ACSAC 2021
December 6–10, 2021 • Online

WARWICK
THE UNIVERSITY OF WARWICK
WMG
Innovative Solutions

Cyber Security Centre

Trustworthy Selection and Use of Commodity Products and Services

Prof. Ian Bryant

[WMG/CSC/UCR/073332 | v1.0 | 20211204]

In partnership with

Secure Collaboration
UKCeB

Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?

Trustworthy Selection and Use of Commodity Products and Services

- **What Are Commodities?**
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?

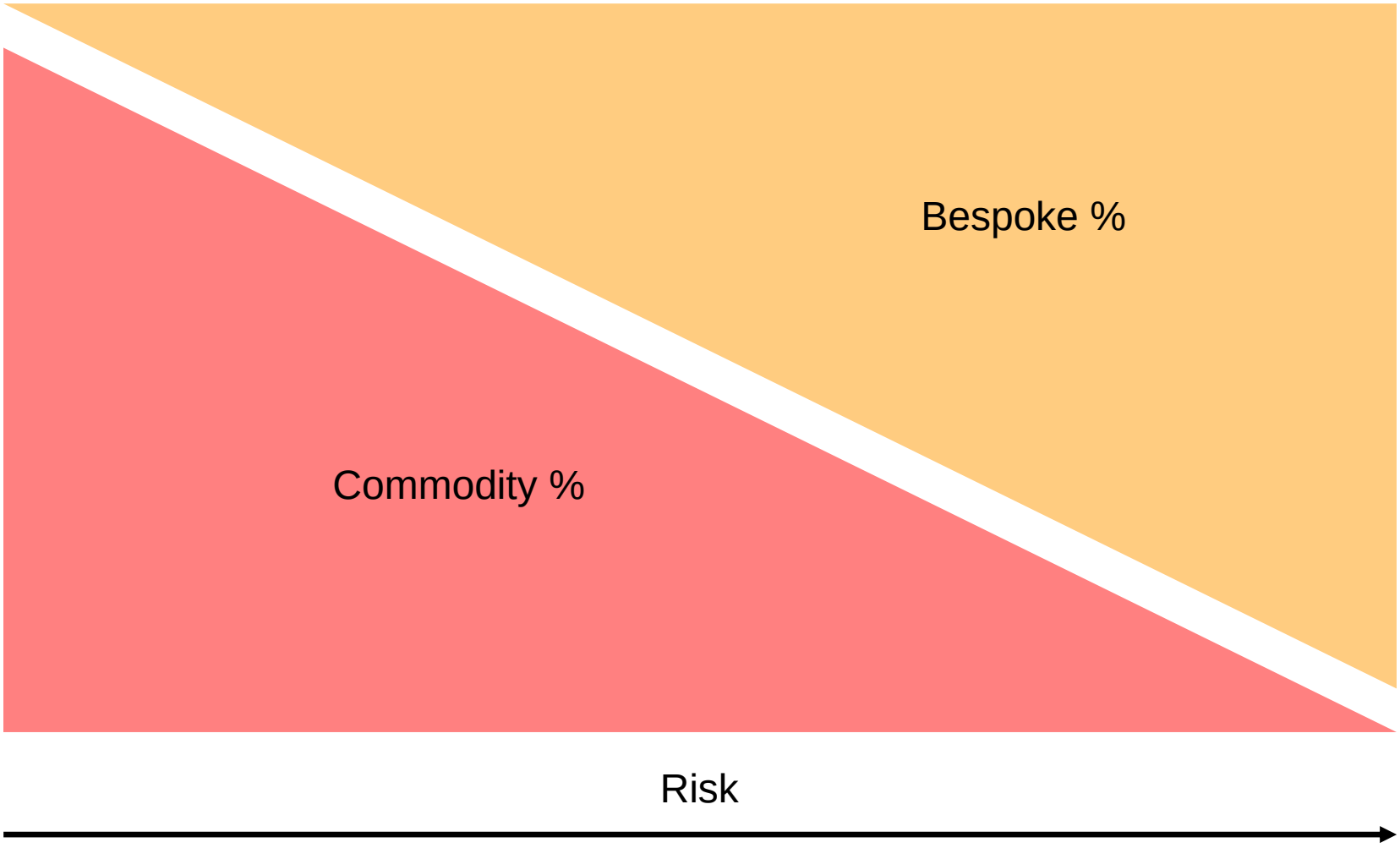
What Are Commodities?

