Risky Business – Developing an Approach to Managing Technical Systemic Risks

Ian Gibson, Atkins
Glyn Duffield, retired
Michelle Holford, MOD DE&S
Jon Brooking, MOD DE&S

Overview

Context

The Nature of Systemic Risks

Understanding the Problem

Definition of Systemic Risks

An Approach for Technical Systemic Risk Management

Implementation of the Approach

Conclusions

Context

This material is based upon an investigation for the MOD Defence Functional Authority for Technical, Quality and Standardisation into managing Technical Systemic Risk that started in January 2020

Recognition that policy and guidance was needed in this area to enable effective management of risks that did not sit neatly within organisational boundaries (both the risks themselves and their mitigations)

Opportunity to define a cross-cutting approach that could be implemented across Defence

The Nature of Systemic Risks

Systemic Risk is well recognised within the financial sector

- When systemic financial risks manifest themselves, the results are hard to ignore
- “Systemic risk refers to the risk of a breakdown of an entire system rather than simply the failure of individual parts” [Systemic Risk Centre definition]

Systemic Risks are insidious

- They can build up over time
- Sometimes reflecting a build-up of residual risks which were never dealt with first time around
- Sometimes the result of multiple local mitigations to problems which ought to have been owned further up the chain
- Sometimes just reflecting repeating patterns of organisational behaviour
- Systemic risks require a systemic response

Definitions of “Technical”

MOD policy for Technical Governance and Assurance of Capability, JSP 901 Pt 1:

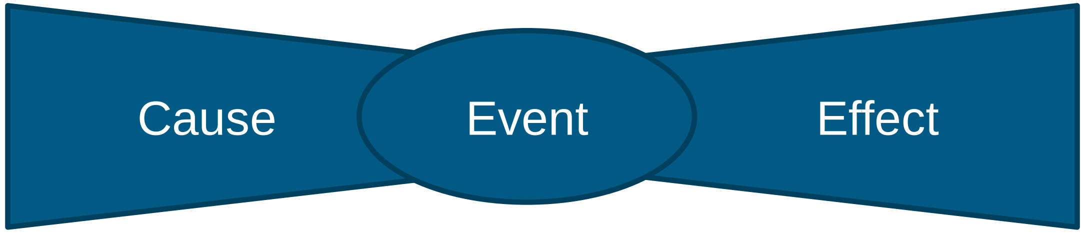
- The term ‘**Technical**’ should be considered to cover the broad range of professional, specialist, engineering, science, quality and related **disciplines** that enable Defence capability to be procured and supported safely and effectively across the capability lifecycle.
- This includes **people involved in a broad range of capability management activities** including solution maturation; requirements and acceptance; in-service support; P3M; and test and evaluation.

INCOSE SE Handbook v4 definition of Technical Risk:

- The possibility that a technical requirement of the system may not be achieved in the system life cycle. Technical risk exists if the system may fail to achieve performance requirements; to meet operability, producibility, testability, or integration requirements; or to meet environmental protection requirements. A potential failure to meet any requirement that can be expressed in technical terms is a source of technical risk.
- Technical risks should not be confused with project risks even if the method to manage them is the same. **Technical risks address the system itself, not the project for its development**. Of course, technical risks may interact with project risks.

Relationship to Risk Management

Risk Management typically follows a "Bow Tie" model where risks are categorised by where the cause of the risk is found



However, the nature of Systemic Risks is that the causes, events and effects can be interrelated so that a "non-technical" cause results in a "technical" effect

So Technical Systemic Risks are:

