ACSAC 2022
December 5-9, 2022 · Austin, Texas, USA
And Virtual

WARWICK
THE UNIVERSITY OF WARWICK

Gaining Assurance in Commodities within Trustworthy Systems

WMG
Innovative Solutions

Prof. Ian Bryant

[UCR/082562 | v1.0 | 20221205]

Cyber Security Centre

ABSTRACT: Gaining Assurance in Commodities within Trustworthy Systems

Virtually any Trustworthy System is an assemblage of multiple smaller Elements, and it is a fact universally acknowledged that in the modern era, a proportion of such elements are likely to be Commodity Products and Services.

A challenge with Commodity Elements is that although a variety of Assurance Schemes have been created over the years, these tend to be short lived, and not directly compatible.

This Case Study examines an approach, called the Commodity Usage Principles and Assurance Service (CUPAS), that is intended to enable confidence in the consumption of Commodity Elements of a variety of sources and provenances, by the establishment of an enabling normalisation process.

ACKNOWLEDGEMENTS

Co-Investigator : Prof. Colin Williams
Mansfield College
University of Oxford

The authors wish to acknowledge the support of:

- The UK Ministry of Defence (MOD)
- The UK Trustworthy Systems Foundation (TSFdn)
- ADISA Certification

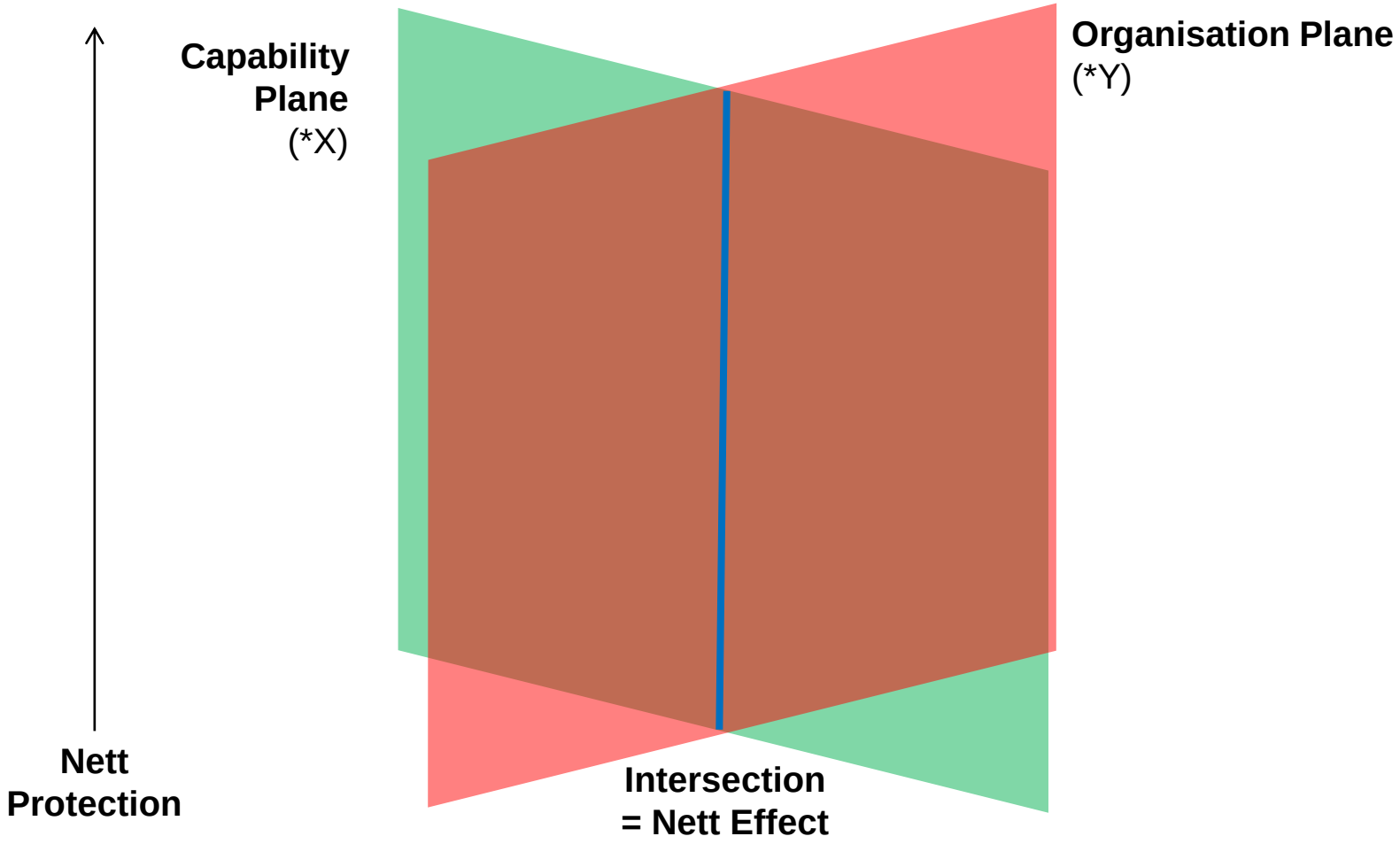
In supporting the Pilot of the approach described

