



Trustworthy Software Initiative (TSI)

Sharing Data / Information

Update Briefing for TF-CSIRT
Thursday 26th September 2013, London, UK

Ian Bryant
TSI Technical Director

DMU/CSC/TS/2013/156
v1.0
2013-09-26

Speaker Profile

- (Principal Professional Engineer on Academic Sabbatical from HM Government)
- Technical Director at UK Trustworthy Software Initiative (TSI)
- Visiting Lecturer at De Montfort University (DMU) Cyber Security Centre (CSC)
- Deputy Panel Chair at British Standards Institution (BSI), shadowing ISO/IEC JTC1 SC27 WG4
- Co-Chair at UK National Information Assurance Forum (NIAF)
- Lead Information Security Expert for EU DG JLS Projects “MS3i” (2008-2009) and “NEISAS” (2009-2011) Projects

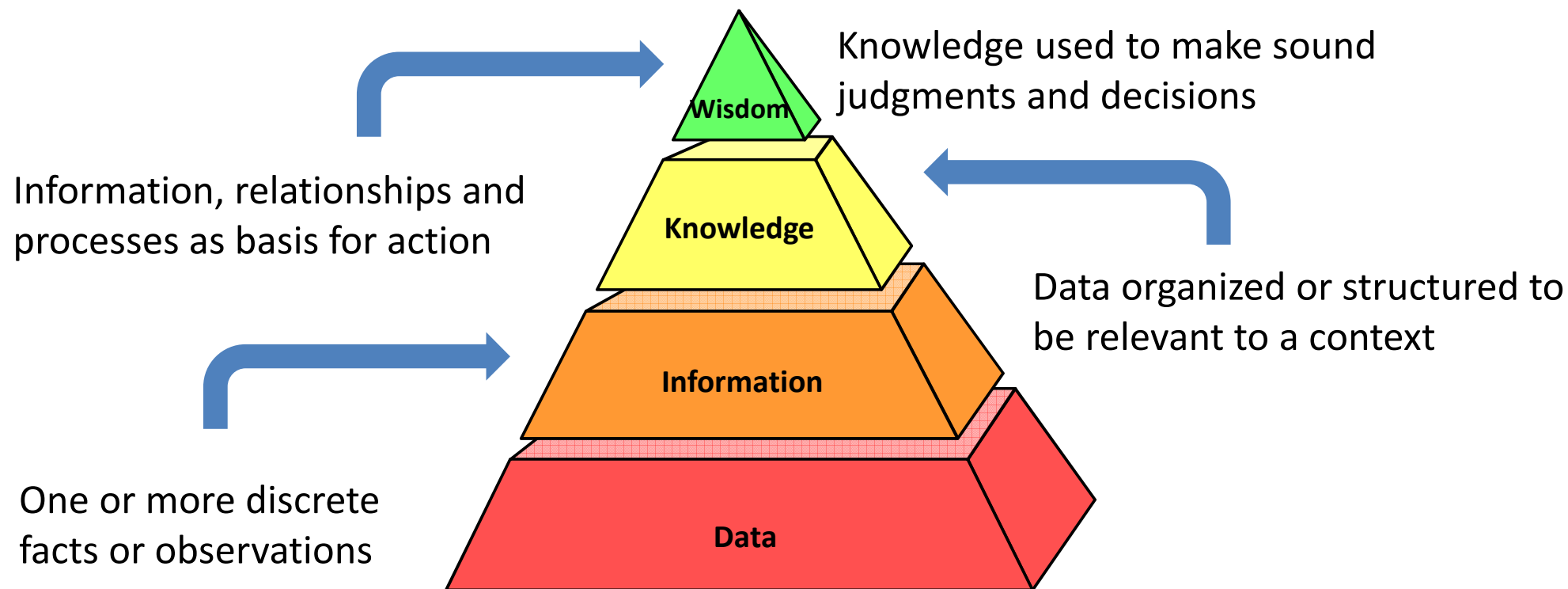


Acknowledgements



- The MS3i and NESIAS Projects were co-funded by the European Commission (EC), Directorate General for Justice, Freedom and Security (DG JLS) as part of the “*European Programme for Critical Infrastructure Protection*” (EPCIP) Programme under the original title: “*Messaging standards for computer network defence warnings and alerts*”
- It was performed with the support of the EC DG JLS “*Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*” Programme

Terminology: D – I – K – W





Data / Information Sharing – Previous TF-CSIRT Efforts

- TF-CSIRT has always had an interest in Data and Information Sharing
- Early output was Incident Object Description and Exchange Format (IODEF), which was donated to IETF
- Members have been active in Request Tracker for Incident Response (RT-IR)
- Working Group ran for a number of years on Vulnerability and Exploit Description and Exchange Format (VEDEF), but aborted when no consensus could be achieved with vendors

UK Trustworthy Software Initiative (TSI)