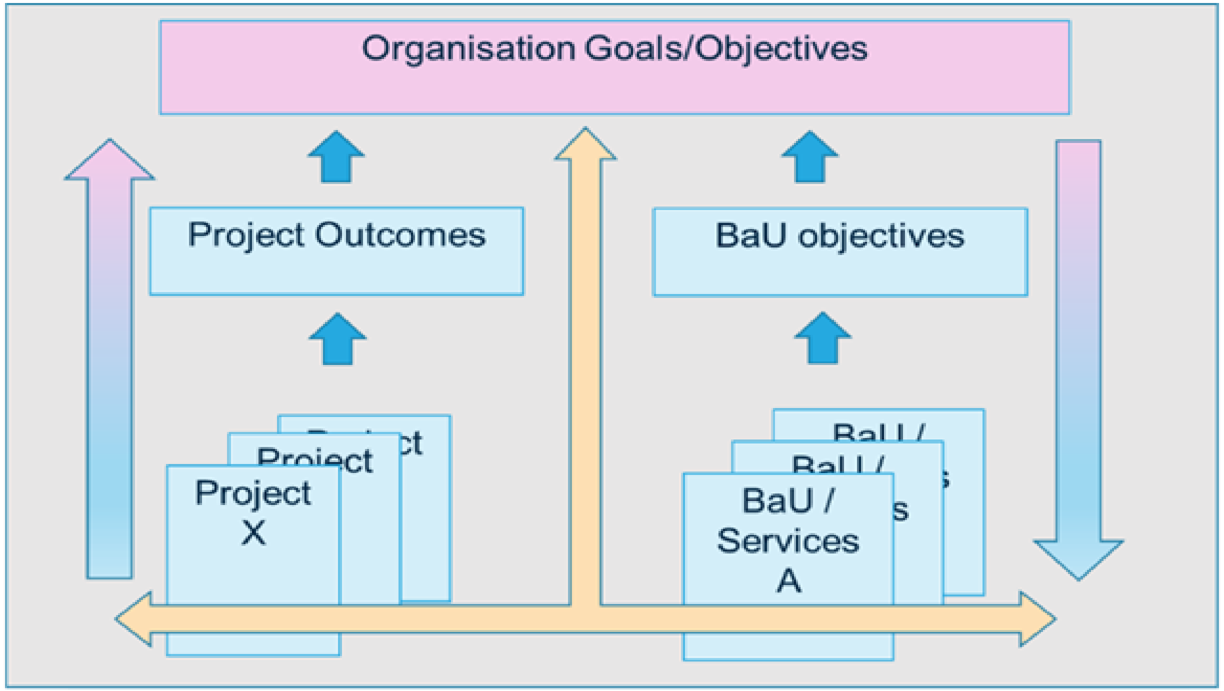
- Related to both the performance of technical engineered systems, and to the technical activities which develop and support them
- Amplified by interactions between interrelated elements across the socio-technical system leading to emergent effects which may be driven by feedback loops and unintuitive patterns

