Security and Privacy within an Intelligent Sensor Grid

Somalia,Strong Resolve (Norwegen), Adventure Exchange (Spanien), Roving Sands (USA), Determined Effort (Jugoslawien), Battle Griffin (Norwegen), IFOR, SFOR, KFOR, Central Enterprise, Enduring Freedom, ISAF

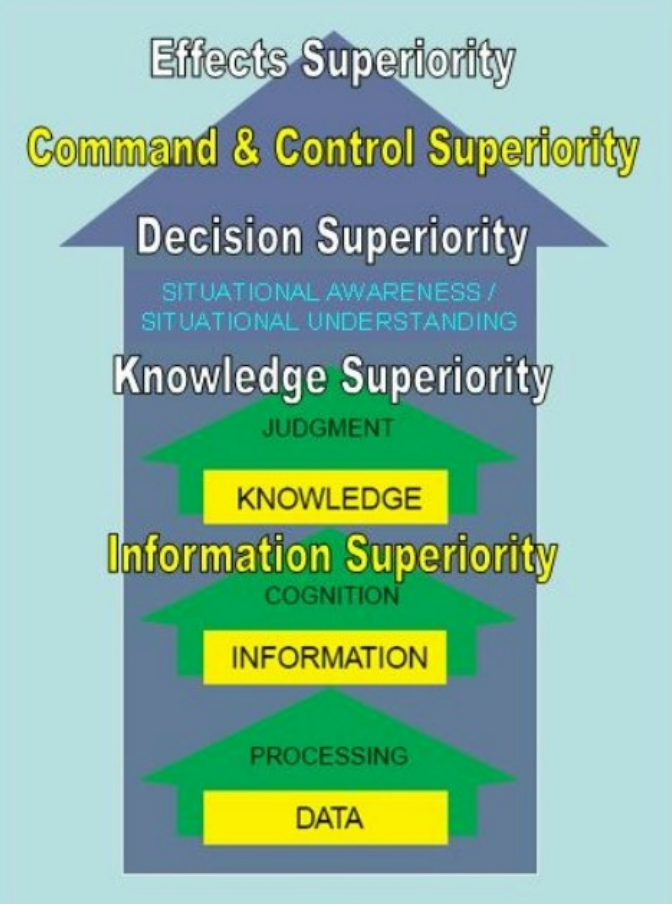
11th International Command and Control Research and Technology Symposium
Coalition Command and Control in the Networked Era

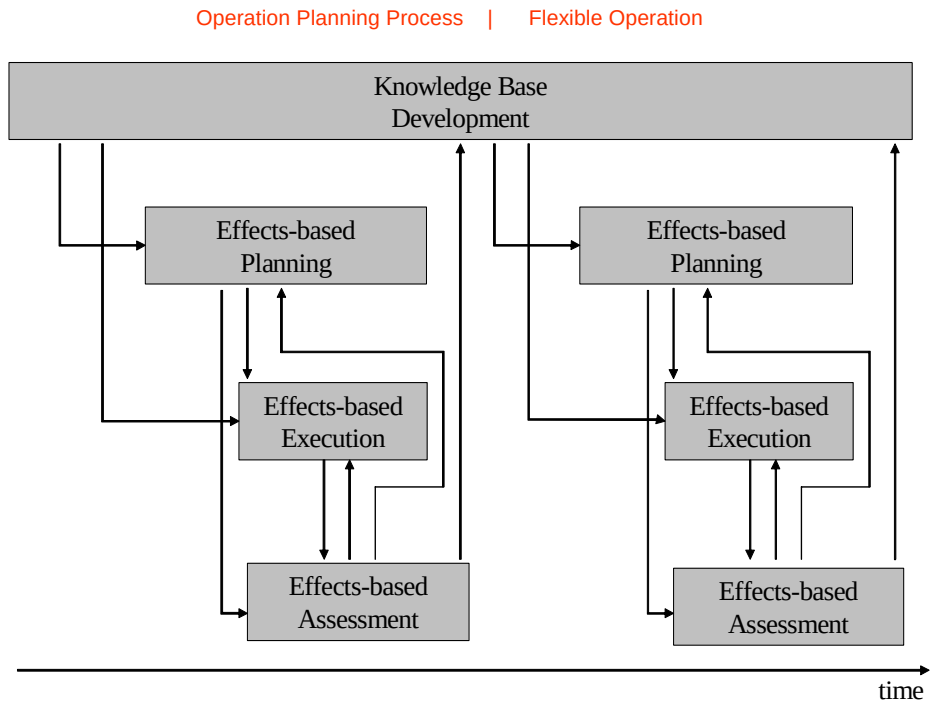
Margarete Donovang-Kuhlisch, mdk@de.ibm.com