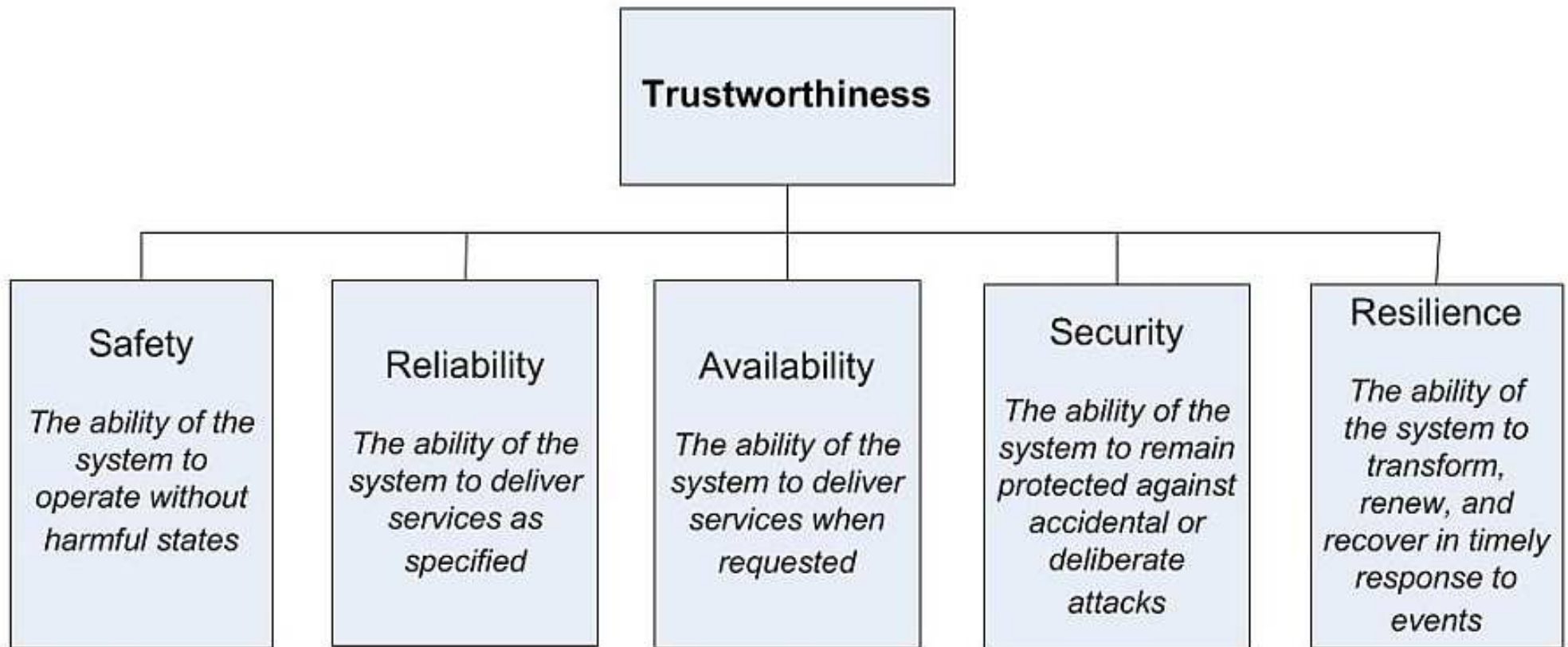
- Minister for the Cabinet Office Francis Maude, stated in respect of the Future Plans for UK's Cyber Security Strategy in December 2012:

“We support and fund the Trustworthy Software Initiative, which aims to improve cyber security by making software more secure, dependable and reliable, and to educate on why trustworthy software is important”

- TSI President, Sir Edmund Burton, describes the goal as being to provide a *“significant, strategic foundation for the UK Cyber Security Strategy”*
- TSI role is therefore to provide a *“Public Good initiative for cultural transformation”*



