ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

INFORMATION EXCHANGE FRAMEWORK

POLICY-DRIVEN, DATA-CENTRIC INFORMATION SHARING AND SAFEGUARDING (ISS)

SUPPORTING CYBER SITUATIONAL AWARENESS

December 2016

DISCUSSION OBJECTIVES

- Requirements for Cyber Information Sharing and Safeguarding
  - Threat-Risk / Response
  - Intelligence
  - Situational Awareness
- Information Exchange Framework (IEF) Objectives
- Information Exchange Framework (IEF) Approach and Components
- Benefits of the IEF approach

INTELLIGENCE / CYBER INTELLIGENCE

The practices, methods and technologies used to gather, store, report, and analyze business/operational data in order inform business decisions

The Practices, method and technologies use to gathering, store, analyze and report threat, risk and response data In order to track, assess and counter digital security threats

ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

SITUATIONAL AWARENESS
(A DEFINITION)

The ability to maintain cognizance or awareness of the pertinent elements and events in the environment in order to effectively conduct operations and achieve desired outcomes

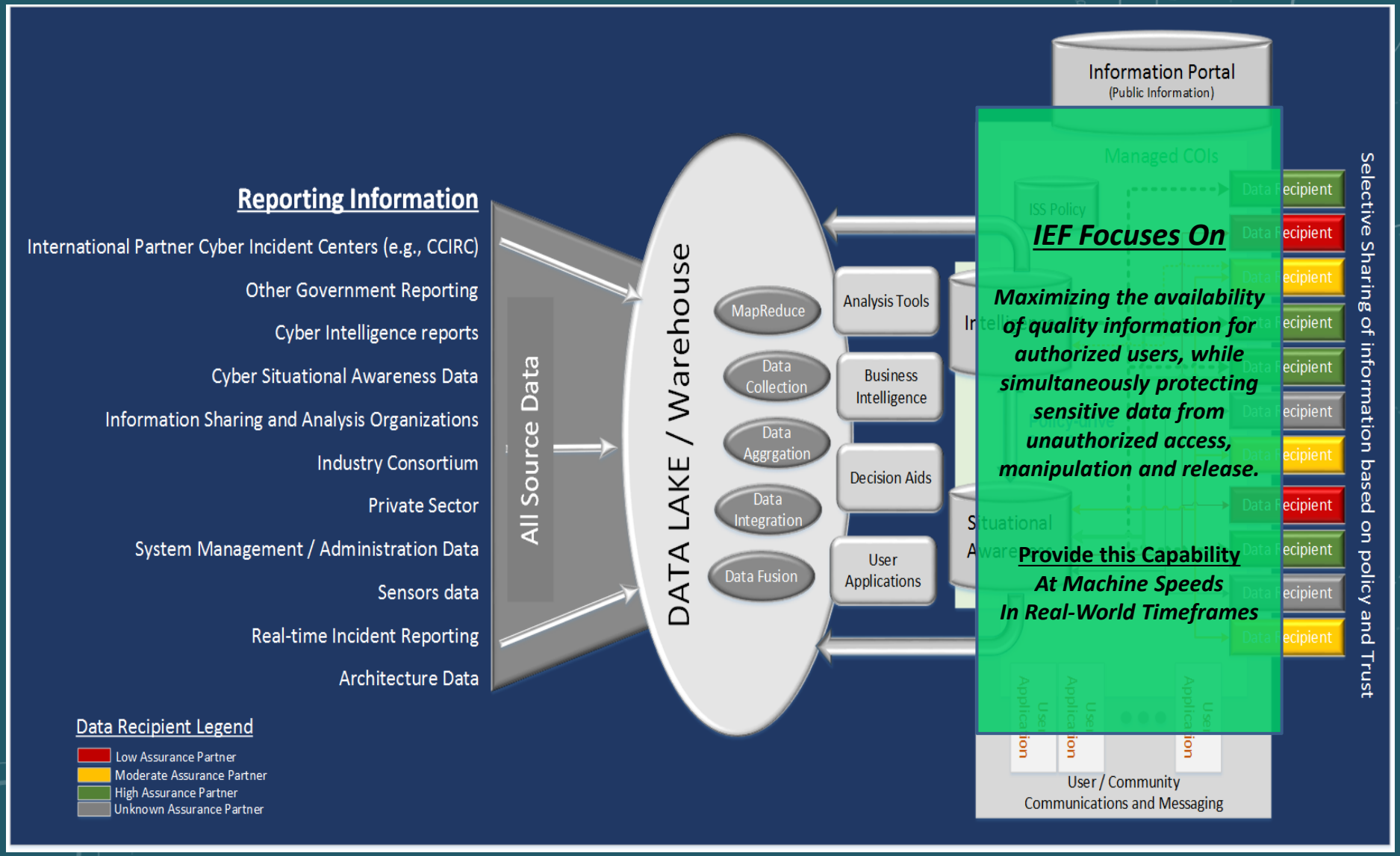
The ability to maintain cognizance or awareness of the pertinent elements and events in the environment in order to effectively conduct operations and achieve desired outcomes

