



HM Government

Assuring Information in the Longer Term

Ian Bryant

IA Projects Advisor

DSSA, UK MOD

24th ACSAC

12 December 2008

Anaheim CA US

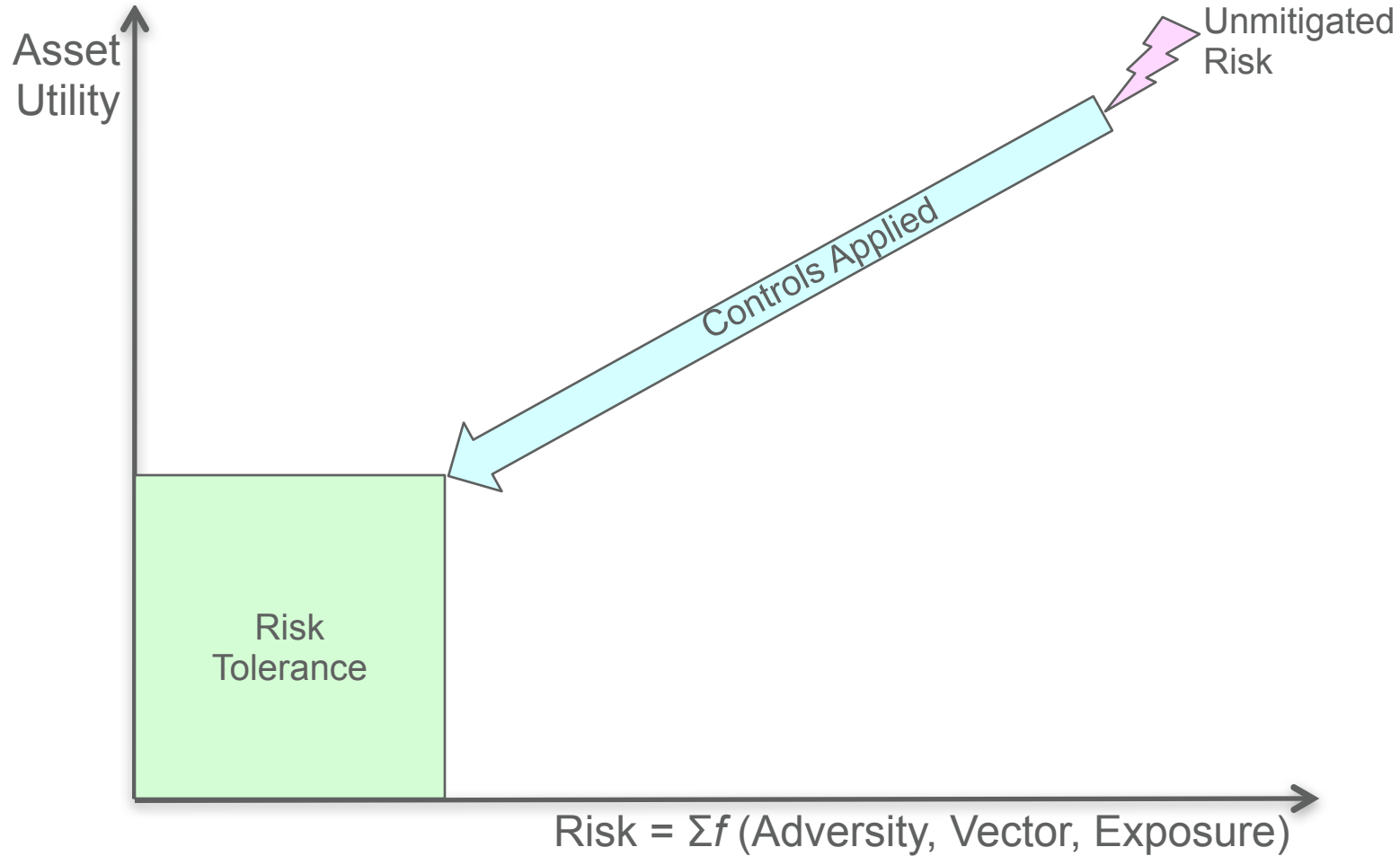
This Case Study is a fusion of work done on behalf of, or in conjunction with, amongst others :

- The UK National Archives (TNA)
- The UK National Information Assurance Forum (NIAF)
- The NATO Research and Technology Organisation (RTO) Task Group on XML in Cross Domain Solutions