“Trustworthiness” Facets

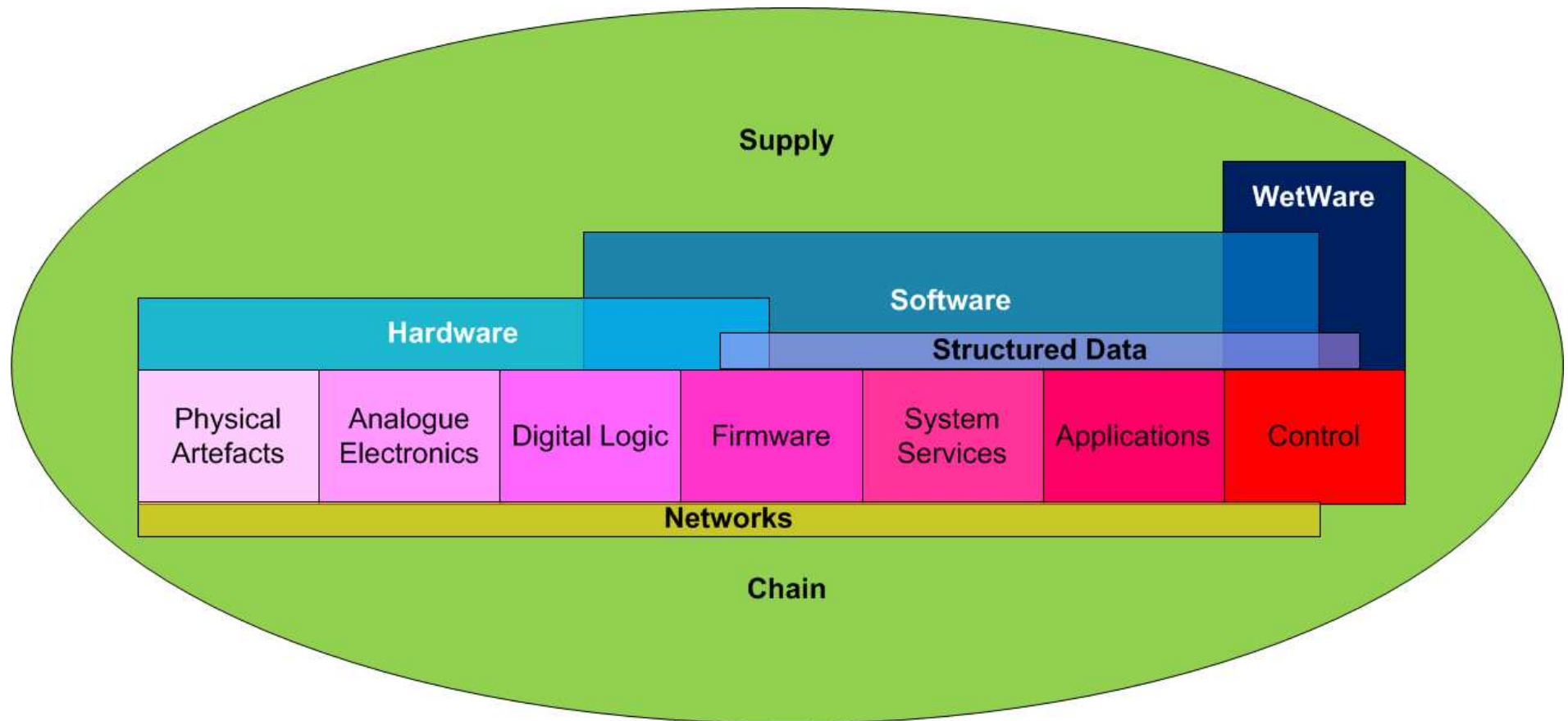


Security and Trustworthiness

| Management Concept | | | | |
|---------------------------|----------------------|------|-----------------------------|------------|
| Trustworthiness Component | Governance | Risk | Controls (P ³ T) | Compliance |
| Software Safety | Trustworthy Software | | | |
| Software Reliability | | | | |
| Software Availability | Cybersecurity | | | |
| Software Resilience | | | | |
| Software Security | | | | |
| Other | | | | |



Software in the Cyber Ecosystem



Software Incident Impact

- Software problems are high cost to economy:
 - US Government National Institute of Standards & Technology (NIST) ~\$60 billion / year to US alone
 - No definitive figure for UK / worldwide
- Software a major source of IT project failure:
 - University of Oxford Saïd Business School / McKinsey 2011; Standish Chaos Reports 2004 onwards; *et al*
- Software bugs “source of 90% of ICT Incidents”
 - (GovCERT-UK, 2012-09)
- Mitre’s Common Weakness Enumeration (CWE) is a maintained list of generic software weakness types
 - 918 distinct CWEs at v2.4