ATKINS Member of the SNC-Lavalin Group

Ministry of Defence

de&s

Understanding the Problem

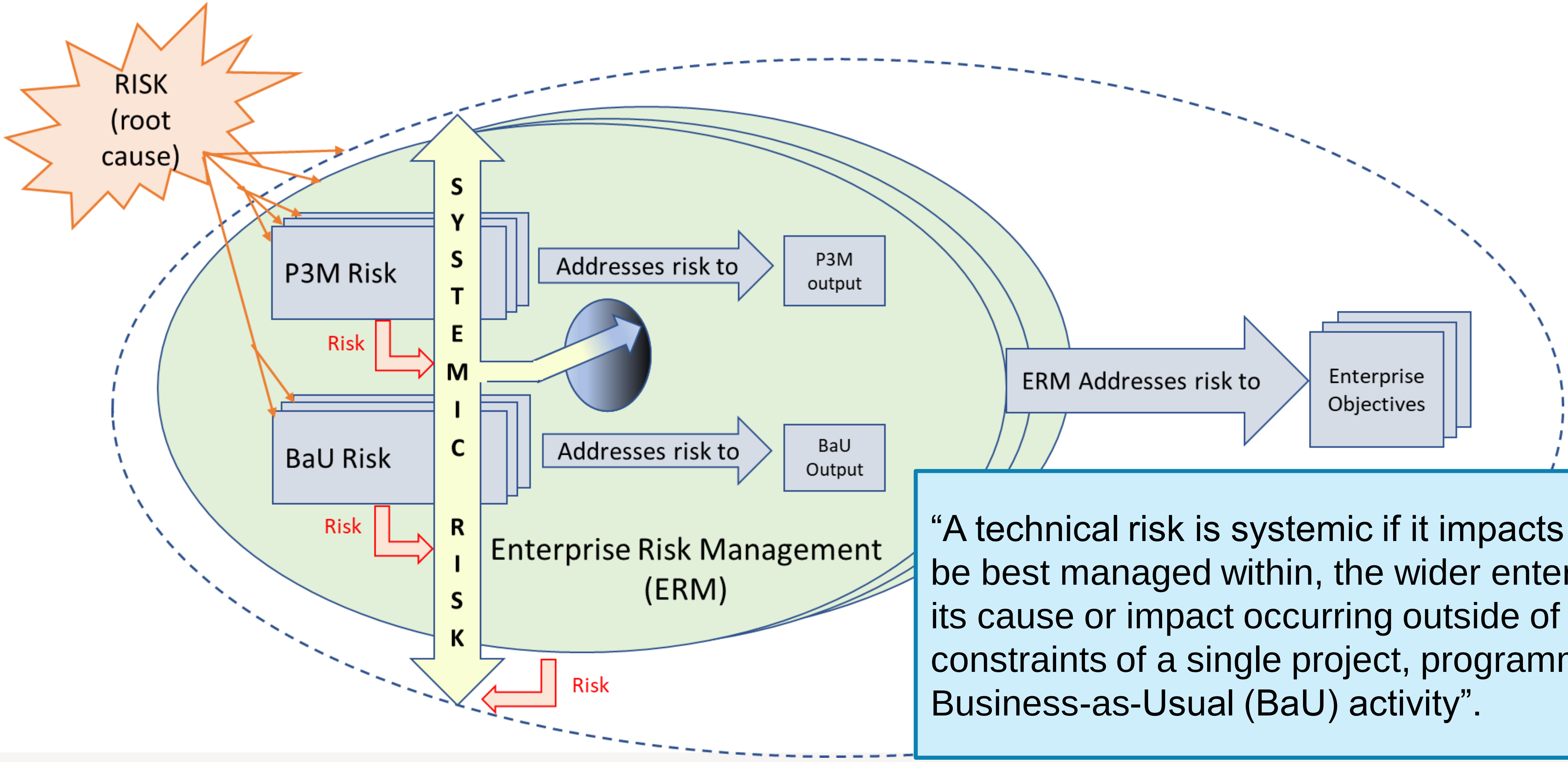


<u>P3M / Traditional</u>
What is the risk to delivery of my Project Outcomes / BaU Objectives? (Looks externally and upwards to escalate risks)

<u>Enterprise Risk Management</u>
What is the risk to delivery of my Organisation's Goals & Objectives?
(Looks inwardly and downwards to identify risks)