- Commodity items are predominantly “Off The Shelf” (OTS), largely mainstream Commercial (COTS), but also specialised, Government / Military versions (GOTS / MOTS)
- This can include some Modified items that are based upon OTS, and made available under call-off arrangements
- These items include
  - Products
  - Services
- There are Trustworthiness considerations for both
  - Commodities explicitly providing Protective features
  - Commodities with No explicit Protective features
- 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)

Commodity Usage

- Commodity Products and Services may be used:
  - Individually
  - As part of a Solution Assemblage, including
    - Infrastructures
    - Bespoke Solutions
- The End User may :
  - Be the Customer, with a direct relationship with the Supplier
  - Have an indirect relationship with the Supplier
    - Through an in-house function, who are the Customer
    - Though an outsourced function (e.g. delivery partner), who are the Customer
    - Through a delivery partner, who are themselves only in an indirect relationship
- Diverse and Disjointed market means the interests multiple Customers ("Relying Parties" - RP) are seldom clear to the Supplying Parties (SP)

Typical Solution Composition



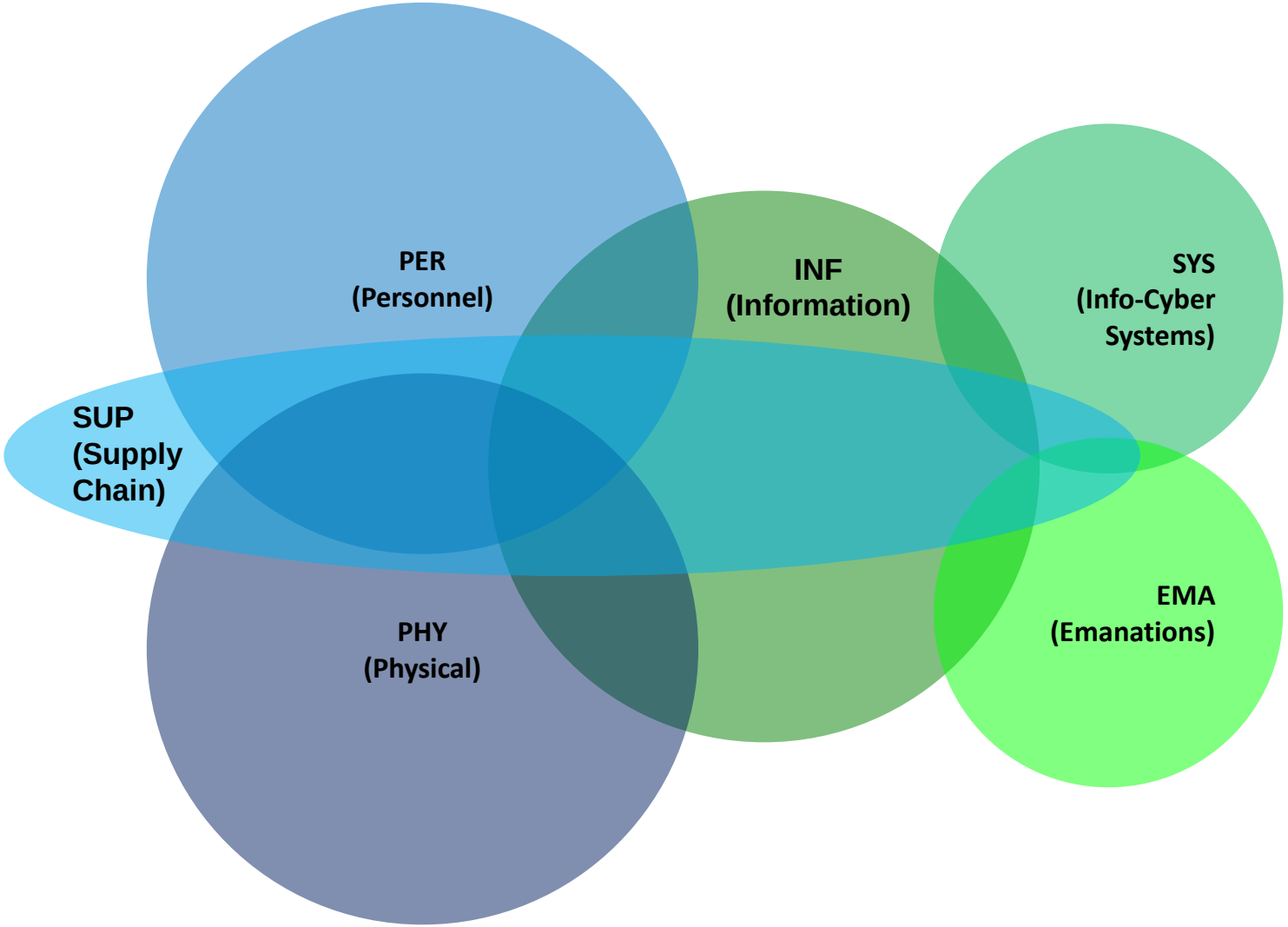
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- ➢ **What Has Gone Before?**
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?