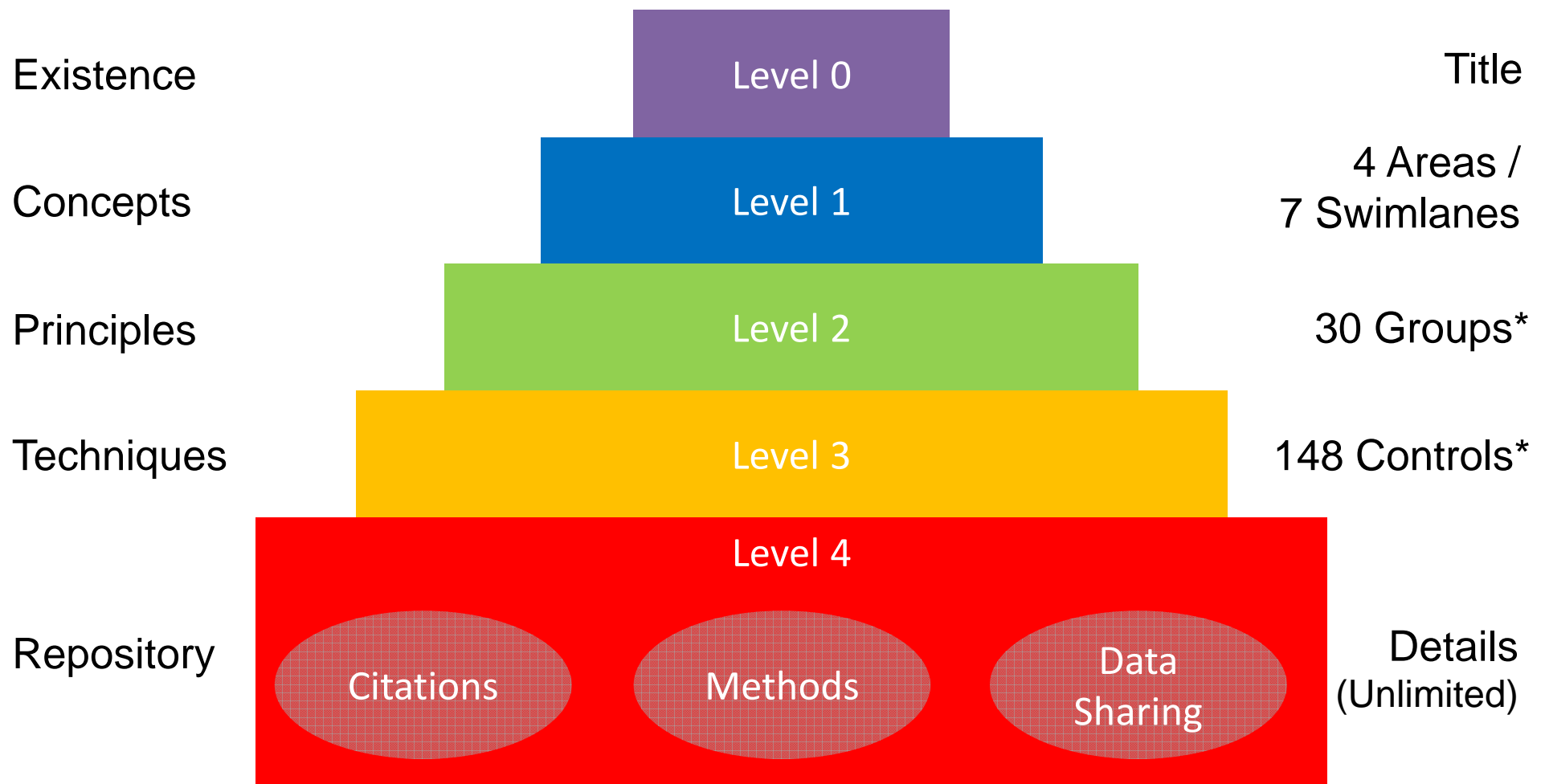


TSI Philosophy

- Many of principles and techniques needed for Trustworthy Software have existed for many years
- “Due Diligence” implies software should be **reasonably** trustworthy, although implementations vary with Audiences and Assurance Requirements
- TSI focuses on Pareto (“80:20”) approaches to *Making Software Better*, iteratively using existing learnings and interpreting them for Public Good
 - e.g. Switching on and acting on Compiler Warning Flags obviates many common “repeat offender” weaknesses



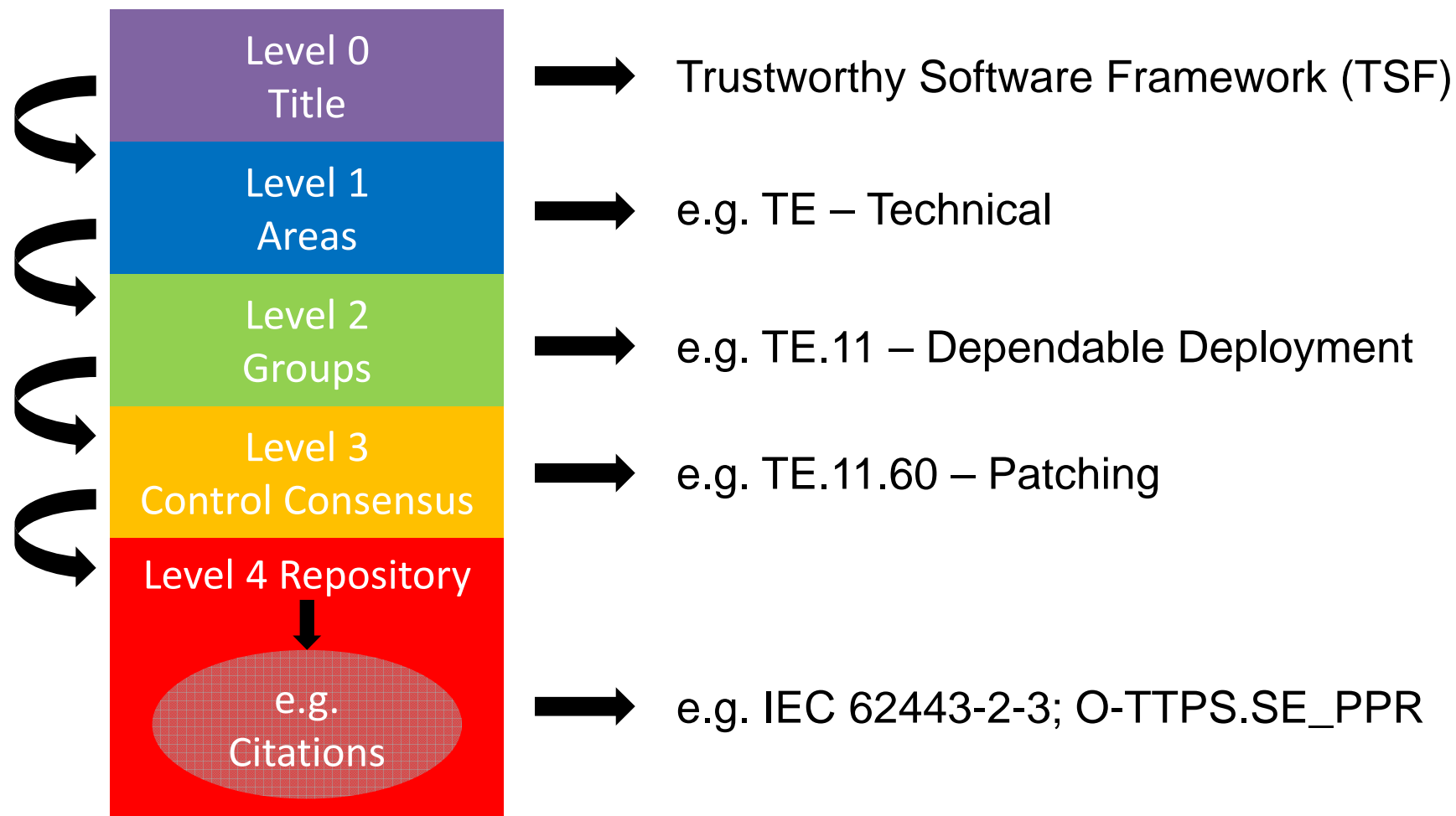
Trustworthy Software Framework (TSF) - Structure