Agenda

- Effects-Based Planning and Operation
- High-Level Enterprise Architecture & Business Model
- Technical Architecture Approach for an ISG
  - Service Oriented Architecture
  - Secure Enterprise Bus
- Security & Privacy
  - IT as a Business
  - Management Domains
  - Identity Federation & Regulatory Compliance (Privacy)
- Semantic Models – evolving Management Infrastructure
- Q&A

Concept of Effects-Based Planning & Operation (EBO)

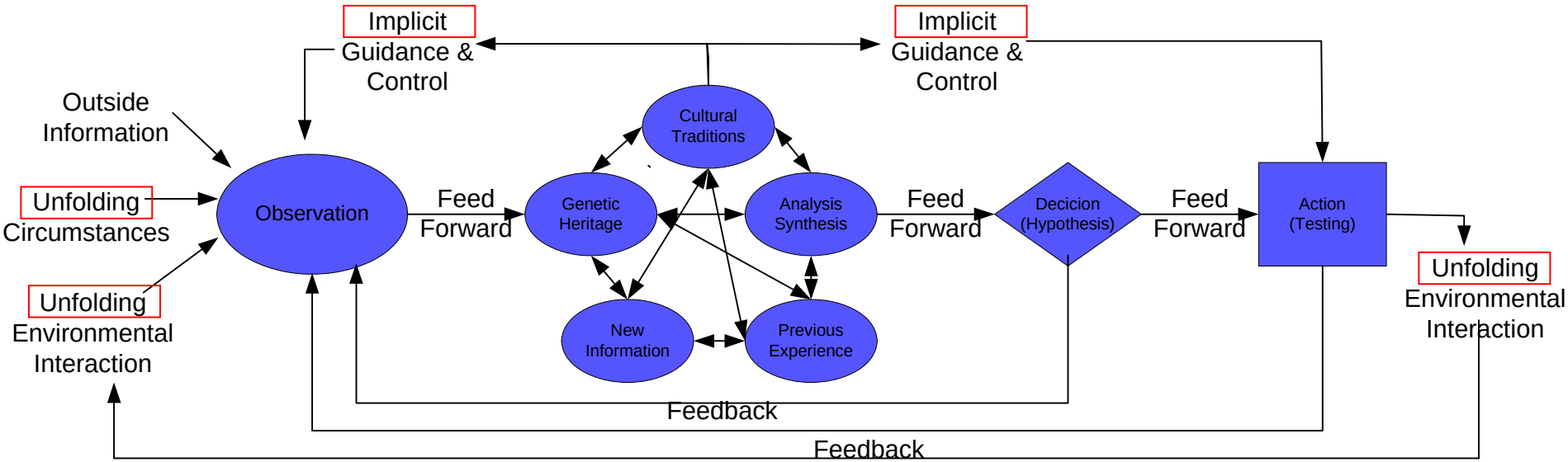


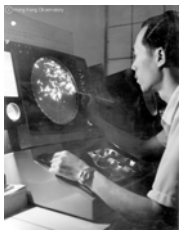


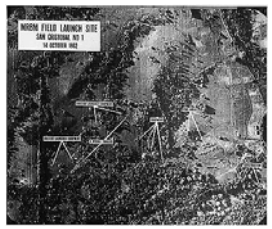
Source: MNIOE White Paper: InfoOp in Future Coalition Operation (Multinational Information Operations Experiment)

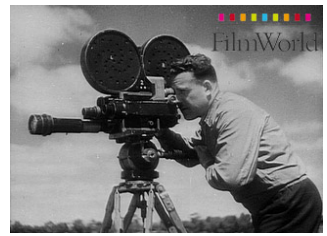
EBO – Partial Automation of the OODA Cycle thru KBD