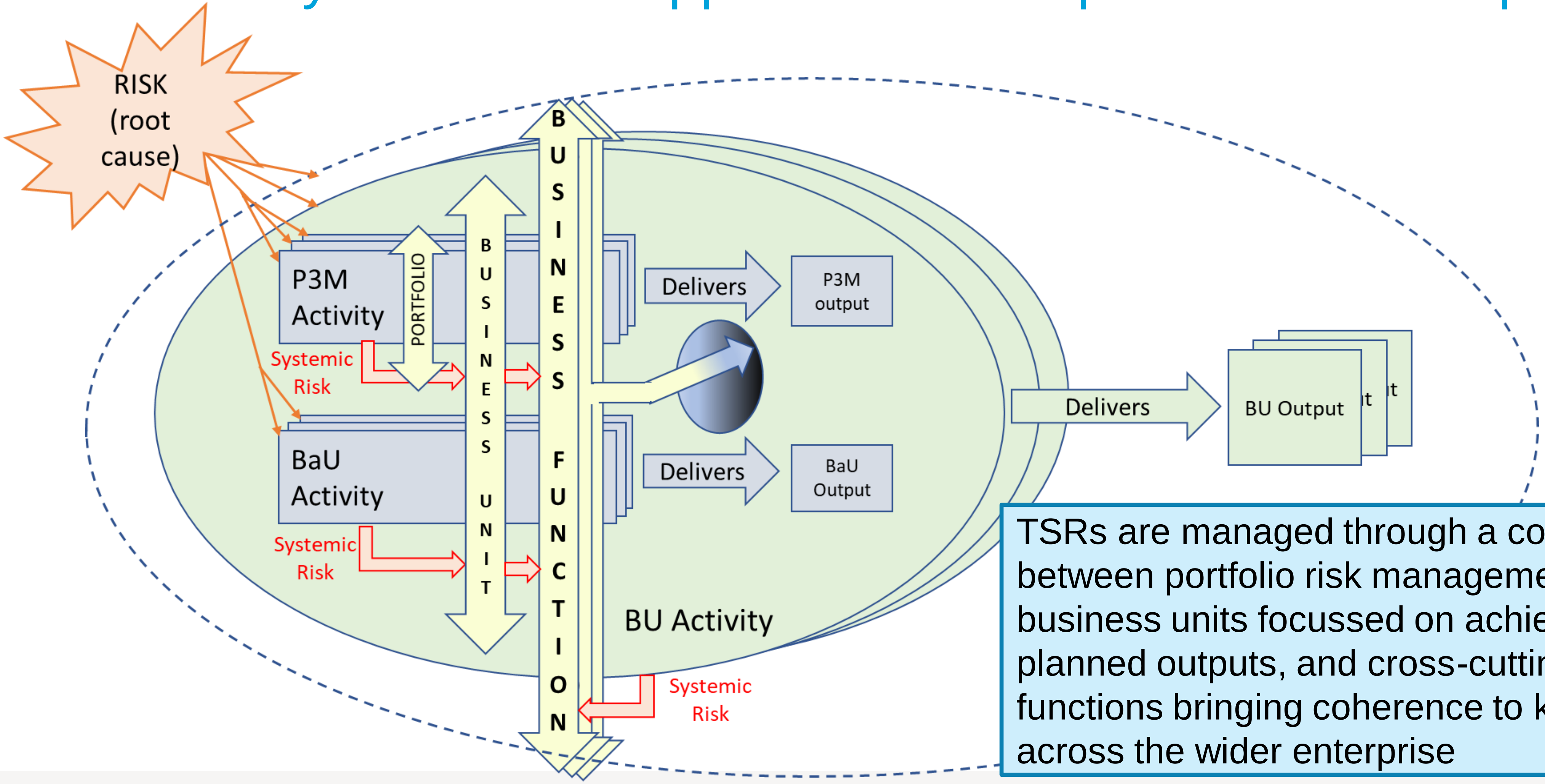
<u>Technical Systemic Risk Management</u>
What are the risks to effective and efficient delivery of my objectives across the business?
(Looks across organisation to identify common risks and mitigations)

What is Technical Systemic Risk? A Definition:



“A technical risk is systemic if it impacts upon, or could be best managed within, the wider enterprise due to its cause or impact occurring outside of the constraints of a single project, programme or Business-as-Usual (BaU) activity”.