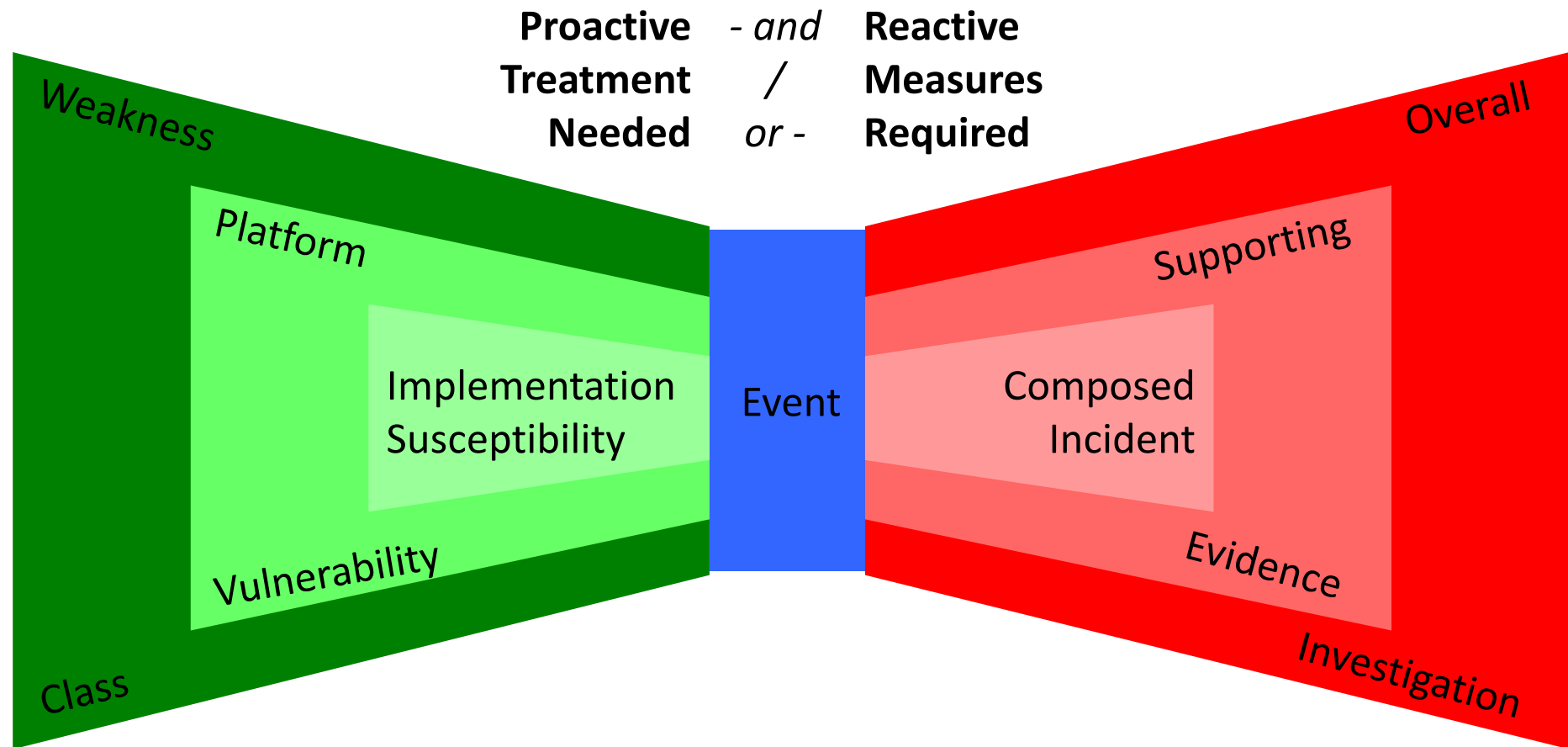
* At Version 2.3 (September 2013)