Approach to Info-Cyber Protection

- Protection of Info-Cyber Assets should be Risk-based
- Based on the PACE philosophy
  - Pragmatic
  - Appropriate
  - Cost Effective
- And using an blended, balanced set of P^3T measures
  - Personnel (Pe)
  - Physical (Ph)
  - Procedural (Pr)
  - Technical (Te)

[Cabinet Office, Central Sponsor for Information Assurance (CSIA), 2003]

Locus of Protection

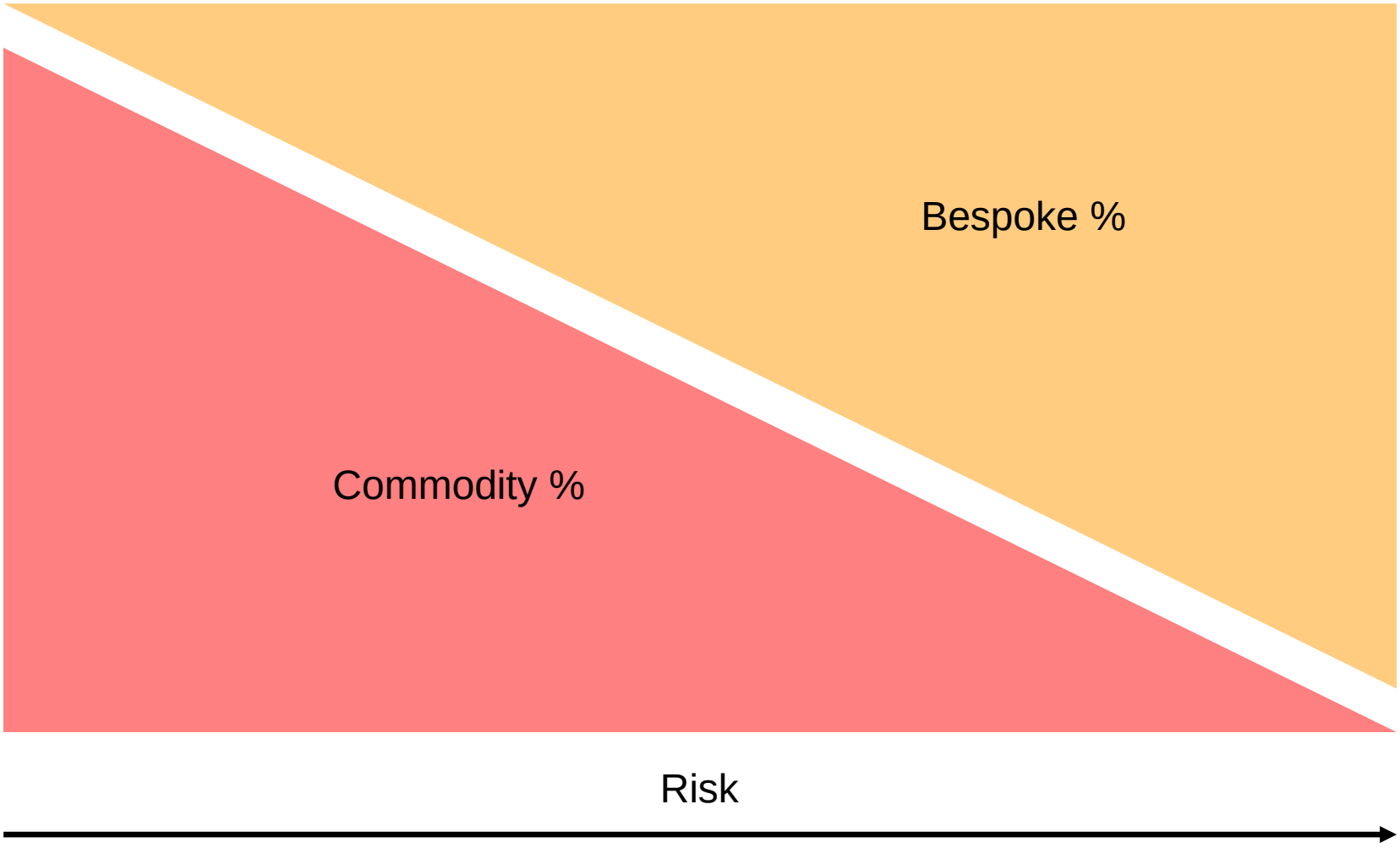


*(Simplified – may be X*Y intersections, and may be non-Euclidean Planes)*

What are Commodities?