Technical Systemic Risk applied to the Acquisition Landscape



TSRs are managed through a collaboration between portfolio risk management, business units focussed on achieving planned outputs, and cross-cutting business functions bringing coherence to key areas across the wider enterprise

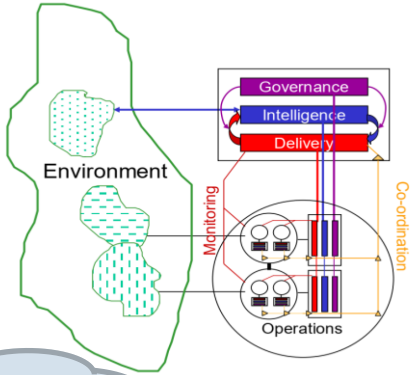
Towards an Approach

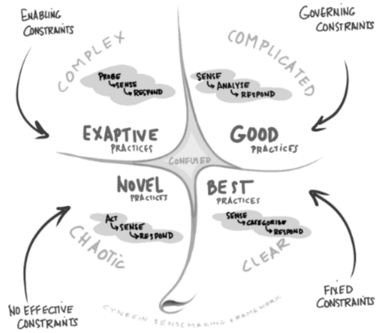
Common failure modes in complex organisations

VSM Pathologies

Retrospective Coherence + Pattern Sensing