Network Awareness

Threat / Risk Awareness

Mission / Operational Awareness

REPRESENTATIVE CYBER INFORMATION FLOW



ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

SITUATIONAL AWARENESS CHALLENGE

Is An Information Sharing and Safeguarding Challenge

Data Rich - Information Poor

Providing Information that informs decisions (Actionable)

Delivering the "Right Information – Right Person – Right Time"

Achieving a Historic and Future Requirement

Increasing the Willingness of Internal/External Partners to Share Information

Both Partners Inside and Outside an Organization are Reluctant to Share Cyber Information
Change Culture across a Broad Community of Partners
Require Policy that Authorizes the Sharing of Cyber Information

Adapting to Change

Threats Change, Missions/Operations Change, Partners Change, Policies Change
No plan survives first contact with adversaries

Designing Capabilities and Solutions for Tomorrow's Requirements

The only constant about ISS requirements is change
Flexibility, Agility, adaptability and sustainability need to be architected into ISS solutions

SITUATIONAL AWARENESS SOLUTIONS SEEK TO DELIVER QUALITY INFORMATION

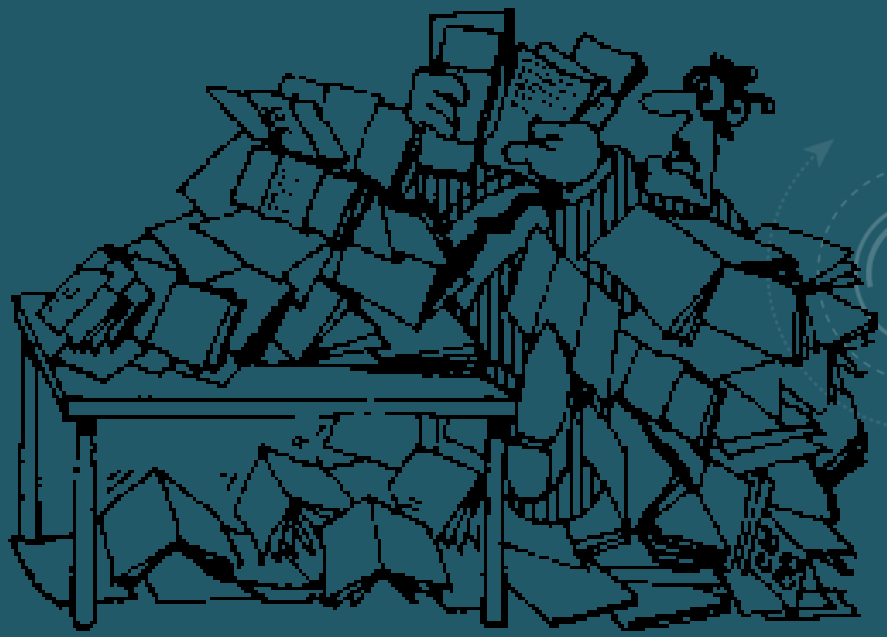
User want Information that has the following qualities:

- Timely
- Accurate
- Current
- Actionable
- Complete
- Concise
- Accessible
- Relevant
- Consumable / Understandable
- Reliable
- **Trusted**

Information:

(1) Data in context

(2) Data that informs decisions



Right Information, Right Person, Right Time

BUILDING BLOCKS OF A SA STRATEGY/SOLUTION

1. Separation of Concerns

- Policy Development separated from Application/System Development
- Best Practices for the Development & Management of the Policies governing 'access to' and the 'release of' data and information elements (translation of policy into machine executively rules and constraints)

2. Policy-driven Data-centric Information Sharing and Safeguarding (ISS)

- Traceability from Policy Instrument to Implementation
- Defence in depth (Securing the data ('THE ASSET') vs. the networks, platforms, infrastructure and applications)
- Increased flexibility, agility and adaptability
- User (Data Owner) control over the release of information