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

Domains of Security Activity



Learning from Lessons Identified

- From Assurance
  - Churn and Costs of Formal Schemes
  - Poor Robustness and Reuse of Informal Methods
- From Market
  - Lack of Consensus from Relying Parties as to Gaps
  - Lack of Standards to which Supplying Parties can Conform
- From Implementation
  - Poor Consensus between Security Domains, for instance a Physical Device relying on Digital Controls
  - Assurance tasks typically too rigidly documentation-centric
  - Wedded to single delivery model, for instance “Cyber” strongly aligned to Software, with poor understanding of Hardware
  - Poor responsiveness to Novelty and Innovation
  - Business Models marginalise low margin items, for instance Free and/or Open Source Software (FOSS)

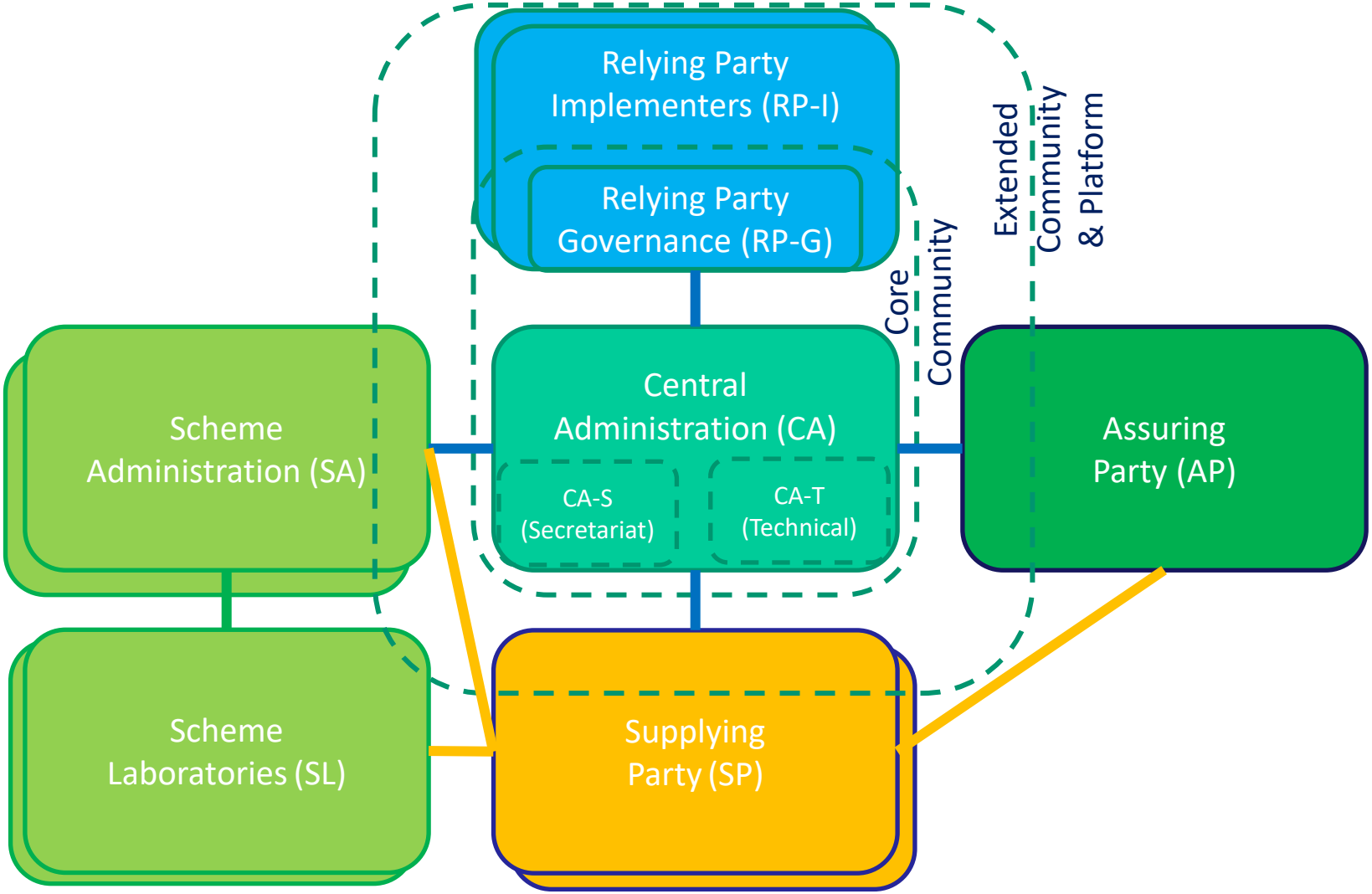
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- ➢ **What Is Needed Now?**
- What Is CUPA?
- How Is CUPA Used?
- Questions?

Understanding Assurance

- Trustworthiness can be characterised as a Spectrum, with widely accepted limits:
  - Optimal – Reviewed and endorsed by Trusted Party
  - Intolerable – Substantive rationale against from Trusted Party
- There are also middle areas:
  - Known:
    - Has been used by Trusted Parties, but not formally reviewed
    - Have encountered no substantive reasons to desist
  - Unproven:
    - Not known to be used by Trusted Parties, nor formally reviewed
    - No Open Source substantive reasons to desist
- Assurance Artefacts need to provide sufficient information to allow Relying Parties (RP) to place Commodities on the spectrum