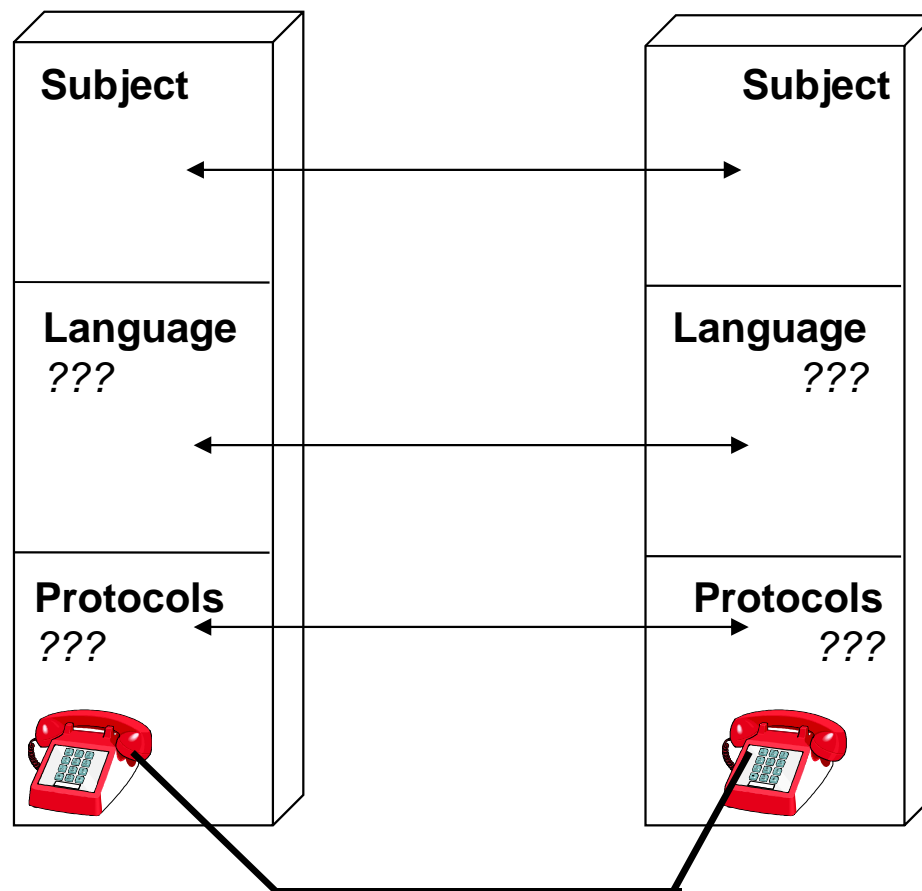
Trustworthy Software Framework (TSF) - Use



Data and Information Sharing: Bow Tie LifeCycle Example



Visualisation of Sharing Challenge





Challenges with modelling trust in (potentially *ad hoc*) data / information sharing environments:

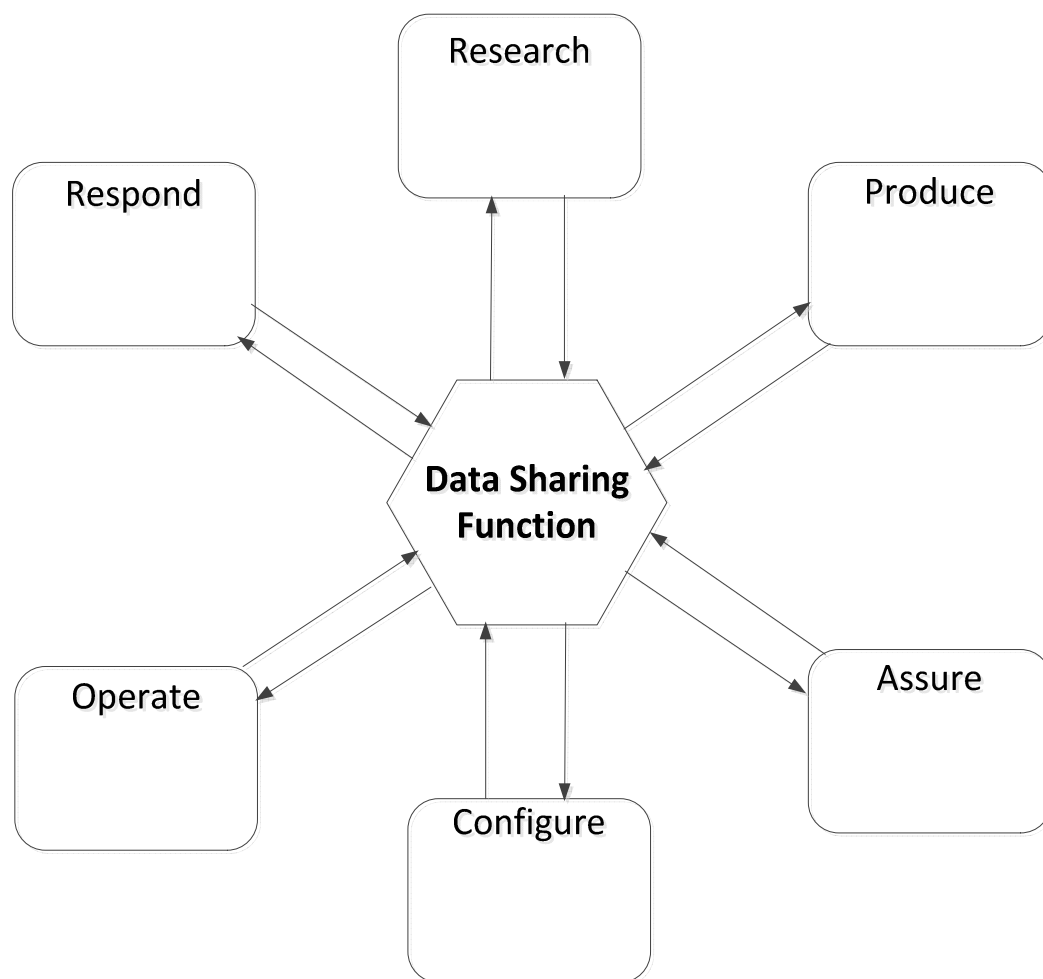
- The Communities are not necessarily aligned to the natural Circles of Trust
- The communities may not share either a common language and/or ontology
- The communities may not know trustability of *ad hoc* partners

Perception and Cognitive Bias

| | |
|--|--|
| <p>Perceptual Biases</p> <p>Expectations. We tend to perceive what we expect to perceive. More (unambiguous) information is needed to recognize an unexpected phenomenon.</p> <p>Resistance. Perceptions resist change even in the face of new evidence.</p> <p>Ambiguities. Initial exposure to ambiguous or blurred stimuli interferes with accurate perception, even after more and better information becomes available.</p> | <p>Biases in Evaluating Evidence</p> <p>Consistency. Conclusions drawn from a small body of consistent data engender more confidence than ones drawn from a larger body of less consistent data.</p> <p>Missing Information. It is difficult to judge well the potential impact of missing evidence, even if the information gap is known.</p> <p>Discredited Evidence. Even though evidence supporting a perception may be proved wrong, the perception may not quickly change.</p> |
| <p>Biases in Estimating Probabilities</p> <p>Availability. Probability estimates are influenced by how easily one can imagine an event or recall similar instances.</p> <p>Anchoring. Probability estimates are adjusted only incrementally in response to new information or further analysis.</p> <p>Overconfidence. In translating feelings of certainty into a probability estimate, people are often overconfident, especially if they have considerable expertise.</p> | <p>Biases in Perceiving Causality</p> <p>Rationality. Events are seen as part of an orderly, causal pattern. Randomness, accident and error tend to be rejected as explanations for observed events. For example, the extent to which other people or countries pursue a coherent, rational, goal-maximizing policy is overestimated.</p> <p>Attribution. Behavior of others is attributed to some fixed nature of the person or country, while our own behavior is attributed to the situation in which we find ourselves.</p> |

Source:
"A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis", US Central Intelligence Agency (CIA),
 March 2009

Data Sharing - “Boundary Objects”



- A mutually recognized means of Data Sharing across domain and/or linguistic boundaries
- Used to encapsulate one or more discrete facts or observations

- An Information Sharing Agreement is a means for willing parties to assume and document obligations amongst themselves
- In multi-jurisdictional cases, these need to consider:
 - Generic legal requirements for Agreements
 - Legal issues specific to Information Sharing
 - Approaches as laid down in Standards
 - Trust Models

Data Sharing Formats – Standards Bodies

| Acronym | Name |
|----------|---|
| CPNI | Centre for Protection of National Infrastructure |
| DFRWS | Digital Forensics Research Workshop |
| FIRST | Federation of Incident Response Security Teams |
| ICASI | Industry Consortium for Advancement of Security on the Internet |
| IETF | Internet Engineering Task Force |
| ITU | International Telecommunications Union |
| MSM | Making Security Measurable |
| NISCC | National Infrastructure Security Coordination Centre |
| NIST | National Institute for Standards and Technology |
| NHTCU | National Hi-Tech Crime Unit |
| NSA | National Security Agency |
| OMG | Object Management Group |
| RTG-031 | NATO RTO - Research Task Group 31 |
| SecDEF | Security Description and Exchange Format |
| TagVault | TagVault |
| TF-CSIRT | Task Force on Computer Security Incident Response Teams |