3. Open Standards (Community Accepted Specifications)

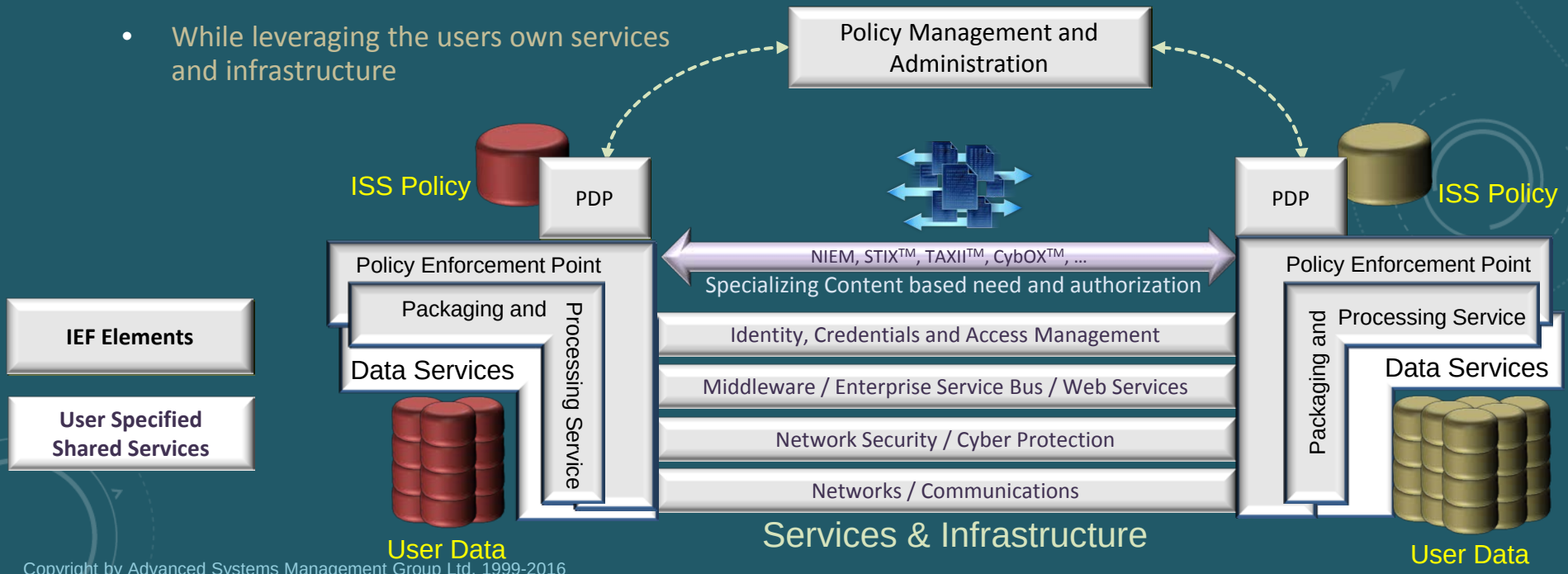
- Access to industry leading practices and knowledge
- Higher levels of interoperability
- Competitive Procurement / Multiple vendors and integrators
- Shared (common) services, platforms and infrastructure (Available through multiple sources / vendors, Interoperable)
- Risk Mitigation

4. Integration of User Solutions and Infrastructure

INFORMATION SHARING AND SAFEGUARDING (ISS) SERVICES

- There is a lot more to the delivery of interoperability then Semantics defined by the common canonical information models (e.g., NIEM, CAP, EDXL, etc.)
- The Information Exchange Framework (IEF) is seeking to:
  - Align the required capability
  - While leveraging the users own services and infrastructure

IEPD: Information Exchange Package Document
PPS: Packaging and Processing Services
PEP: Policy Enforcement Point
PDP: Policy Decision Point
PAP: Policy Administration Point



ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

IEF OBJECTIVES

1. Separation of Concerns: Separate the development and management of ISS rules from the technology needed to enforce it

2. Policy-driven Data-centric Information Sharing and Safeguarding automating ISS to individual data and Information Elements

3. Machine Speeds: Machine speed:
   - Tagging and labelling of information assets
   - Adjudication of Data, Access and Release Policy

4. Selective Sharing of Information elements between users based explicit rules and constraints mapped to policy instruments and trust profiles