- Commodity items are predominantly “Off The Shelf” (OTS), both mainstream Commercial (COTS) and specialised, Government / Military versions (GOTS / MOTS), but could include some Modified items that are based upon OTS and made available under call-off arrangements
- These items include both
  - Products
  - Services
- And Scope needs to cover all Commodities
  - Explicitly enforcing **Functional Trustworthiness (FT)**
  - Expectation of **Non-Functional Trustworthiness (NT)**
- Unlike Bespoke (a.k.a. Tailored) delivery, individual Customers (Relying Parties) have minimal influence over either the nature of the item, or the associated delivery Terms & Conditions (T&C)

Typical Solution Composition



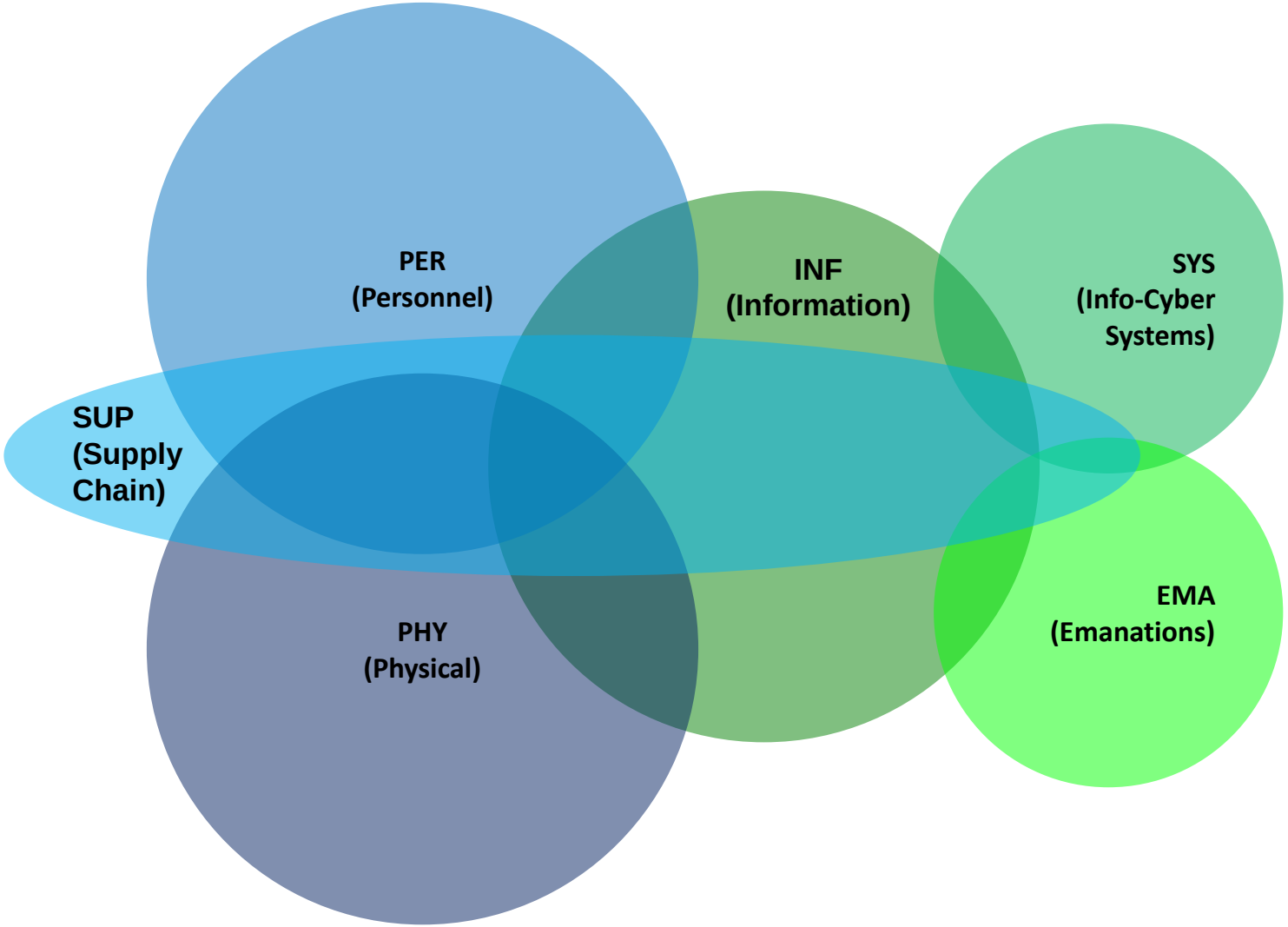
Assurance Approaches

- Formal Schemes
  - Based on Consensus, but not always a Single Consensus
  - Typically well documented, but can presented a constantly moving target, confusing both Supplying Parties and Relying Parties
  - Requires niche skills, leading to Group Think, and presenting communication barriers to the consumers
  - Often expensive, and time-consuming
- Informal Methods
  - Not based on any Consensus
  - Neither method – nor Commodities! – often well documented
  - Typically performed without SQEP (Suitably Qualified and Experienced Personnel)
  - Limited opportunities for Reuse