Viable System Model (VSM)





Cynefin Framework

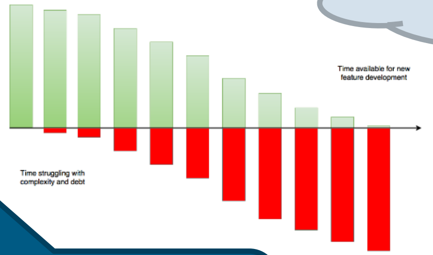
Intra-Organisation interfaces

Enterprise Risk Management (ERM)

Outcome oriented risk management

But where's the flowchart?

Work left "undone"



Technical Debt

Financial Risk

Endogenous risk + Amplification

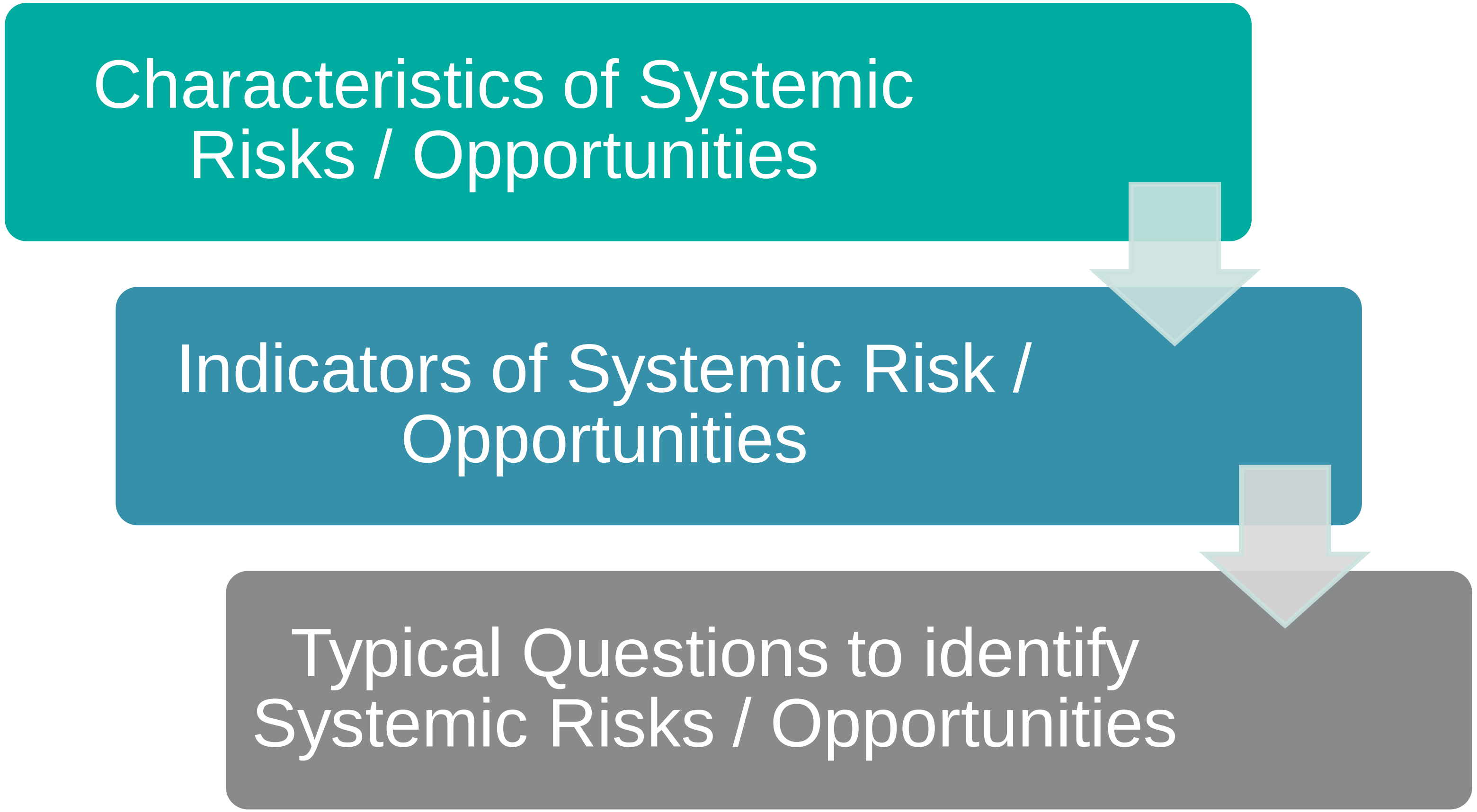
VSM graphic is © P Hoverstadt
Cynefin graphic is © D Snowden
VSM pathologies graphic is © J Cusin
Technical Debt graphic is © C Verwijs