5. Rapid Adaptation to ISS to accommodate changes in operational context (threats, missions, partners, roles, …)

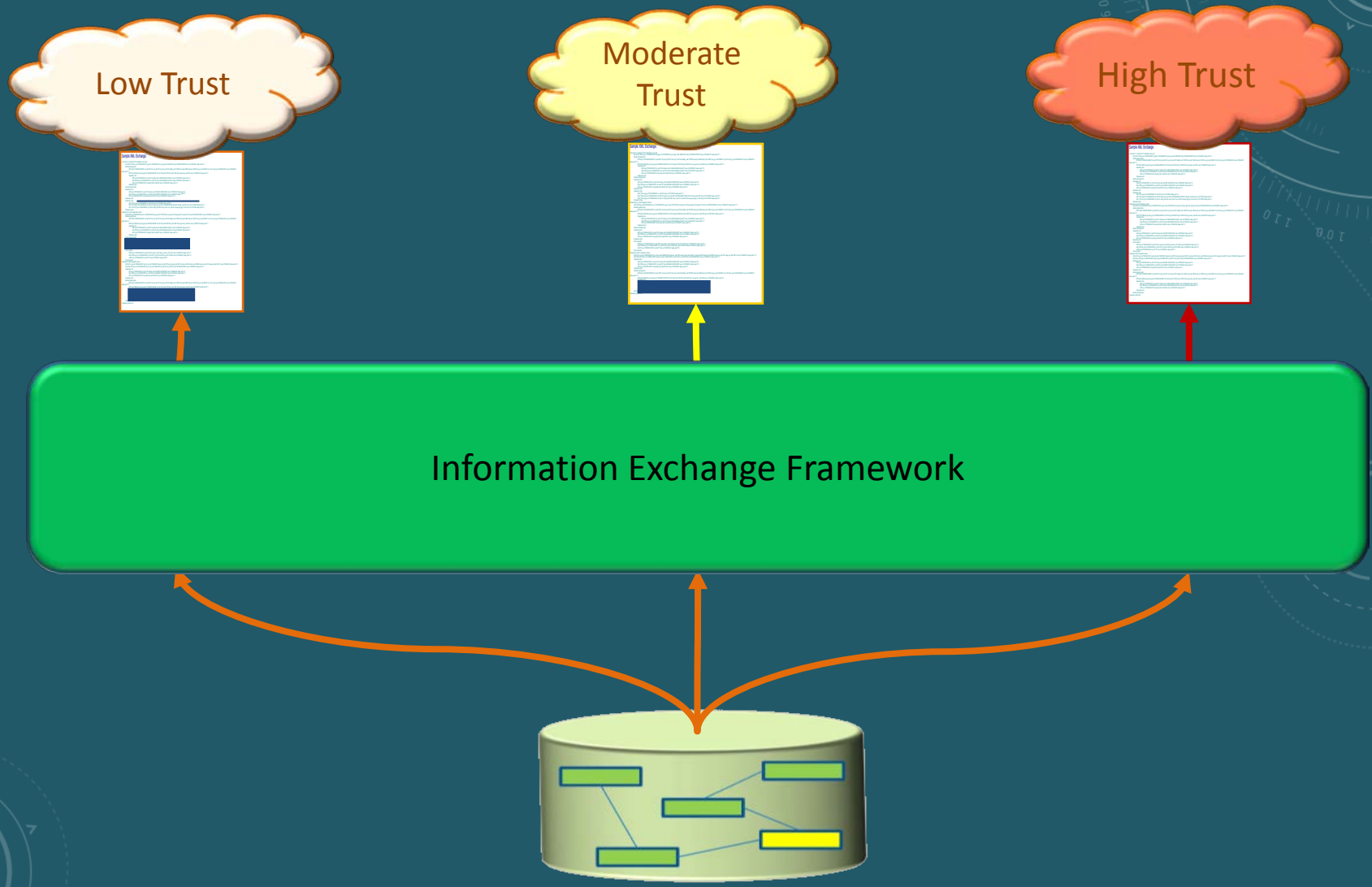
6. Raise Stakeholder Trust Levels through explicit capture of ISS policy, integrated into architecture, and governance

IEF – IMPLEMENTATION GOALS

- NOT a rip-and-replace capability: Leverage existing investments in infrastructure and systems, providing an efficient mechanism to integrate and interoperate
- Eating the elephant in small bites: Approach encourages incremental implementation
- Customer Self Served: Add new data, data sources, policies and rules as needed
- Maturity and Risk controls: Implementation pace aligned with organizational maturity and risk tolerance