Problems with Current Commodity Usage

- No common method of gaining Assurance in Products and Services before use, as previous Schemes atrophied
- Poor quality of Configure-Operate-Maintain+dispose (COM) documentation
- Massive replication of effort from individual Projects and Systems in reviewing Products and Services: lack of baseline, so not reusable
- No common understanding of problems encountered in-use
- No consensus over marketplace Gaps in Products and Services, so limited pipeline of new offerings

Domains of Security Activity

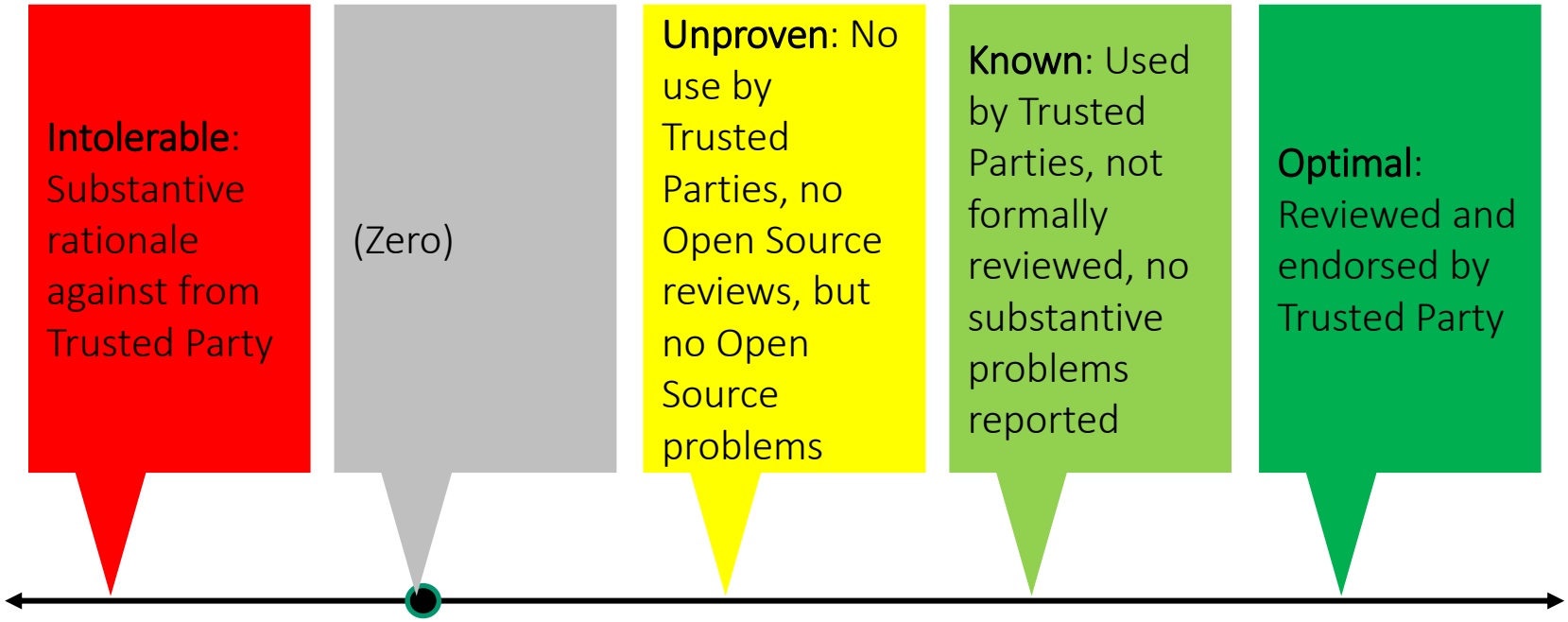


Goals for Future Commodity Usage

- Maximise the opportunities for reuse
- Support diversity of solutions
- Support diversity of implementation patterns
- Be catholic about 3rd party sources of assurance
- Be holistic in scope
- Be agnostic as to the solution type
- Be dynamic in maintaining currency of Assurance
- Provide a means for feedback between the Relying and Supplying Parties, such that Gaps may be addressed

Generic Confidence Spectrum

- Trustworthiness can be characterised as a Spectrum, with widely accepted limits:



- Any approach needs to allows Relying Parties (RP) to place Commodities on the spectrum