ATKINS
Member of the SNC-Lavalin Group

Ministry of Defence

de&s

How to spot a Systemic Risk or Opportunity

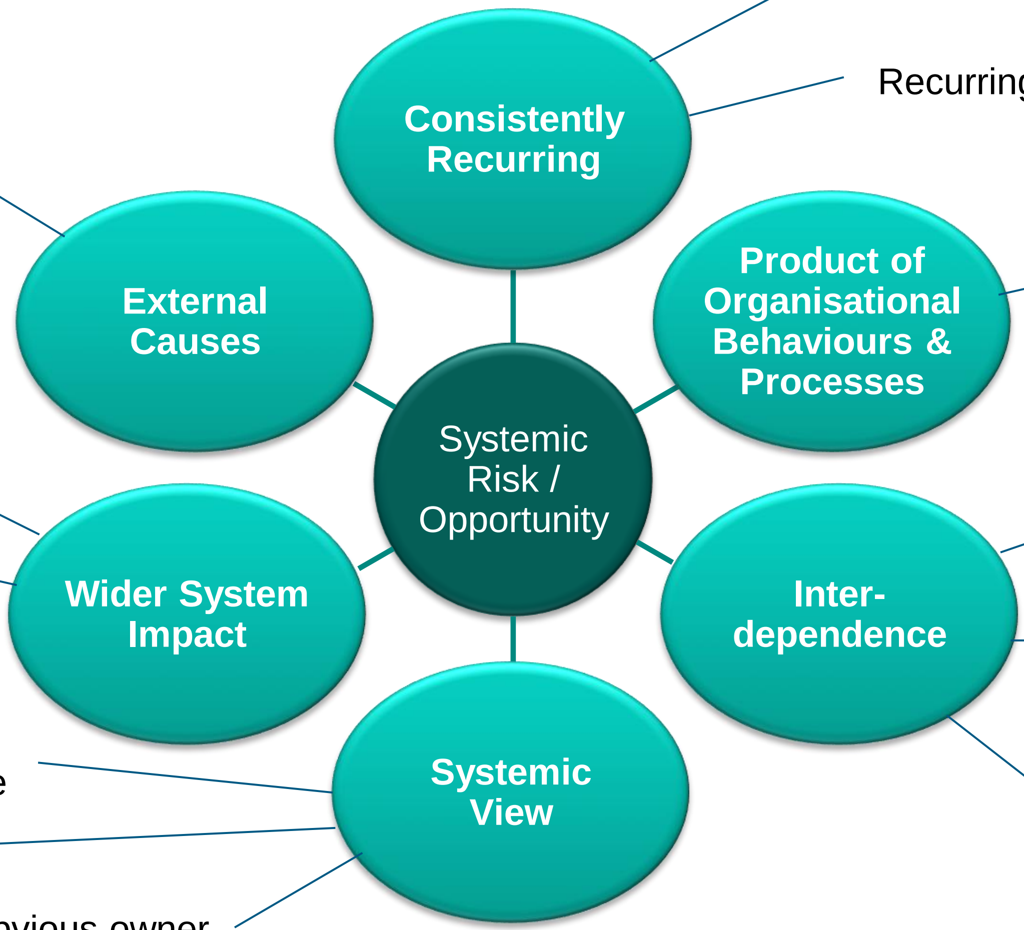


Characteristics of Systemic Risks / Opportunities

Indicators of Systemic Risk / Opportunities

Typical Questions to identify Systemic Risks / Opportunities

Characteristics of Systemic Risks



Multiple occurrences

Recurring

Does not directly impact a BU output – but impacts elsewhere in the system requires BU activity to mitigate

“Every time we do x, there is a risk of y happening”.

Risk has significant wider adverse effects

Local mitigation may have adverse effects elsewhere in Defence.

Interlinkages and interdependences within and across the system

Amplified by system connectivity (minor impact in one area = disproportionate impact elsewhere)

Not effectively managed and impacts treatable by one area of the business alone

Only observable at a higher, aggregated level

Not a single obvious owner

Critical failure/compromise elsewhere in Defence

ATKINS
Member of the SNC-Lavalin Group

Ministry of Defence

de&s

Mitigating Systemic Risks

Global Mitigation	Can be overkill if done in a heavy-handed manner System may be impacted – could even cause a systemic risk!	Considers wider system implications and efficiencies Offers the opportunity to solve the problem in a “best for the business” way, improving and transforming the system… but not always locally optimal
Local Mitigation	This is traditional risk management	Multiple local mitigations likely to be inefficient and have knock-on effects at the global level No appreciation of wider impacts, may hide or amplify the problem
	Non-Systemic Risk	Systemic Risk

Indicators – “Consistently Recurring” Example

? Does this risk relate to a cause or event which frequently occurs or is likely to recur elsewhere and should be considered for a common risk approach?

? Is this a risk that is likely to recur in the future and is a candidate for proactive opportunity management?

Learning from Experience

During stakeholder engagement, several different organisations flagged up that they did not think that they were exploiting their lessons identified as effectively as they could be, potentially leading to recurrent problems that could be addressed by better visibility of similar risks on recent programmes.

An LFE toolset was identified that was already in use and would be straightforward to roll out across these organisations. An investigation was proposed into using data analytics on this toolset, aiming to move from cataloguing LFE to actively exploiting it.