Community Based Approach



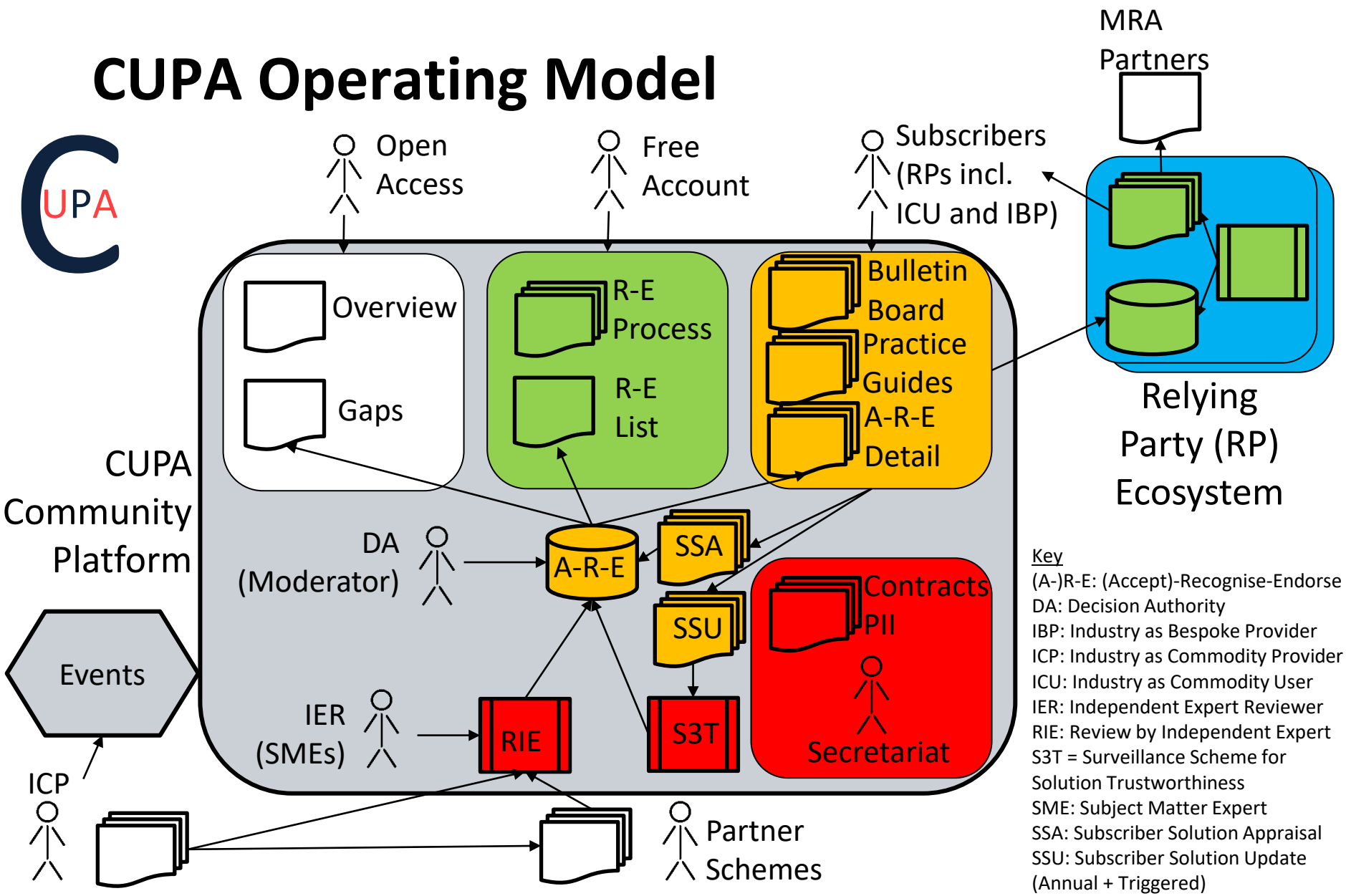
Function of Central Administration

- Support a Community-based and Owned approach to Trust and Confidence in Off The Shelf (OTS) Products and Services
- Provide interaction route(s) for
  - Understanding Stakeholder Demand
  - Documenting Use Cases
  - Establishing, maintaining, and expressing list of Gaps
- Standardise a spectrum of Assurance approaches
  - Establish and maintain way of Normalising, and levelling-up, multiple Schemes' outputs
  - Provide Configure-Operate-Maintain (COM) Consensus
  - Provide scalable and reusable input to multiple System / Platform / Infrastructure Approval
  - Establish and maintain Usage and Issue Monitoring