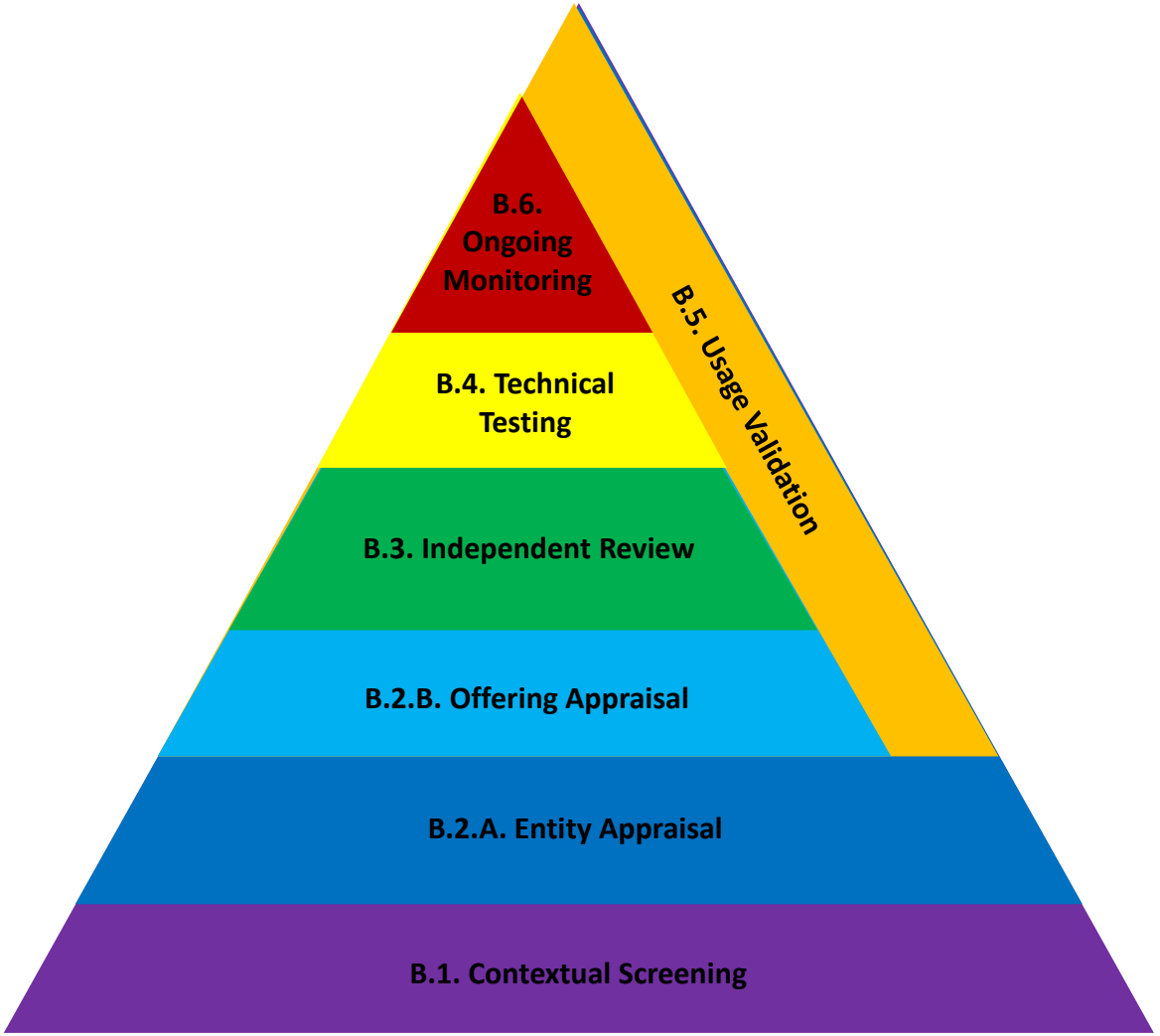
Risk-based Effort Consensus

Level	Protection Goal	Effort Expectation
0	Nil	Nil
1	Provision of protection against simple, indirect or collateral, adversities only with limited exposure	Due Care
2	Provision of protection against simple, indirect or collateral, adversities only with unlimited exposure, or simple, direct, adversities with limited exposure	Due Diligence
3	Provision of protection against simple, direct, adversities with unlimited exposure, or moderate, direct, adversities with limited exposure	Reasonable Endeavours
4	Provision of protection against moderate, direct, adversities with unlimited exposure	Reasonable and Diligent Endeavours
5	Provision of protection against significant, direct, adversities with limited exposure	All Reasonable Endeavours
6	Provision of protection against significant, direct, adversities with unlimited exposure	Best Endeavours

Sources of Assurance

Assurance Contributor (AC) Type		AL0	AL1	AL2	AL3	AL4	AL5	AL6
AC-0	Nil: no AC Review		✓					
AC-I	Unknown: AC Output, no process mapping			✓	(✓)			
AC-II	Known: AC Output, process mapped, with Gaps				✓			
AC-II*	Augmented: AC Output, process mapped, with Gaps Topped Up					✓	(✓)	(✓)
AC-III	Aligned: Partner AC meeting all process requirements					✓	(✓)	(✓)