ATKINS
Member of the SNC-Lavalin Group

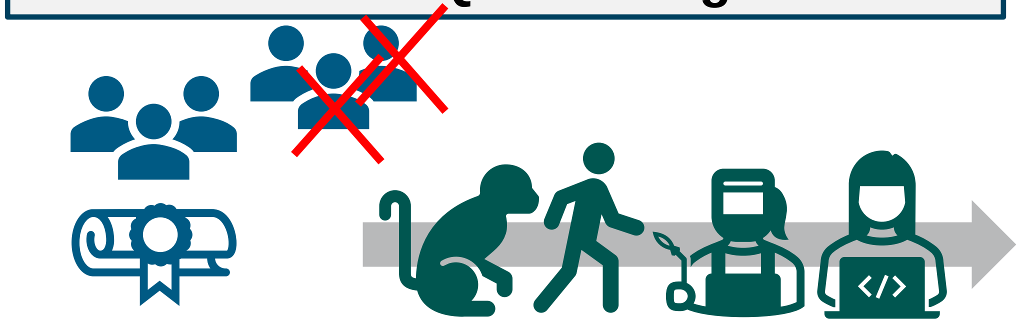
Ministry of Defence

de&s

Indicators – "Interdependence" Example

Does this risk have an impact beyond your area of responsibility and, if so, could it lead to disproportionate effects elsewhere in the business and hence needs a wider risk management approach?

Workforce SQEP Management



Most stakeholders have raised risks around workforce planning and the need to have access to Suitably Qualified & Experienced Personnel to support their programmes and activities – noting that they are often in short supply.

Mitigations such as offering better pay and conditions would be likely to solve a local problem at the expense of creating one elsewhere in the wider enterprise.

A broader approach would be to look at creating centres of excellence for certain key disciplines (such as Quality) that can be drawn upon, changing roles & responsibilities within the processes, or taking a longer term view across the business to enable better workforce planning to meet evolving skills needs.

ATKINS Member of the SNC-Lavalin Group

Ministry of Defence

de&s

Indicators – "Systemic View" Example

? Is it realistic to try and manage this risk within your own area of responsibility or does it require (or could it be better managed by) a wider set of mitigation activities?

Requirements Interface

A pattern was spotted between risks raised within customer organisations and risks raised within acquisition organisations relating to the technical requirements interface. One side felt that they didn't always get enough technical support to develop the requirements, the other felt that they didn't always get enough firm direction and scope on what the requirement was.

This is recognised as an opportunity to improve Front Door services, particularly in the Programme Definition and Concept Phases where requirements should be developed in more of a collaborative manner between customer and supplier organisations.

ATKINS
Member of the SNC-Lavalin Group

Ministry of Defence

de&s

Stakeholder Engagement

The characteristics and indicators have proved useful in explaining the approach: most risk practitioners and managers recognised the concept of technical systemic risk but lacked the vehicle to address it

Areas of the business that naturally seek to make connections and have to regularly work across organisational divides have been early adopters

Taking a more collegiate “community of interest” approach to making TSRs visible between stakeholders has created a relatively “safe space” for discussions

High priority TSRs are being escalated to a senior stakeholders forum for agreement and sentencing

Conclusions Relating to Implementing TSR management

Traditional risk management practice tends to overlook Systemic Risks, often due to lack of vision beyond project and programme focus or organisational and functional boundaries

Technical Systemic Risk management allows risks that may be common to, or impacting upon, several areas of the business to be identified, and managed. This will allow common and consistent risk mitigation to be applied in a “best for the business” way

Technical Systemic Risk management is complementary to existing P3M and ERM approaches, providing an almost orthogonal view on the same problem-spaces and solution-spaces

Technical Systemic Risk management is equally applicable to business-as-usual activities as it is to projects and programmes

Conclusions Relating to Systemic Risks

Learning from experience (LFE) reviews are a rich source of potential Systemic Risks, and were valuable in developing the indicators

The approach outlined above is an accessible and useful approach which risk practitioners should find easy to adopt and can be readily adapted for non-technical Systemic Risks

Systemic Risk management is a useful addition to the toolbox when doing Systems Engineering at an enterprise level, providing a cross-cutting view across existing risk management approaches, giving visibility of risks that might otherwise be lost in the fog

This innovative approach should be readily applicable in any enterprise which is grappling with the issues outlined in this presentation

Questions?