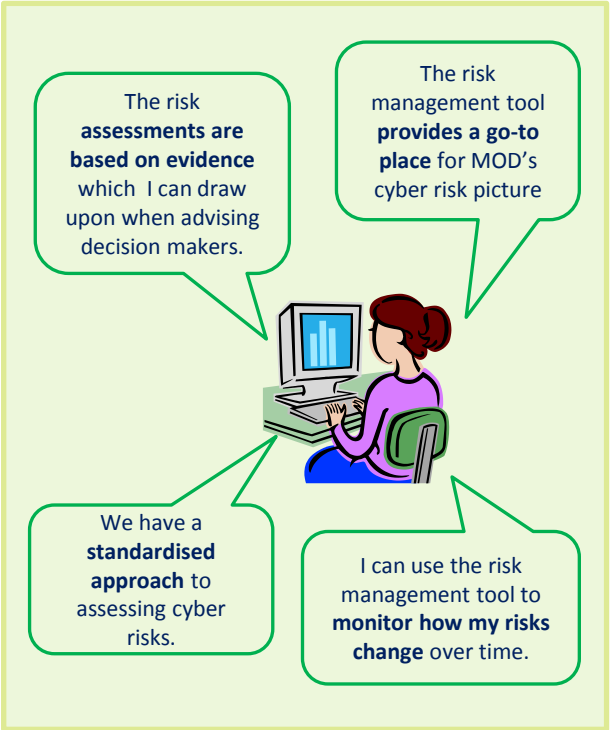
- Collect & collate data articulating the **financial impact of cyber incidents**, where those incidents have direct relevance to UK MOD.

Key activities

- The collection of financial (in UK monetary terms) impact data for cyber incidents
- The collation and categorisation of evidence based on these collated data (and input from Dstl cyber SQEPs)
- The production of an evidence dataset (to agreed formats & standards), with any associated categorisation schemes.
- The production of a methodology for generating, and maintaining, a cyber financial impact dataset for MOD use.

Conclusions

- Developed a standardised approach for cyber-related risks
- Aligned to extant MOD risk management guidance
- Developed requirements for MOD risk management decision support tools
- Ongoing research to mature processes, tools, techniques, and integration with wider risk management activities



Questions?

Contact:

cjjeffery@dstl.gov.uk