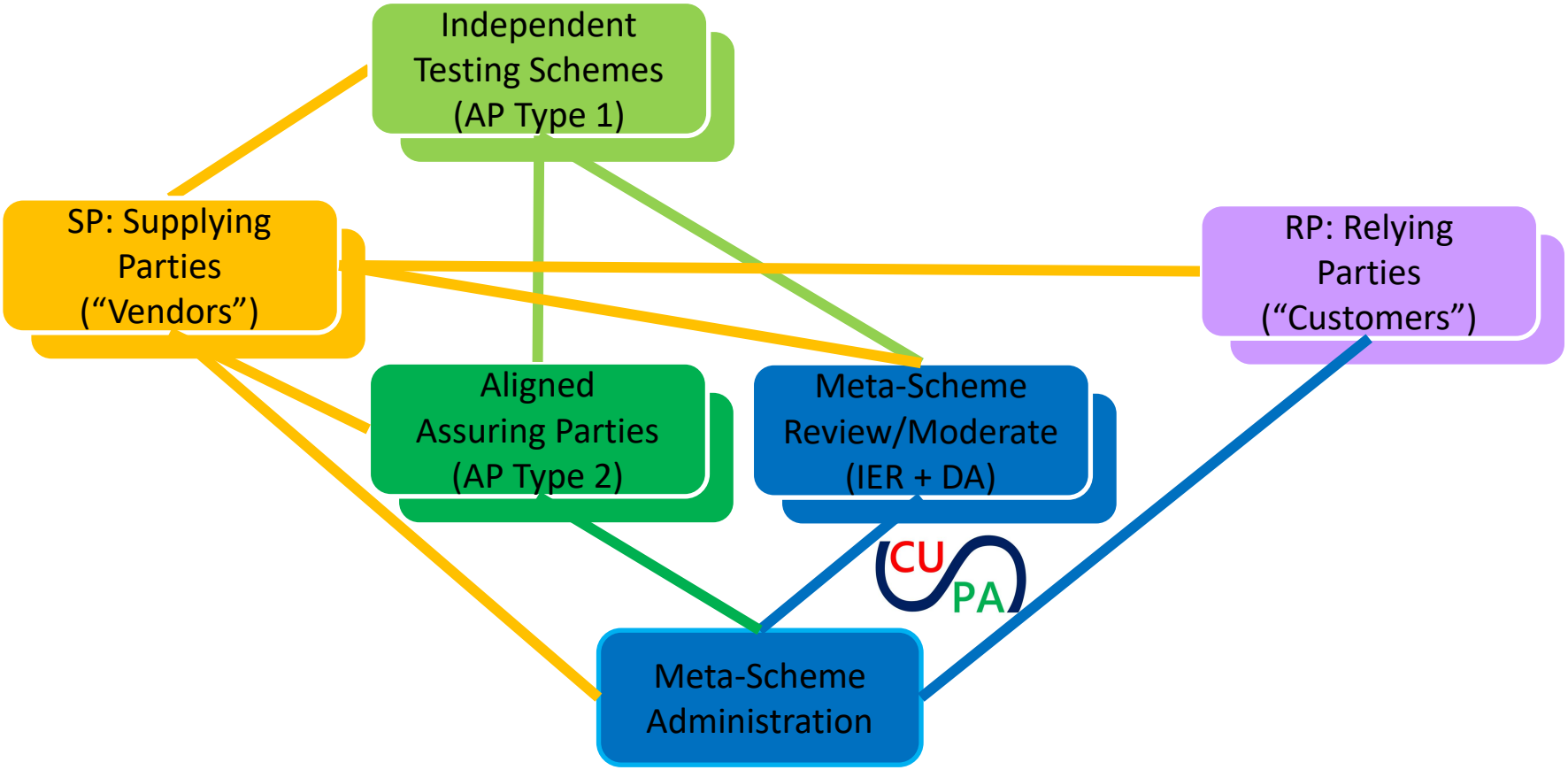
Elements of OTS Assurance



Assurance Actors

Activity		SP	RP	AP1	AP2	IER	DA
B.1	Contextual Screening	✓	✓	×	×	×	×
B.2.A	Entity Appraisal	✓	✓	×	×	✓	✓
B.2.B	Offering Appraisal	✓	✓	×	×	✓	✓
B.3	Independent Review	×	×	✓	×	✓	✓
B.4	Technical Testing	✓	×	✓	✓	✓	✓
B.5	Usage Validation	✓	✓	×	×	×	×
B.6	Ongoing Monitoring	✓	✓	✓	×	✓	✓

Contributory Assurance



Meshed nature of Assurance activities intended to de-risk habitual Churn of Test Bodies and Schemes