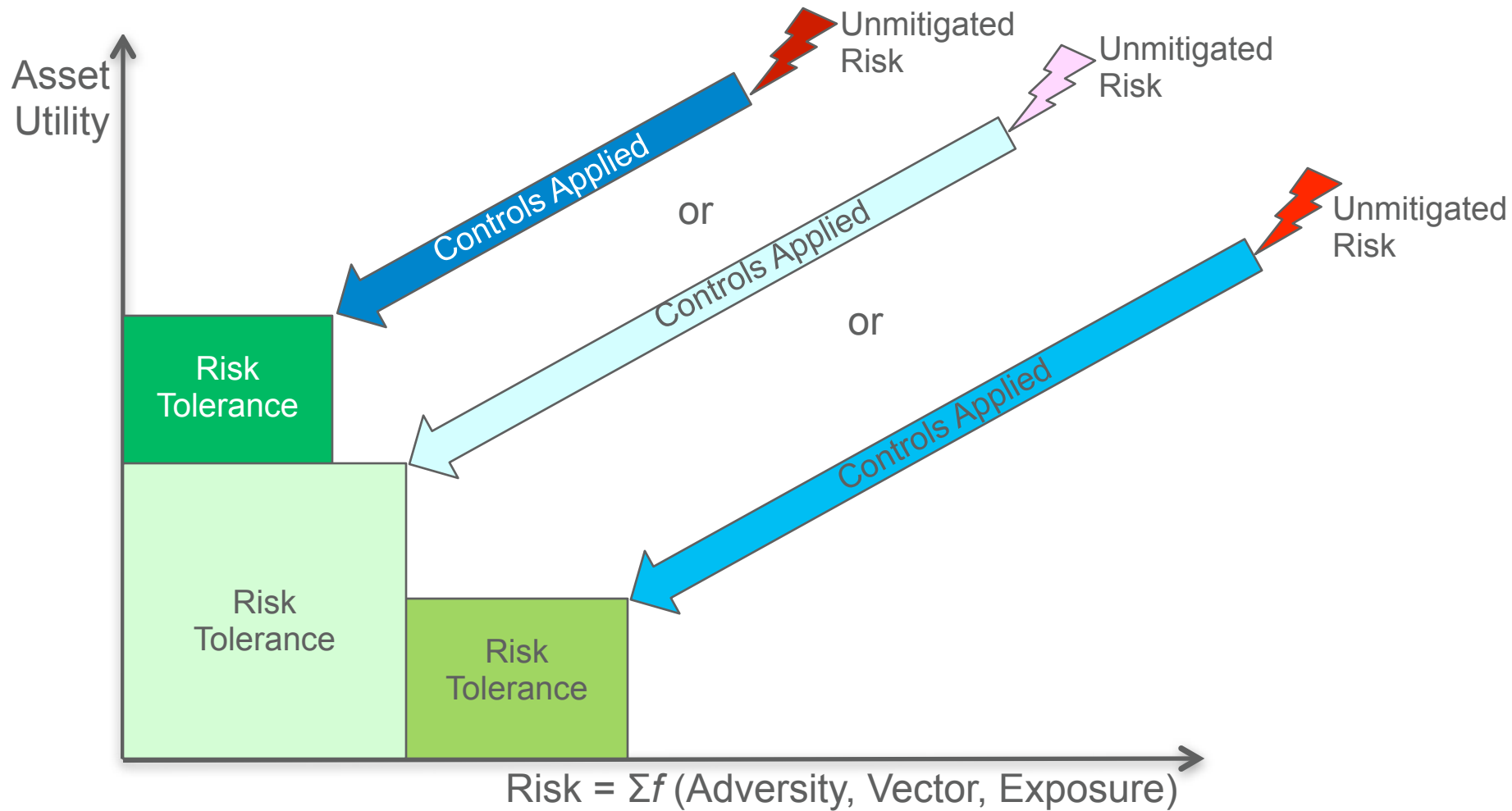
Disclaimer

The ideas presented in this presentation are not necessarily current UK Government Policy, nor are they a commitment for the UK Government to develop Policy and/or Guidance in these areas