Trustworthy Selection and Use of Commodity Products and Services

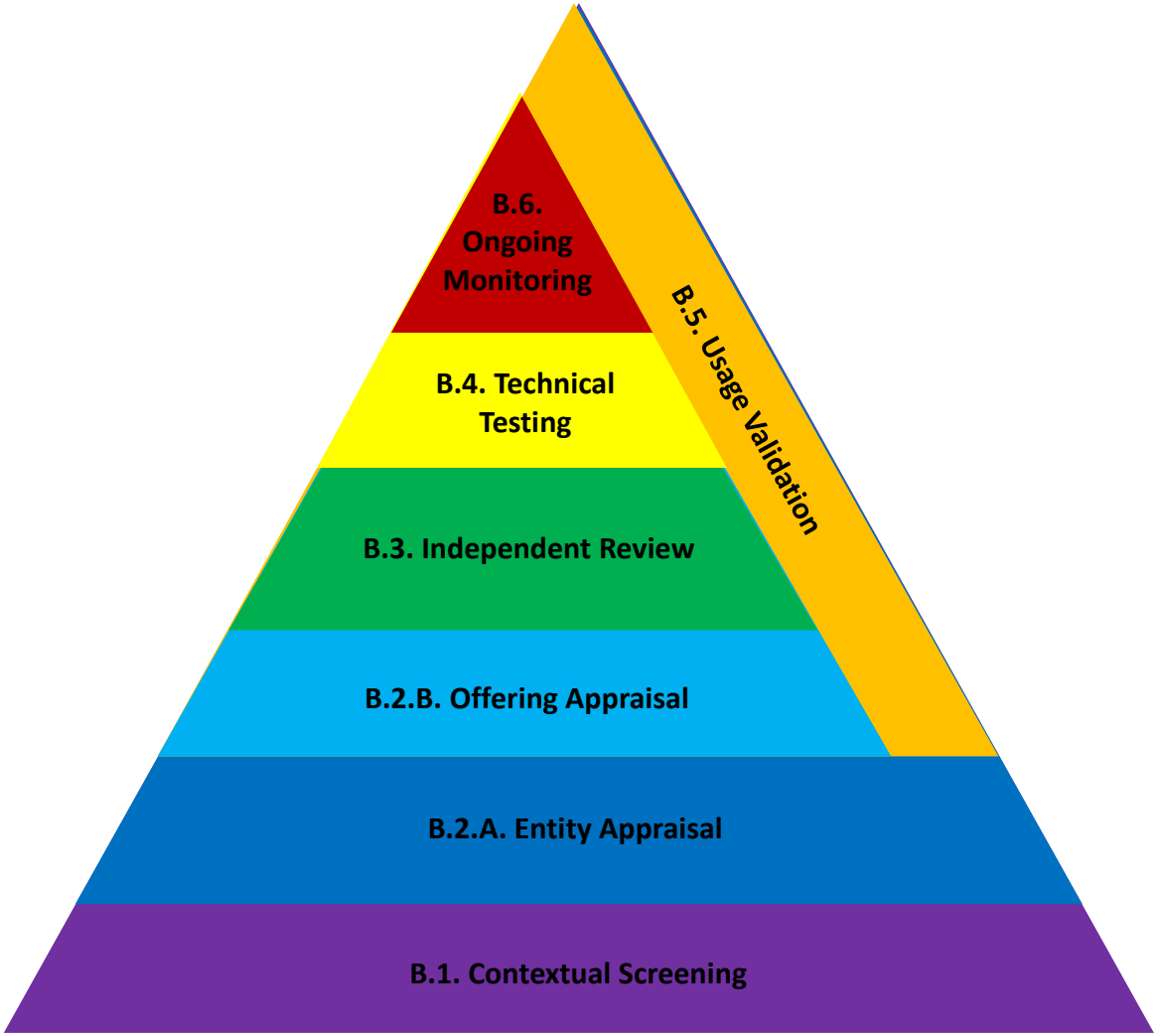
- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- ➢ **What Is CUPA?**
- How Is CUPA Used?
- Questions?