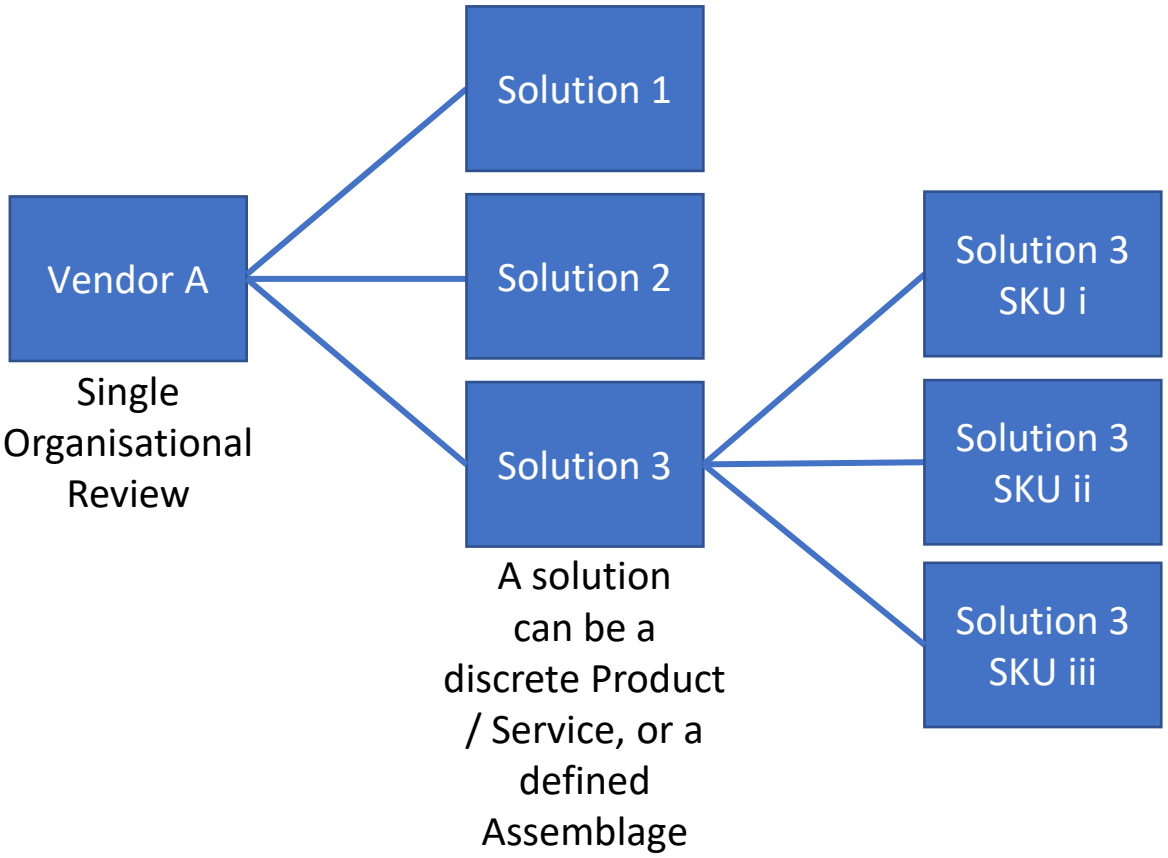
The Meta-Schema

- CUPAS is intended to be a Meta-Scheme; a Scheme About Schemes
- It is intended to Independent
- It is intended to be Enduring
- It is intended to Provide:
  - A consensus mapping of Assurance Activities to Assurance Levels
  - A mapping of Assuring Parties and their Scheme(s) to the consensus Assurance Levels
  - Management of the processes of Registration and Assessment, against the agreed, normalised, Assurance Levels, including the issue of an Assurance Mark
  - Through-Life, Iterative, Assurance
    - Monitoring for Known Issues
    - Engaging with Relying Parties for Feedback
    - Promulgating advice, and, if necessary, varying Assurance Level allocations