ISO/IEC 27010:2012 – Information Security – Management of inter-sector and inter- organizational communications

- **Trust:** The Standard should support trust in the messages received. This could include verification and validation of the information source, as well as the value of the content and how it should be handled.
- **Interoperability:** The ability of the Standard to support messages between a variety of computing systems and a variety of operational users.
- **Adoptability:** The Standard should be straightforward and cost effective to adopt, aligned to the needs of businesses and governments.
- **Robustness:** The Standard should be resistant to failures, both at a technical and understanding level.
- **Speed:** The Standard should not impose undue constraints on performance, providing the ability to deliver timely information through a number of different channels.
- **Flexibility:** Messages from a variety of sources and provenance ratings should be accommodated. Given the changing nature of information, the Standard should also be able to adapt and grow as the needs evolve.
- **Clarity:** The Standard should support the sharing of information which is in a form that is unambiguous.
- **Compliance:** The Standard should support compliance to the different regulatory and legal regimes across different sectors and member states.
- **Enabler:** The Standard should be seen as an enabler for other standards which have a need to share information and referenced where appropriate.
- **Automation:** The Standard should support the automated transfer and handling of messages, using a number of technical standards.

Data Sharing Formats - LifeCycle



Data Sharing Formats – Initial Inventory

| | | | |
|-----------------|--|-----------------|---|
| ARF | Assessment Result Format | ISI | Information Security Indicators |
| ARF | Abuse Reporting Format | KDM | Knowledge Discovery Metamodel |
| ASR | Assessment Summary Results | MAEC | Malware Attribute Enumeration and Characterization |
| CAP | Common Alerting Protocol | MARF | Messaging Abuse Reporting Format |
| CAPEC | Common Attack Pattern Enumeration and Classification | OpenIOC | Indicators of Compromise |
| CCE | Common Configuration Enumeration | OVAL | Open Vulnerability and Assessment Language |
| CDESF | Common Digital Evidence Storage Format | PLARR | Policy Language for Assessment Results Reporting |
| CEE | Common Event Enumeration | RID | Real-time Inter-network Defense |
| CPE | Common Platform Enumeration | RT | Request Tracker |
| CSAIF | Cyber Situational Awareness Indicator Format | RTIR | Request Tracker for Incident Response |
| CVE | Common Vulnerability Enumeration | SACM | Structured Assurance Case Metamodel |
| CVRF | Common Vulnerability Reporting Format | SBE-NS | Signing, Binding and Encryption Namespace |
| CVSS | Common Vulnerability Scoring System | SBVR | Semantics of Business Vocabulary and Business Rules |
| CWE | Common Weakness Enumeration | SCAP | Security Content Automation Protocol |
| CWRAF | Common Weakness Risk Analysis Framework | {SR-DEF} | Security Requirement DEF |
| CWSS | Common Weakness Scoring System | SWID | Software ID (tags) |
| CVSS | Common Vulnerability Scoring System | SWIF | Structured Warning Information Format |
| CyBOX | Cyber Observable Expression | STIX | Structured Threat Information Expression |
| {EI-NS} | Event and Incident Namespace | TAXII | Trusted Automated Exchange of Indicator Information |
| {EI-SS} | Event and Incident Scoring System | {VADEF} | Verification Activity DEF |
| {EIRAF} | Event and Incident Reporting and Analysis Format | {VEDEF} | Vulnerability and Exploit DEF |
| {FIDEF} | Forensic Investigation DEF | VERIS | Vocabulary for Event Recording and Incident Sharing |
| {HT-DEF} | Hazard and Threat DEF | VEXWM | Vulnerability and Exploit eXtensible Weighting Metric |
| IDMEF | Intrusion Detection Message Exchange Format | XACML | eXtensible Access Control Markup Language |
| IL-NS | Information Labelling Namespace | XCCDF | Extensible Configuration Checklist Description Format |
| IODEF | Incident Object DEF | | |





- Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)
 - Arose from 16 Nation Multi-National Experiment 7 (MNE7)
 - Defence, Suppliers and Critical Industry Sectors
- Information Sharing Framework (ISF) aims to *“increase organisations’ cyber Situational Awareness (SA), enabled by sharing information across a trusted community of interest”*
- Intention is for DST inventory to be transferred to MACCSA custody as part of ISF

Questions ?



TSI : UK's Public Good initiative for Making Software Better

Contact

Ian Bryant

Technical Director T S I

TSI Office

Gateway House pp4.30

De Montfort University - Cyber Security Centre

The Gateway, Leicester, LE1 9BH, England



ian.bryant@uk-tsi.org

[+44 79 7312 1924](tel:+447973121924)

www.uk-tsi.org

[\(Twitter: @uktsi\)](https://twitter.com/uktsi)



TSI : UK's Public Good initiative for Making Software Better