CUPA Operating Model



Key
(A-)R-E: (Accept)-Recognise-Endorse
DA: Decision Authority
IBP: Industry as Bespoke Provider
ICP: Industry as Commodity Provider
ICU: Industry as Commodity User
IER: Independent Expert Reviewer
RIE: Review by Independent Expert
S3T = Surveillance Scheme for Solution Trustworthiness
SME: Subject Matter Expert
SSA: Subscriber Solution Appraisal
SSU: Subscriber Solution Update (Annual + Triggered)

Elements of OTS Assurance



Spectrum of Assurance

Approach	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
Partner	✓	✓	✗	✗	✗	✗	✓
Appraisal	✓	✓	✓	✗	✗	✓	✓
Homologation	✗	✓	✓	✗	✗	✓	✓
Legacy	✓	✓	✓	✓	✗	✓	✓
Baseline (Bronze)	✓	✓	✓	✓	✗	✓	✓
Structured (Silver)	✓	✓ (TSM1+)	✓	✓	✓	✓	✓
Granular (Gold)	✓	✓ (TSM2+)	✓	✓	✓ (Susceptibility)	✓	✓
Proven (Platinum)	✓	✓ (TSM3+)	✓	✓	✓ (Adds Claims)	✓	✓

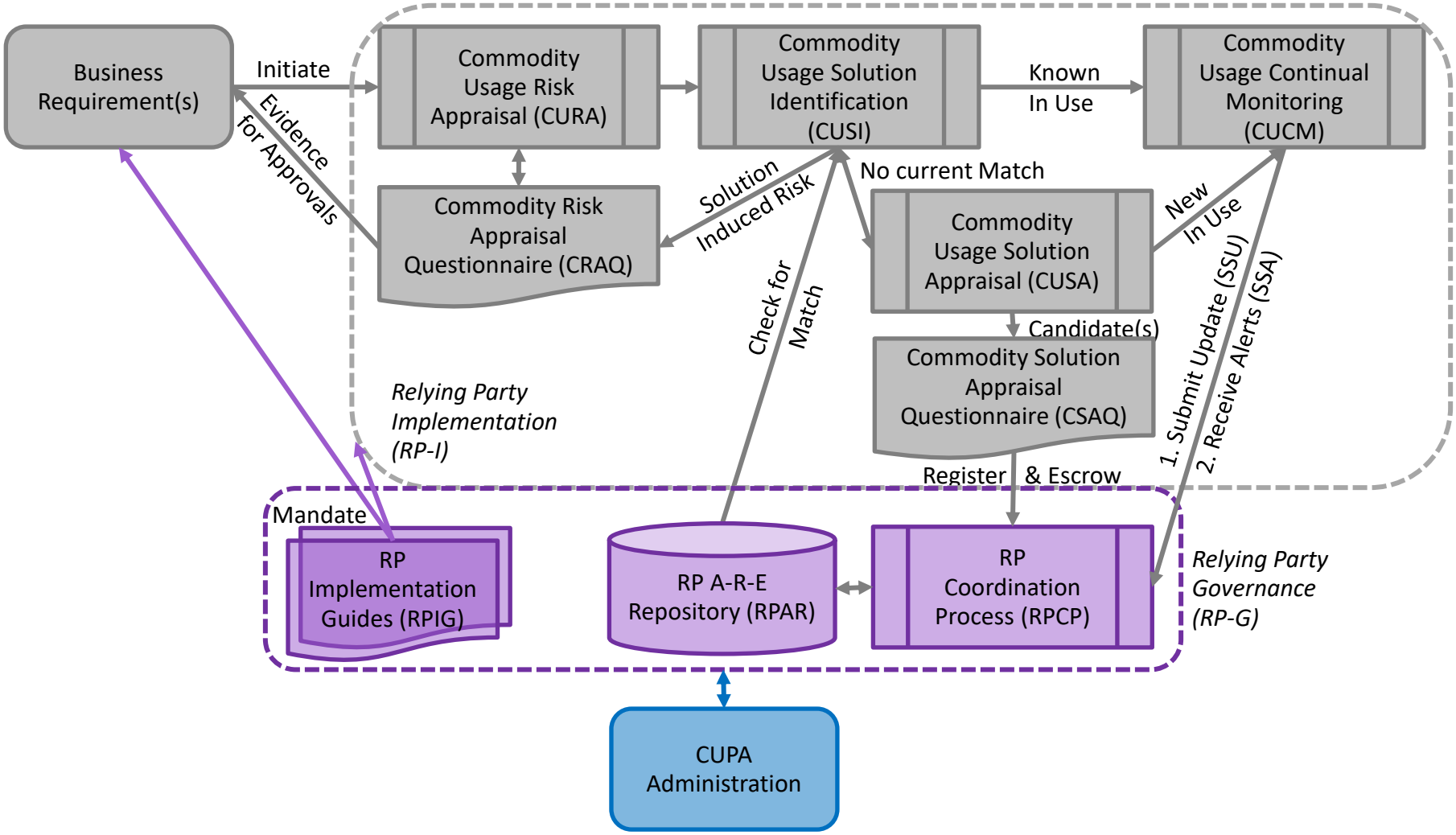
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- ➢ **How Is CUPA Used?**
- Questions?