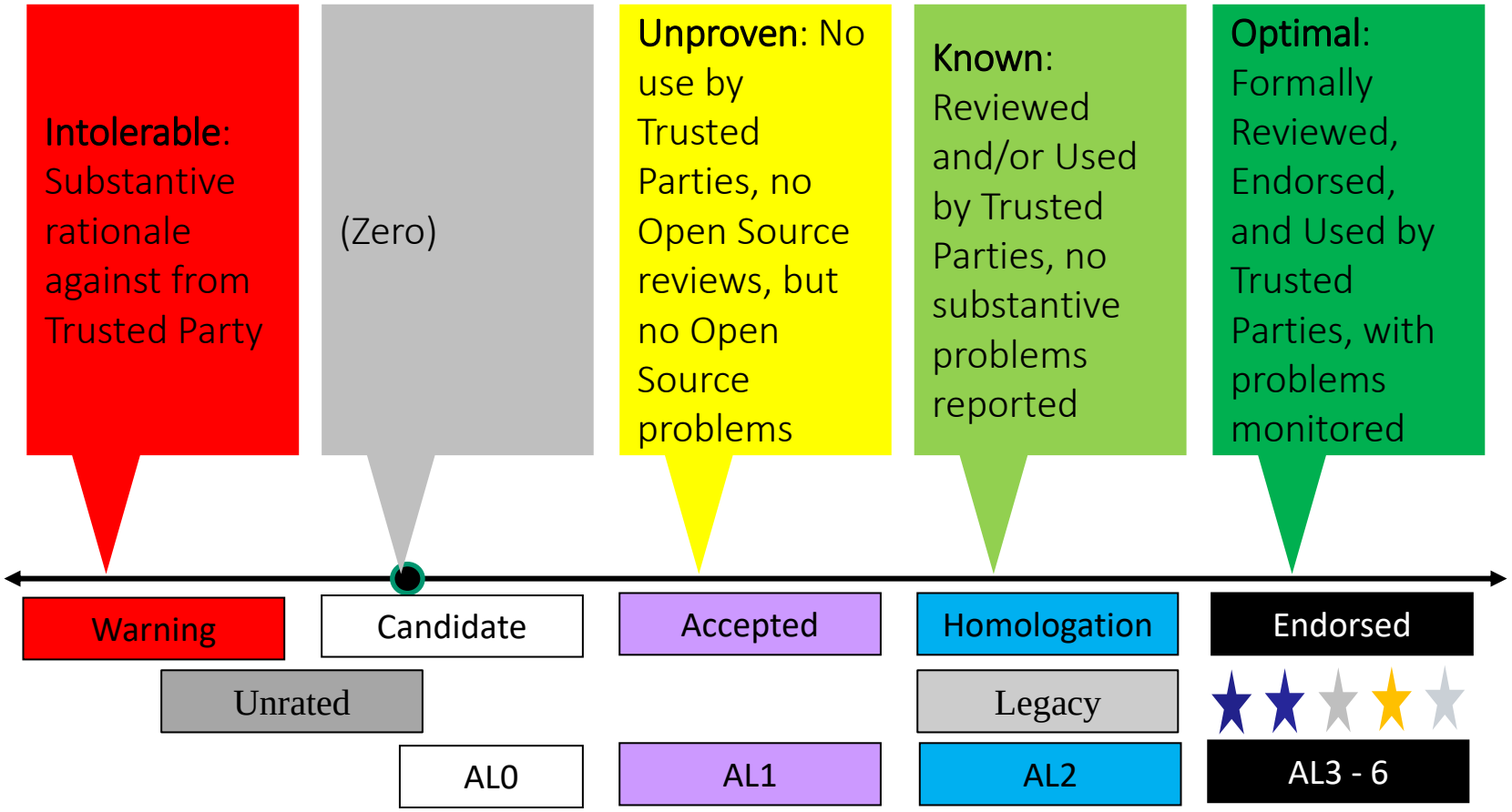
Normalising Assurance Activity

- AA.01: Provider Provenance (PP)
- AA.02: Literature Review (LR)
- AA.03: Vulnerability Review (VR)
- AA.04: Configuration Scan (CS)
- AA.05: Susceptibility Scan (SS)
- AA.06: Gaps Review (GR)
- AA.07: Claims / Characteristics Review (CR)
- AA.08: Exploitability Testing Type 1 (ET) - Tools
- AA.09: ET Type 2 = Penetration Test (PT)
- AA.10: Claims / Characteristics Testing (CT
- AA.11: Robustness Test (RT)
- AA.12: Code Analysis (CA) Type 1 - Static (SC) AA.13: CA Type 2 - Dynamic (DC)
- AA.14: Modelled Testing (MT)
- AA.15: Continual Surveillance (CS)

Reuse and Diversity



CUPAS Confidence Spectrum



Planned Hierarchy of Awards

Approach	Scope	A-R-E Status
Attestation	Non-Functional Trustworthiness (NT) appraisal	AL1: **N**T **A**ccepted
	Functional Trustworthiness (FT) appraisal	AL1: **F**T **A**ccepted
	Partnering with External Assurance Schemes	**R**ecognised
	Unreviewed Adoption from External Assurance Schemes	AL2: **H**omologated
	Revalorisation (e.g. DIPCOG)	AL2: **L**atte **E**ndorsed
Review	Independent review by CUPAS of Organisation (V) or Product / Service (B)	AL3: **V**erdun **E**ndorsed
		AL3: **B**ronze **E**ndorsed
Verification	Independent reviews by CUPAS and Schemes of Product / Service	AL4: **S**ilver **E**ndorsed
		AL5: **G**old **E**ndorsed
		AL6: **P**latinum **E**ndorsed

Lack of Absolution

- The has been a tendency for Certificates from Assurance Schemes to be regarded as Indulgences of Absolution
- This is, at best, naïve, as contextualisation is always import
- The Meta-Scheme provides a replicable, consensus measurement as to the likely confidence that can be assume for a commodity, when properly installed, maintained, and used in the manner intended
- The Relying Party remains responsible for
  - Validating that the Solution is suitable in terms of Functionality
  - Validating that the Solution is suitable in terms of Robustness
  - Ensuring that the solution is Configured – Operated - Maintained / Disposed appropriately
  - Supporting the Community by providing Ongoing Surveillance

Contact

Prof. Ian Bryant

Principal Investigator (UCR)

International Manufacturing Centre

University of Warwick

University Road

Westwood Heath

CV4 7AL

England

i.bryant@warwick.ac.uk

https://is.gd/wmgcsc

ACSAC 2022
December 5-9, 2022 · Austin, Texas, USA
And Virtual

WARWICK
THE UNIVERSITY OF WARWICK

WMG
Innovative Solutions

Gaining Assurance in Commodities within Trustworthy Systems

Cyber Security Centre

Prof. Ian Bryant

Paper Download: https://tinyurl/acsac38bryant