Observation **Orientation** **Decision** **Action**





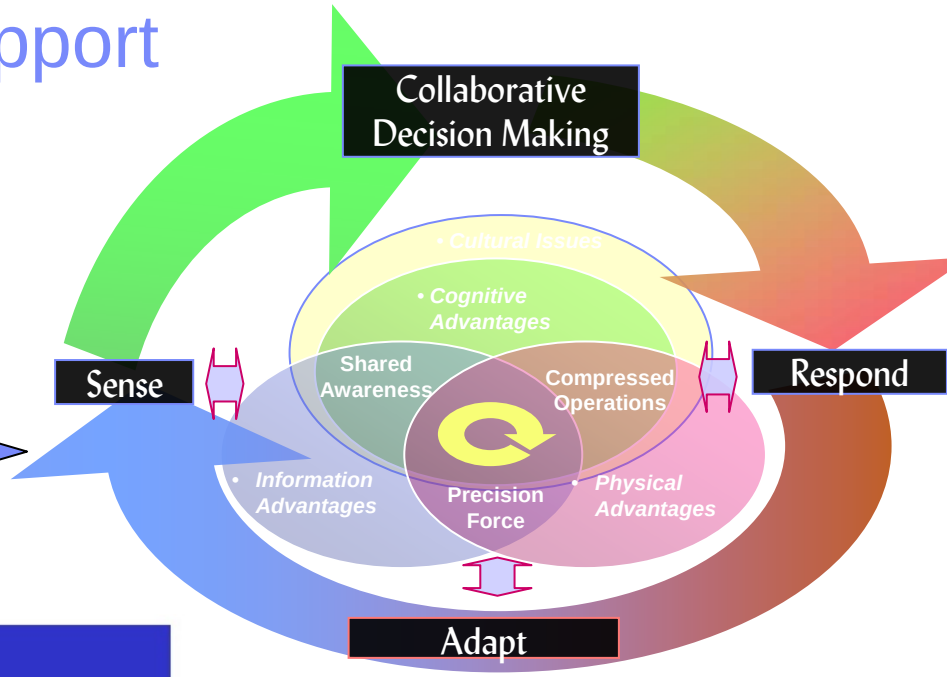




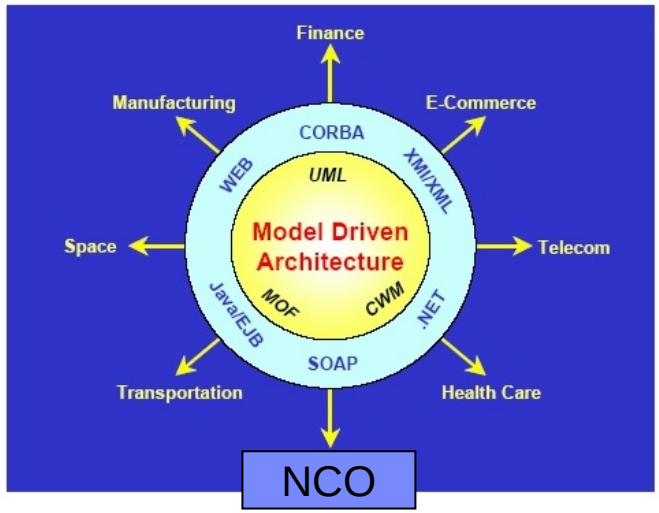
Mission Specific Decision Support

Mission:
EBO

ESB
SOA
ITIL



Generic „Business“ Model
OODA/SoSA



NCO

- ESB: Enterprise Service Bus
- SOA: Service Oriented Architecture
- ITIL: Information Technology Infrastructure Library
- OODA: Observe, Orient, Decide, Act
- SoSA: System of Systems Analysis
- NCO: Network Centric Operation

Schaffung eines einsatzspezifischen on demand Business

Sense&Response Operation – Terms & Characteristics

Department of Defense vision…		
Flexible	*Light*	*Agile*

"We learned on September 11, 2001,that our nation is vulnerable to enemies who hide in caves and shadows and strike in unexpected ways. That is why we must transform our armed forces. Our forces need to be flexible, light, and agile, so they can respond quickly and deal with surprise. The same is true of the man and women who support the Department of Defense. They also need flexibility so that they can move money, shift people, design and deploy new weapons more rapidly and respond to the continuing changes in our security environment." – *Secretary of Defense, Donald Rumsfeld*

A company whose business processes—integrated end-to-end across the company and with key partners, suppliers and customers—can respond with flexibility and speed to any customer demand, market opportunity or external threat. An on demand business has four key attributes: it is responsive, variable, focused and resilient.