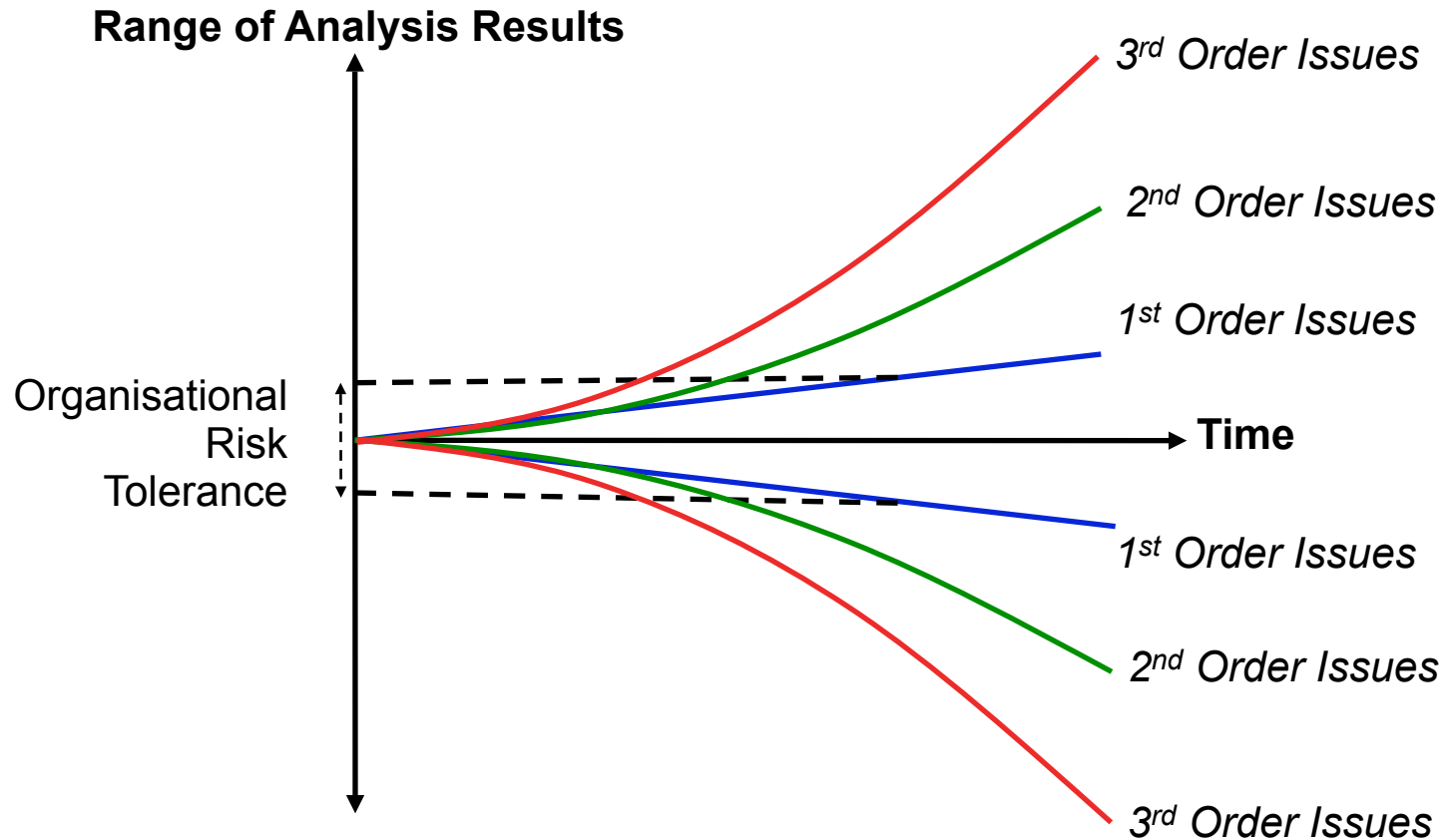
Simplified Risk Management Model



Potential Variation of Risk with Time



Long Term Risk: Temporal Drift



Variant Factors

- Risk Tolerance
- Risk
 - Adversity
 - Vector
 - Exposure
- Controls Applied
 - Strength
 - Efficacy
- Asset Utility



Variant Factors

➤ Risk Tolerance

- Risk
 - Adversity
 - Vector
 - Exposure
- Controls Applied
 - Strength
 - Efficacy
- Asset Utility



Variations in IA Risk Tolerance

- Important to recognise actually this is a “Utility” measure
 - From Economics
 - A measure of (personal) Relative Preferences
- Terminology currently very loosely used: preferable to align with formalised definitions used in Safety realm
 - Aid Risk Owners to understand **Appetite, Balance & Tolerance**
- But these preferences are liable to “PESTLE” pressures
 - Political
 - Economic
 - Social
 - Technological
 - Legal
 - Environmental



Tolerance, Acceptance & Balance (1)

RISK ▶

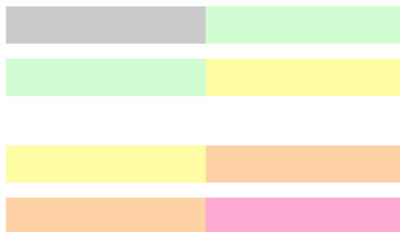
U	K+u	K+u	K+u	K+u
Not Known	Not Practical	Could Address	Will Address	Must Address

◀ COUNTERMEASURES

Where

K Known
 u unknown
 U Unknowable

Boundary Definitions



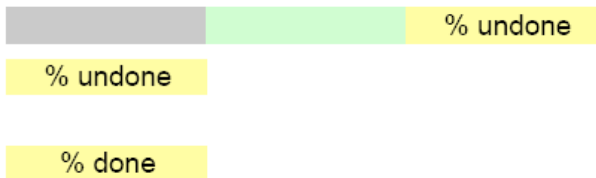
As Low As Physically Possible (ALAPP)