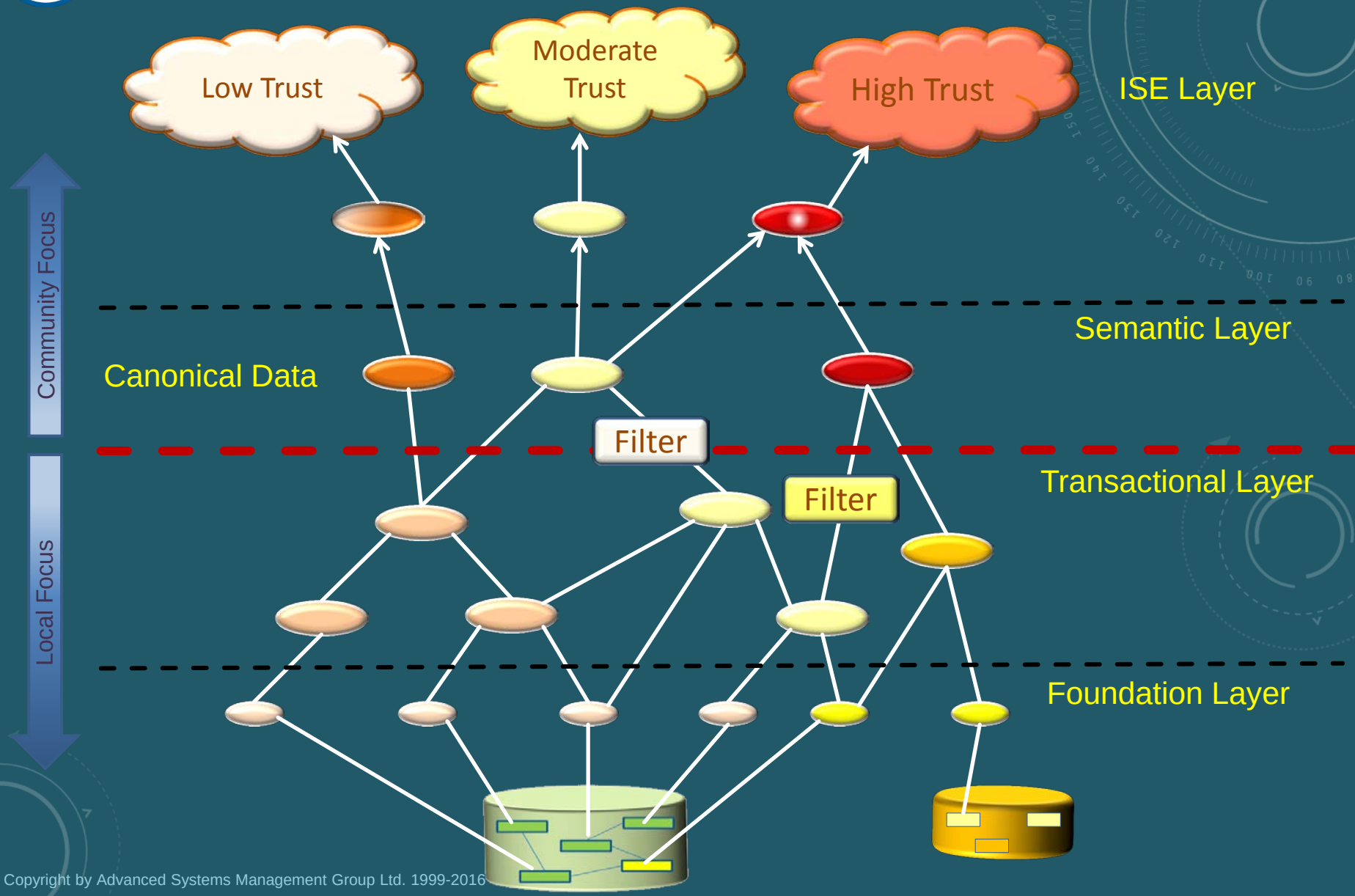
SELECTIVE SHARING OF CONTENT

SECURITY / TRUST /QOS / …

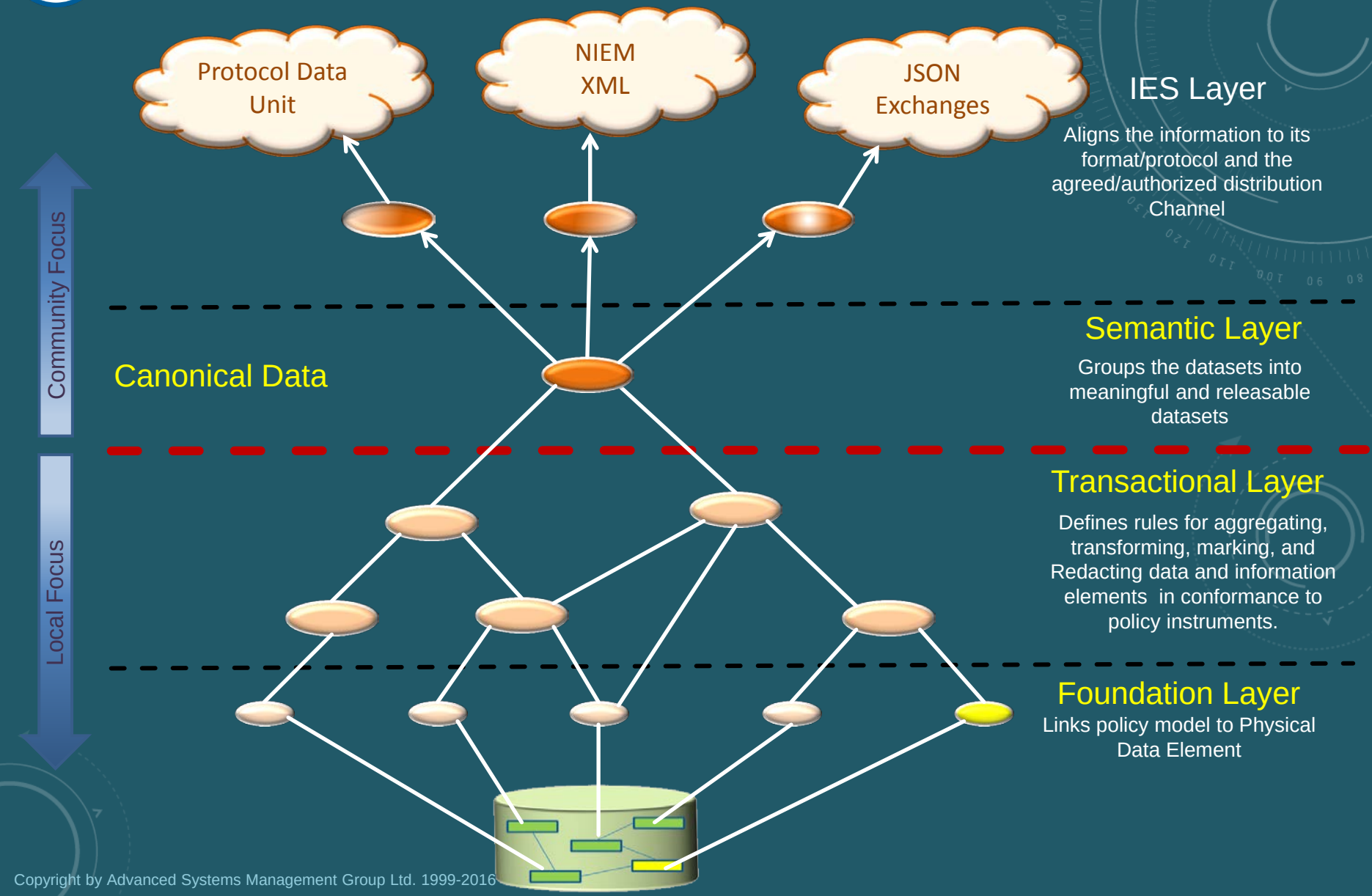


ASMG
ADVANCED SYSTEMS
MANAGEMENT GROUP

SHARE THE CONTENT USING AGREED PROTOCOLS



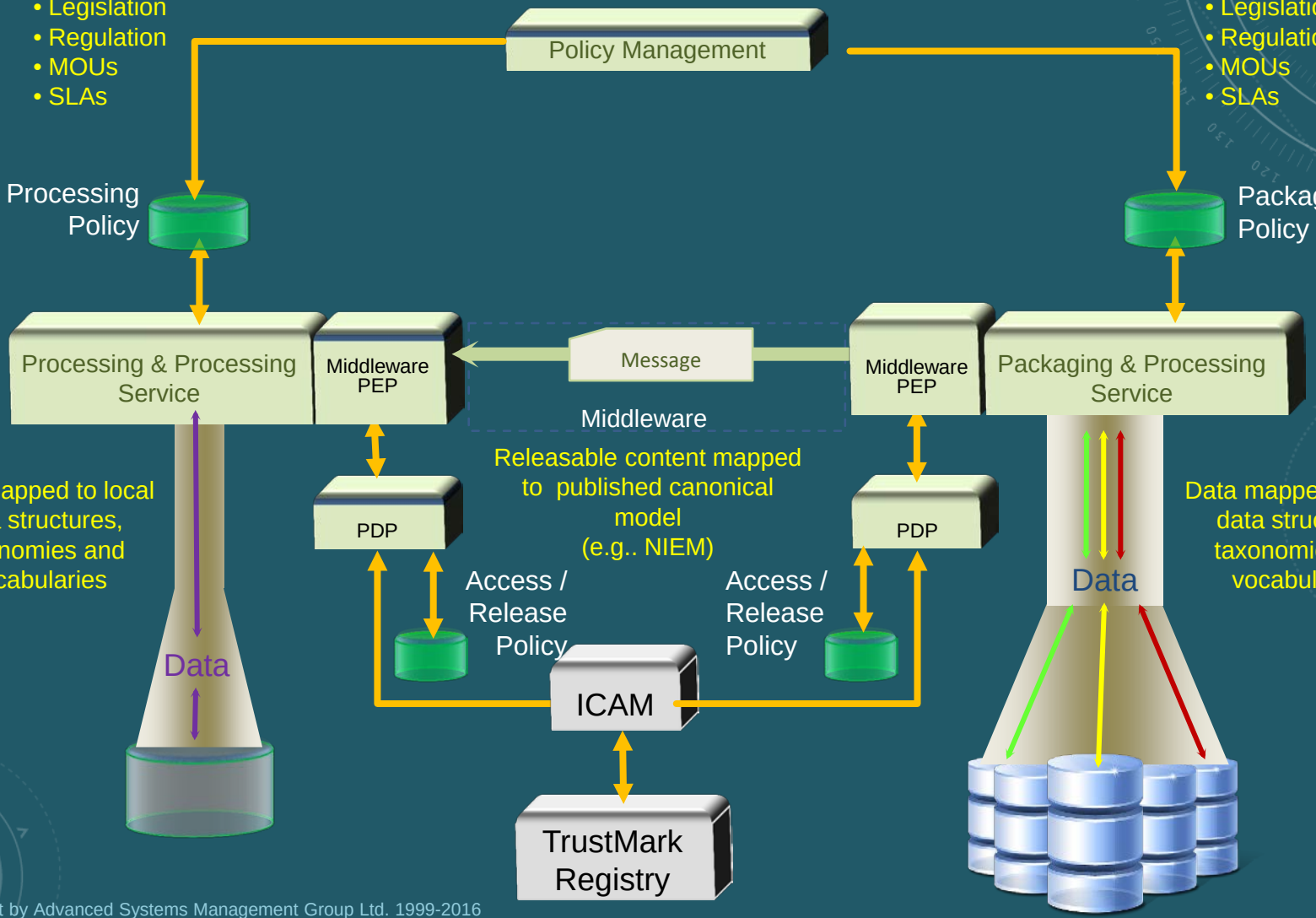
SHARING USING DIFFERENT PROTOCOLS



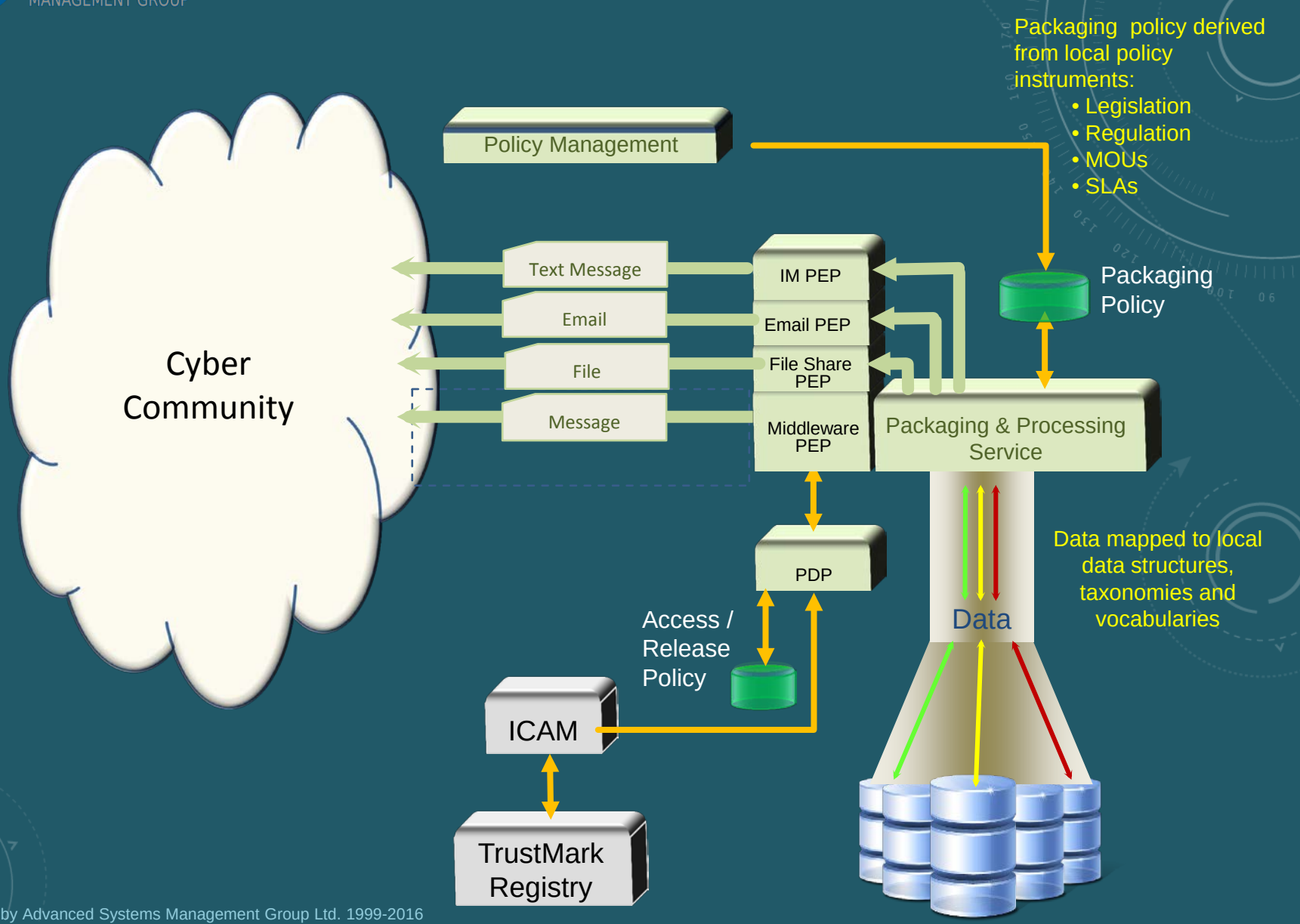
ENABLE MULTIPLE EXCHANGE CAPABILITIES AND USER CAPABILITIES

ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

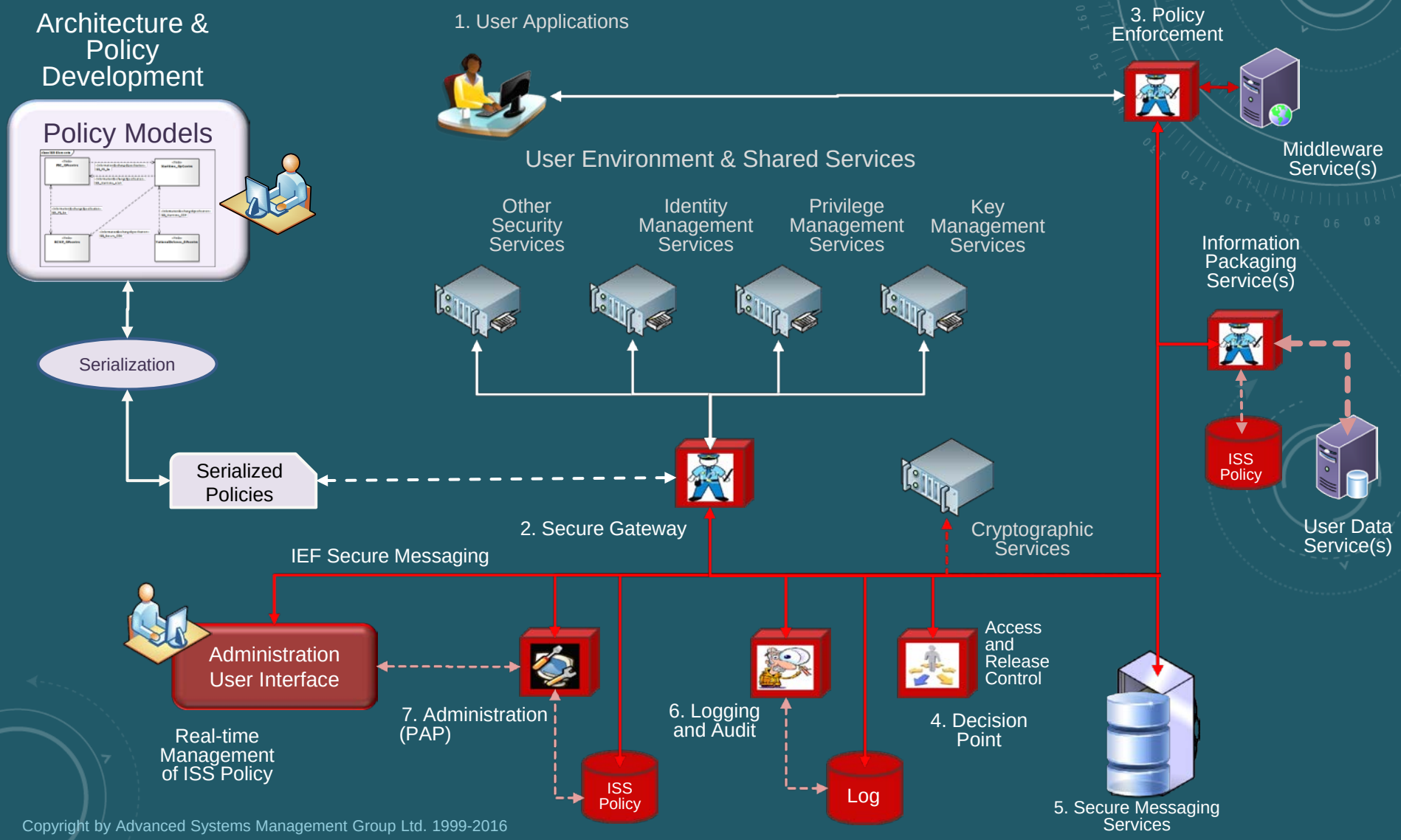
Packaging policy derived from local policy instruments:
- Legislation
- Regulation
- MOUs
- SLAs



ENABLE MULTIPLE EXCHANGE CAPABILITIES AND USER CAPABILITIES



IEF ACCESS AND RELEASE CONTROL



BENEFITS OF THE APPROACH