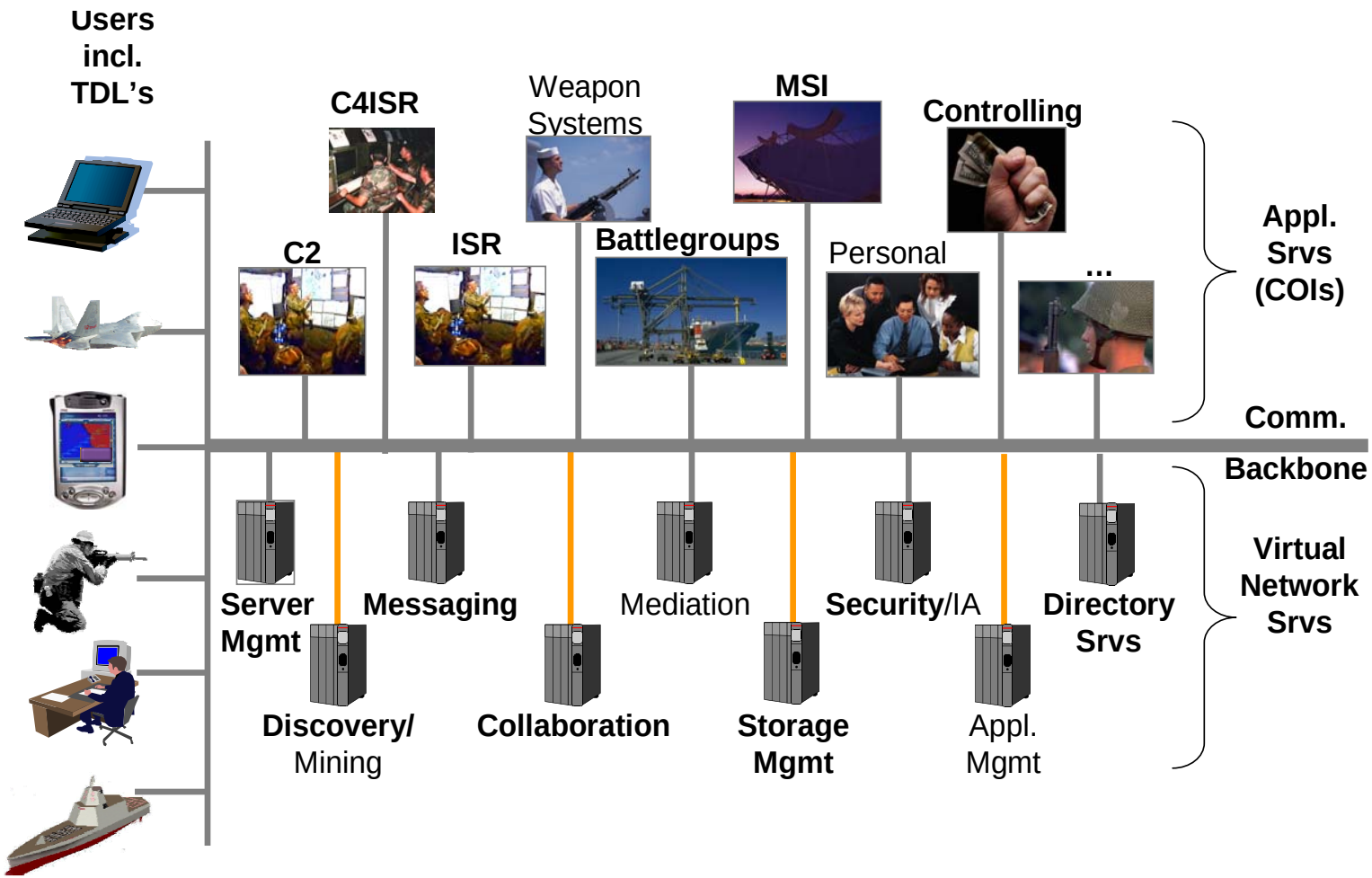
ON DEMAND BUSINESS™

Adaptive, Continuous, Concurrent, and Collaborative Planning -- AC3P

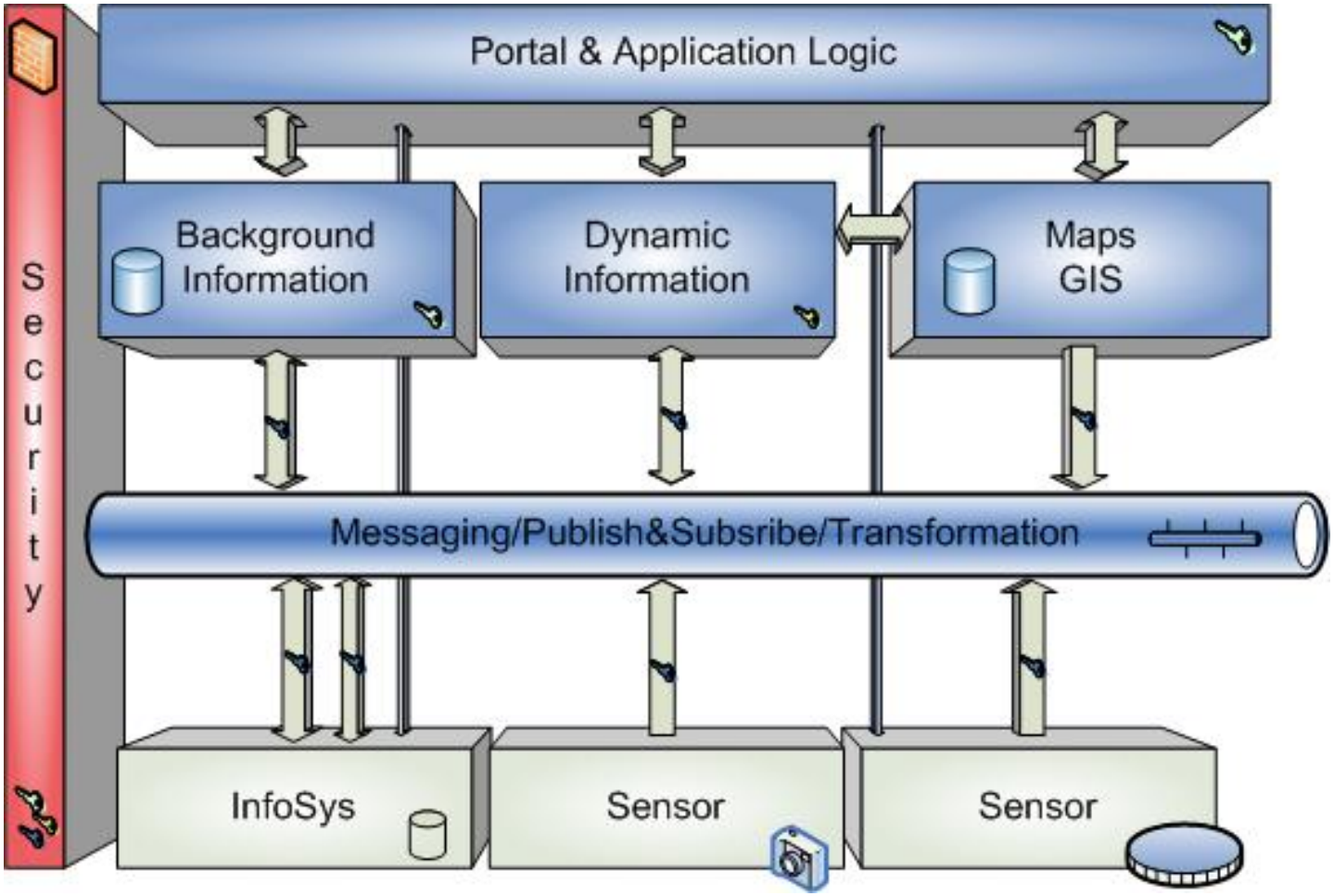
Overall Hypothesis

If a collaborative information and contemporary operating environment can be constructed that will provide the capabilities for seamless connectivity and interoperability between Services, Stakeholders, and Partners, and there is transparency in the use of the tools to accomplish missions, then the Adaptive, Continuous, Concurrent, and Collaborative Planning Process will provide the mechanisms for Anticipatory Understanding to provide Decision Superiority over the Adversary.