As Low As Reasonably Possible (ALARP)
 - sometimes Baseline Protection Objective (BPO)

As Low As Reasonably Acceptable (ALARA)

Baseline Protection Limit (BPL) - from Policy

Utility Measures



Tolerance

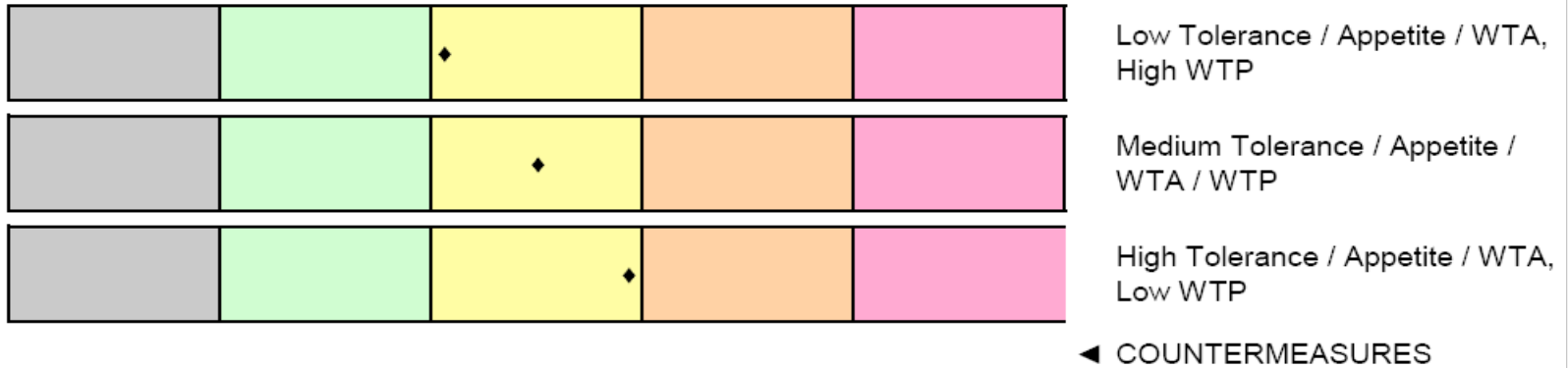
Appetite - Willingness to Accept (WTA) - Disutility
 - The Optional Part of Tolerance

Balance - Willingness to Pay (WTP) - Utility

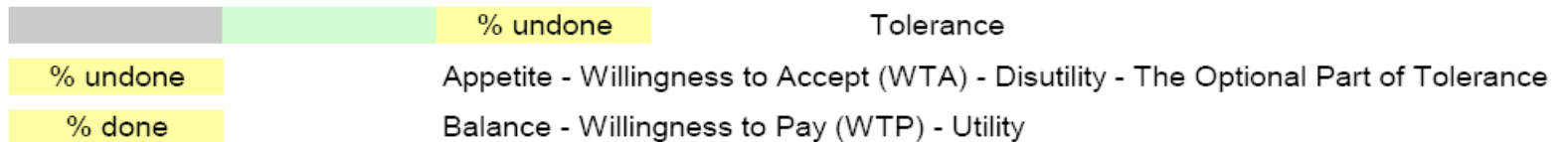


Tolerance, Acceptance & Balance (2)

RISK ▶



Utility Measures



- Remember Organisational Risk Tolerance varies with Time :
 - Political pressures
 - Economic pressures
 - Social pressures
 - Technological pressures
 - Legal pressures
 - Environmental pressures



Variant Factors

- Risk Tolerance
 - **Risk**
 - Adversity
 - Vector
 - Exposure
 - Controls Applied
 - Strength
 - Efficacy
 - Asset Utility



Adversities – 2 Sub-categories

- **Hazards**
 - Typically Stochastic effects
- **Threats**
 - Threats typically regarded as Deterministic, which we historically decompose as:
 - Intent of an Adversary against a Target
 - Capability of the Adversary
 - Therefore traditional approach unable to handle full “KuU” Adversity spectrum (Known, Unknown and Unknowable)
 - But if Threats summed over time, convergence toward mean could allow modelling as if Stochastic
- Allows modelling both as measures of Probability of Occurrence



Adversity Attribute Enumeration

- **Threats**

- *T.Escorted*
- *T.Locations*
- *T.Breakin*
- *T.Seperate*
- *T.Connected*
- *T.Domain*
- *T.Admin*
- *T.Handlers*
- *T.Emanations*
- *T.Bearers*
- *T.Aquisition*