Relying Parties and CUPA

- Central Governance (RP-G) responsible for:
  - Recognition of CUPA as Competent Body on behalf of own Organisation
  - Publication of Implementer's Guidance (e.g. Specific Risk Metrics for OTS selection, …) for own Organisation
  - Tracking of use of OTS across own Organisation
  - Contributing to CUPA Stakeholder Group on behalf of own Organisation
- Implementers (RP-I) responsible for:
  - Validating A-R-E Commodities as providing a Pragmatic, Appropriate, and Cost Effective (PACE), fit to their own use case(s), both for Suitability, and for Robustness
  - Reviewing A-R-E Cautions, SP Configure / Operate / Maintain documents, and SSA + Open Sources for new Susceptibilities
  - Providing Regular and Triggered updates (SSU) into CS3

Relying Party Management Process



Risk-based Selection of Commodities (1)

- A “one size fits all” Solution is not always appropriate
- For instance, when choosing a Rental Vehicle we can postulate a set of “Assets” and “Adversities”:

		Adversity			
		None	Sunshine	Snow	Distance
Assets	1/2 people + shopping	VS-1	VS-2	VS-3	VS-4
	3/4 people + luggage	VS-5	VS-6	VS-7/8	VS-9/10
	5/6 people	VS-11	VS-12	VS-13	VS-11/13

- Where VS = Vehicle Stratum

VS-0	(No Vehicle)	VS-7	SUV
VS-1	City Car	VS-8	AWD Saloon
VS-2	2 seater soft-top	VS-9	Saloon
VS-3	AWD sportscar	VS-10	Estate
VS-4	Grand Tourer	VS-11	MPV
VS-5	Compact	VS-12	AirCon'd MPV
VS-6	4 seater convertible	VS-13	Large SUV

- *(Implied VS only loosely match to the Rental Industry ACRISS / SIPP Codes)*
- Each RP will need to map its own Risk Approach to CUPA Levels

Risk-based Selection of Commodities (2)

- "PEILAT-S": suggested Criteria for Relying Parties to consider
- Initial Requirement – Solution Agnostic
  - Perimeters
  - Entities
  - Interconnections
  - Locales
  - Archetypes
  - Temporal
- Refined Requirement – adjust for Solution-induced Risks (SIR)
  - Solution
- Derive a Hierarchical Protection Requirement
  - Protection Goals (e.g. Threat Actors x Exposures)
  - Effort Expected (e.g. Due Care – Reasonable Effort – Best Effort)
- Map to the Assurance Levels produced by CUPA

Any Questions?

Paper Download: https://is.gd/wmgcsc073331

"*Septem Circumstantiae*"
from "Ethica Nicomachea"
Aristotle
(4th Century BCE)

Contact

Prof. Ian Bryant

Principal Investigator (UCR)

Room 253 International Manufacturing Centre
University of Warwick
University Road, Westwood Heath, CV4 7AL, England

i.bryant@warwick.ac.uk

+44 24-769-51924

https://is.gd/wmgcsc