(Reduced cost and Risk)

- Integration of policy development into architecture frameworks in order to:
  - Provide traceability to legislation, regulation, MOUs, SLA, and Operating Procedures
  - Retain Institutional Memory (knowledge and information)
  - Deliver model driven management and model driven architecture (MDA), which reduces development time, risk and cost
- Enable a Policy development life-cycle, auditing and governance
- Separate the policy development and solution development life-cycles enabling and evolutionary development of ISS capability – do not need all the requirement on day one
- Moving to a standards based approach that will deliver more vendors, products and services, yielding:
  - Competitive acquisition
  - Reduced risk of vendor lock-in
  - Reduce the risks associated with aging IT
  - Increased opportunity for leveraging shared services (as-a-service)
  - Higher adoption rate with partner agencies
- Broad-based Information Sharing and Safeguarding capability using a common framework, services and infrastructure

Mike Abramson

Special Adviser on public safety/security Open Interoperability Standards to Centre for Security Sciences (CSS)

Co-Chair C4I DTF

Chair IEF WG

President Advanced Systems Management Group (ASMG) Ltd.

265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1

Fax: 613-231-2556

Phone: 613-567-7097 x222

Email: abramson@asmg-ltd.com

WHY OPEN STANDARDS

- Targeting open standards will lower total costs (TOC) and increase returns on investment (ROI) by providing the following benefits:
  - Increased Levels of Interoperability
  - Vendor neutrality / Competition
  - Efficient use of existing resources
  - Greater use of automation
  - Increased Flexibility and Agility
  - More options provide more opportunities to optimize
  - Lower and manageable risk
  - Robustness and durability
  - Higher Quality
  - Increase available skills
  - Reduced Life-cycle Cost
- Open Standards will enable users to address unique operational needs, while enabling interoperability with partners
- Provide access to subject matter expertise that is not locally available