- **Hazards¹**

- *H.Utilities*
- *H.WIMPS²*
- *H.Environment*
- *H.Collateral*

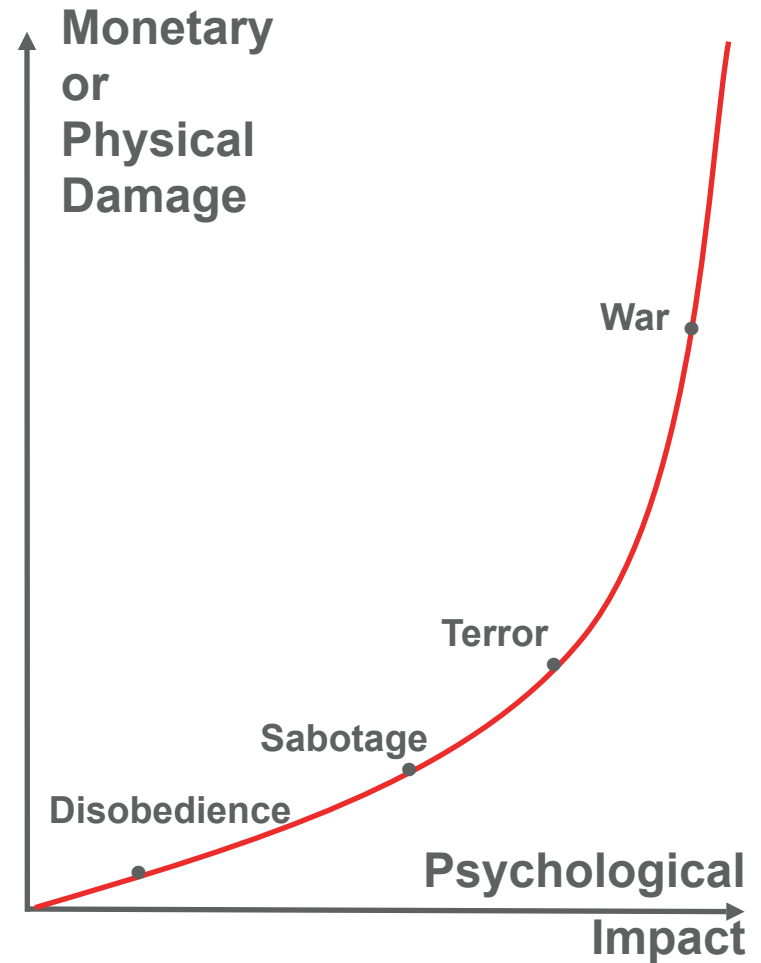
¹ Extension to MOD / QinetiQ Domain Based Approach to Security (DBSy), to add the “other half” of Adversities (c.f. **National Risk Register**)

² **Well Intentioned but Misguided PersonS** – includes Operator Errors and Omissions (E&O)



Threat Spectrum

- 1st order effects (e.g. MalWare, DDOS) impact directly on Cyber environment, and currently tend to count as **Disobedience** or **Sabotage**, not **Terror** or **War**
- 2nd order effects impact on functions on which Cyber environment directly relies, and currently more severe
 - e.g. disruption of power supply
- 3rd / nth order effects impact on functions on which Cyber environment indirectly relies, and currently have most severe Cyber impacts
 - e.g. “9/11” Kinetic DOS (2nd order antennae & switching centre, 3rd order landlines, mobiles, & websites)
 - Potential for Pandemic Disease disrupting communications by reducing staff available

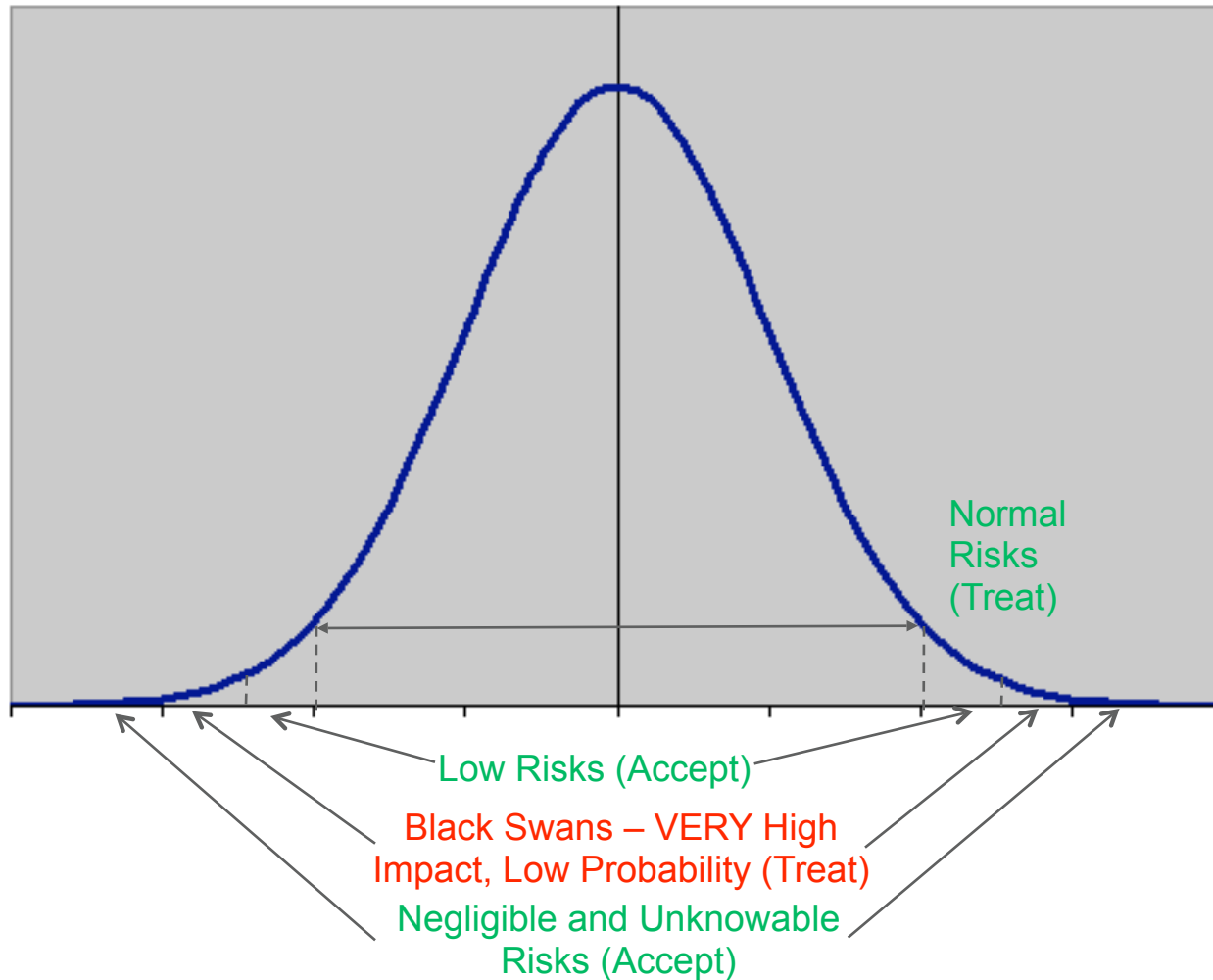


Vectors / Sources of Compromise

- Leakage
 - Deliberate (e.g. “Traitors”)
 - Inadvertent (Well Intentioned but Misguided People - WIMPS)
- Denial of Service
 - Deliberate (e.g Malicious Code)
 - Inadvertent (e.g. Accidents)
- Stimulation
 - e.g. Trojan Horses
- Vulnerability Exploitation
 - “Hackers”
- Procedural Failure
 - WIMPS (q.v.)



Thoughts on the “Black Swan”



Effects of Compromise

- In Long Term, useful to model Adversities by the Compromising Effects they cause
- Initial list of Deleterious Outcomes (DO):
 - Loss of Life
 - Personal Injury
 - Personal Distress
 - Physical Damage
 - Economic Damage
 - Reputational Damage
 - Disrupted Operations
 - Disrupt Relationships
 - Legal Offence
 - Regulatory Noncompliance



Variant Factors

- Risk Tolerance
- Risk
 - Adversity
 - Vector
 - Exposure
- **Controls Applied**
 - Strength
 - Efficacy
- Asset Utility

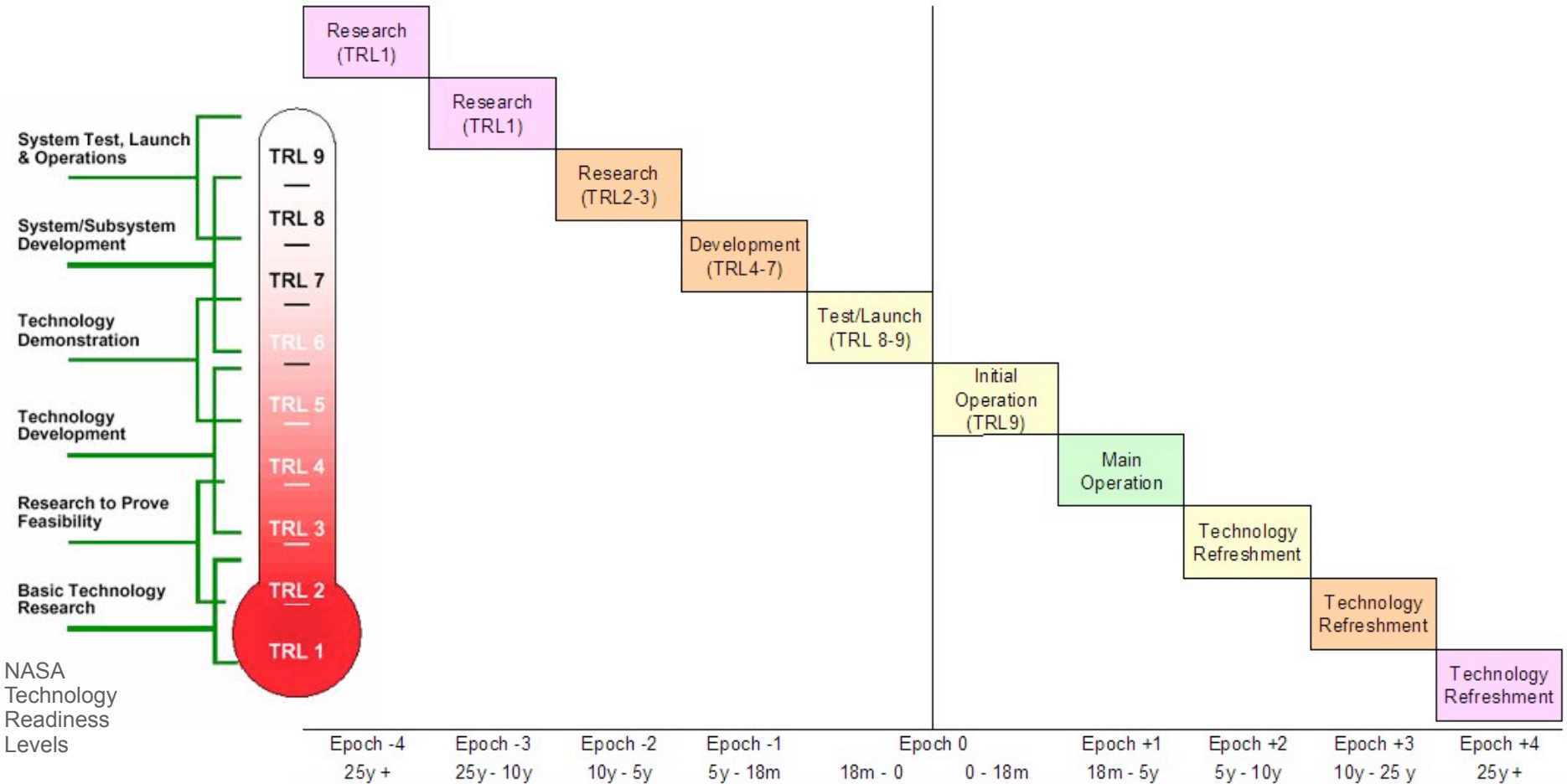


Controls

- Applied controls need to be measured in terms of:
 - Strength of Mechanism (SoM), which gauges the designed in ability to withstand applied Adversities
 - Efficacy of the Implementation(s)
- Both predicated upon Snapshot of the environment
 - Design (SoM) of controls based on the Adversity Model (normally **only** Threat Model) known at Development
 - The agreed Efficacy is normally based upon Testing against Vector set as known at the time
- And Technology change presents both Opportunity (for better SoM) and Challenge (for new Vectors)



Controls – Effect of Technology Change



Variant Factors

- Risk Tolerance
- Risk
 - Adversity
 - Vector
 - Exposure
- Controls Applied
 - Strength
 - Efficacy
- **Asset Utility**



Asset Utility

- The main Asset is normally the Information, **not** the Information System
- As with Tolerance, a Utility (Ordinal / Nominal) rather than Absolute measure
- Asset Utility is not static
 - Differing people and organisations
 - Changes over time
 - Technological evolution increases Reuse
 - Web 2.0
 - Semantic Web

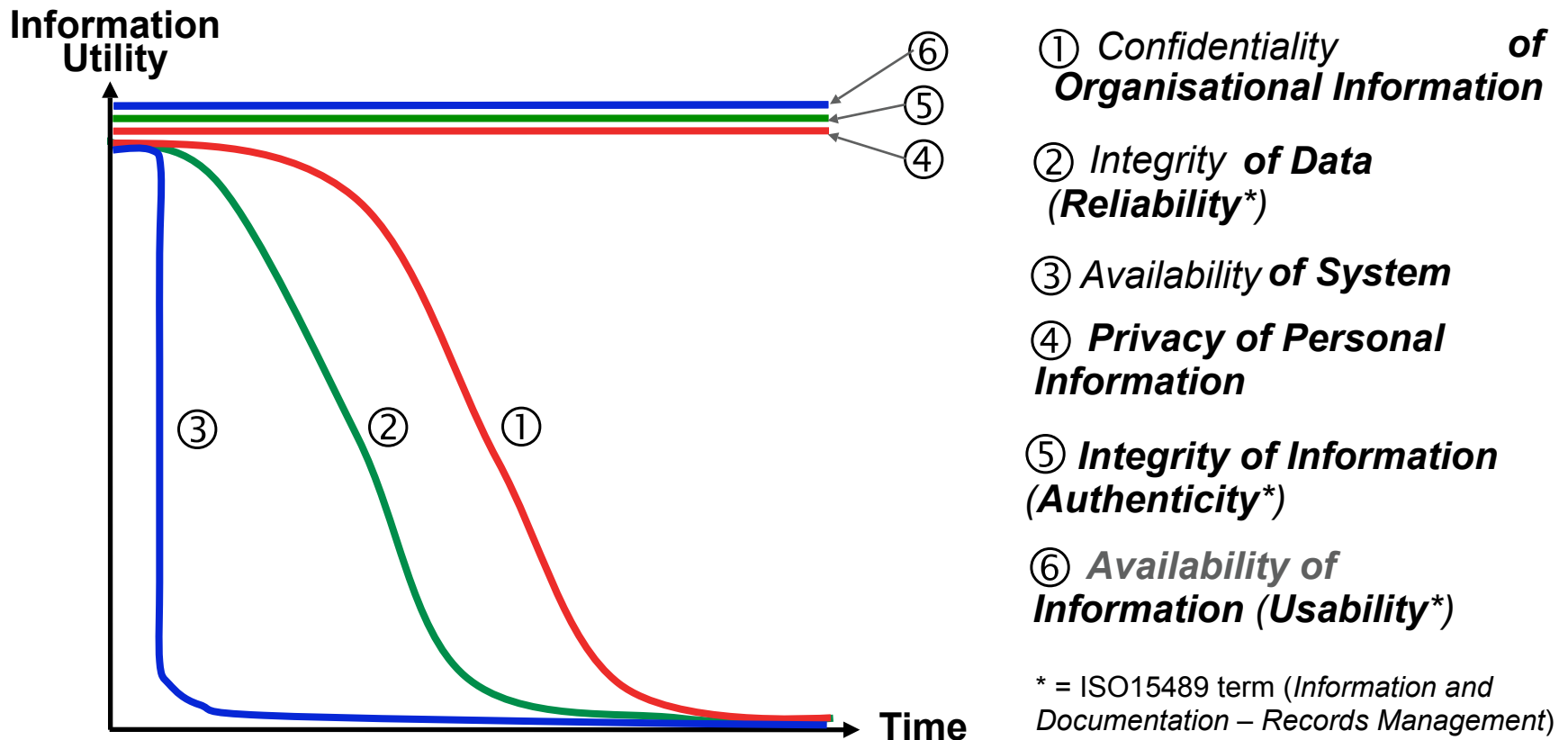


Judging Information Utility

- “Classical” Model uses only 3 Properties (“CIA”)
 - Confidentiality, Availability, and Integrity
- National Archives initial work on collating IA and Information Management (IM) added 2 Properties:
 - **Authenticity**
 - **Usability**
- Personal Information focus of recent **Data Handling Review** led to re-review of Confidentiality
 - Split out **Privacy** as 6th Property
- Parallel but independent “*Parkerian Hexad*”



Information Utility over Time: Intrinsic Properties needed for a Public Record



Completing the Information Property Review (1)



Extension for
Associative /
Transactional Properties

→

Wisdom

Knowledge

Extension for
Accumulative
Properties

←

Privacy, Authenticity,
Usability

→

Information

Confidentiality, Integrity
(Reliability), Availability

←

Data



Completing the Information Property Review (2)

- Subject of current NIAF Working Group
- Includes the concept of **Aggregation**, which is generally used to mean two different things:
 - Effects of the **Accumulation** of Information Elements, which can be modelled from Atomic elements
 - Effects of the **Association** of Information Elements, which cannot be easily modelled from Atomic elements
 - NATO RTG-031 has therefore taken Composite labels Out of Scope
- eGovernment Metadata Standard (eGMS) update to include for all new properties in NameSpace



Assuring Information in the Longer Term Summary

- Risk Management “equation terms” vary with time
- Historic focus of IA practitioners has typically been monitoring for changes to Threat and Vulnerabilities
- For long term Information Assurance, consideration is needed in particular of dynamic features of:
 - Variability in Organisational Risk Tolerance
 - Other Risk components (Adversities beyond Threat)
 - Swings and Roundabouts of Technology Change
 - Asset utility (the wider Intrinsic Information Properties)



Contact Details

Ian Bryant

Information Assurance (IA) Projects Advisor
Office of Defence Security and Safety Assurance (DSSA)
UK Ministry of Defence (MOD)

Main Building
Whitehall, London, SW1A 2HB, England

+44 20 7807 0352; Desk + SmartNumber

ibryant@relay.mod.uk

<http://www.mod.uk>