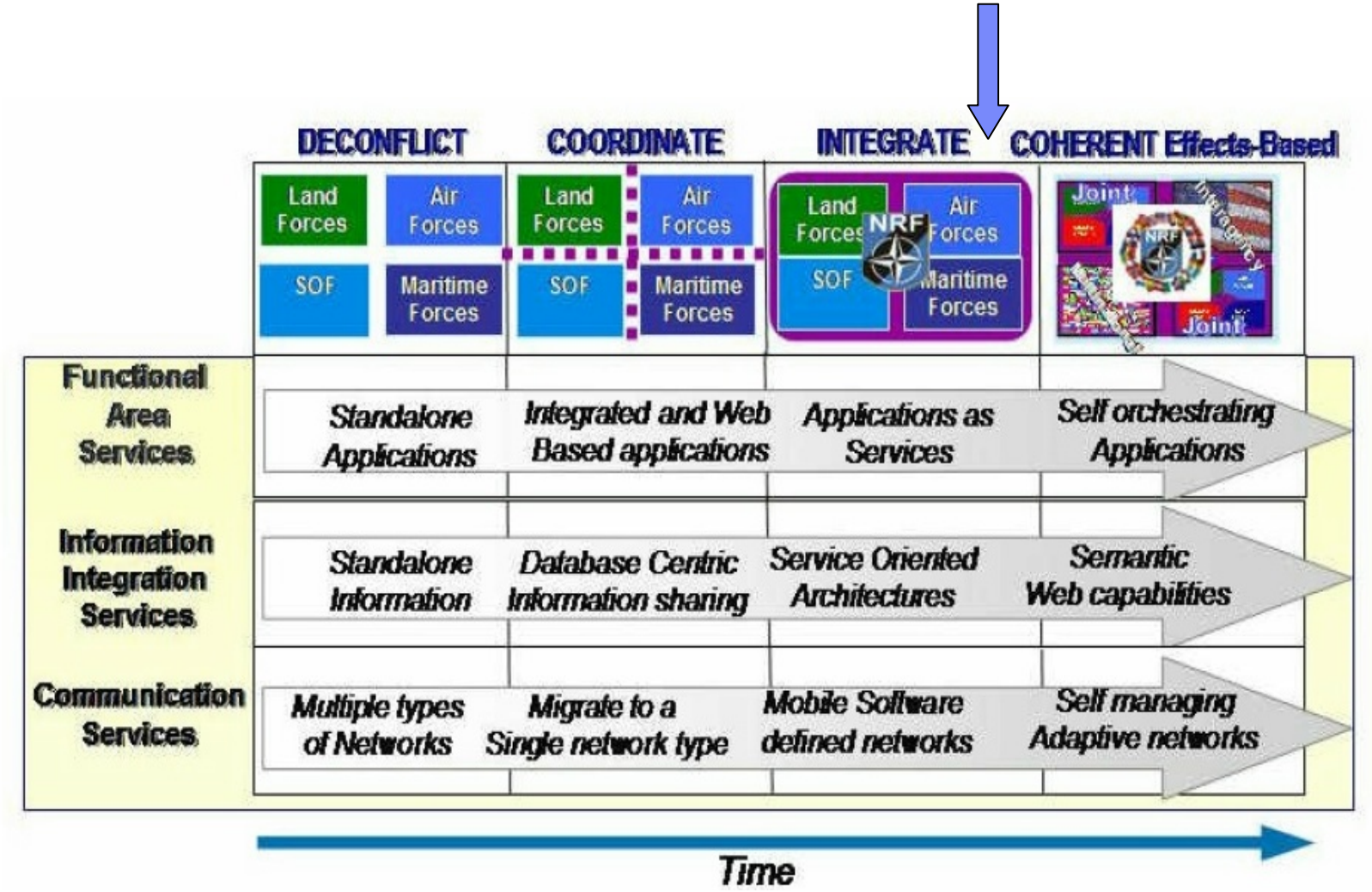
Core Enterprise Services in the Global Information Grid



Secure Enterprise Service Bus: Intelligent Sensor Grid

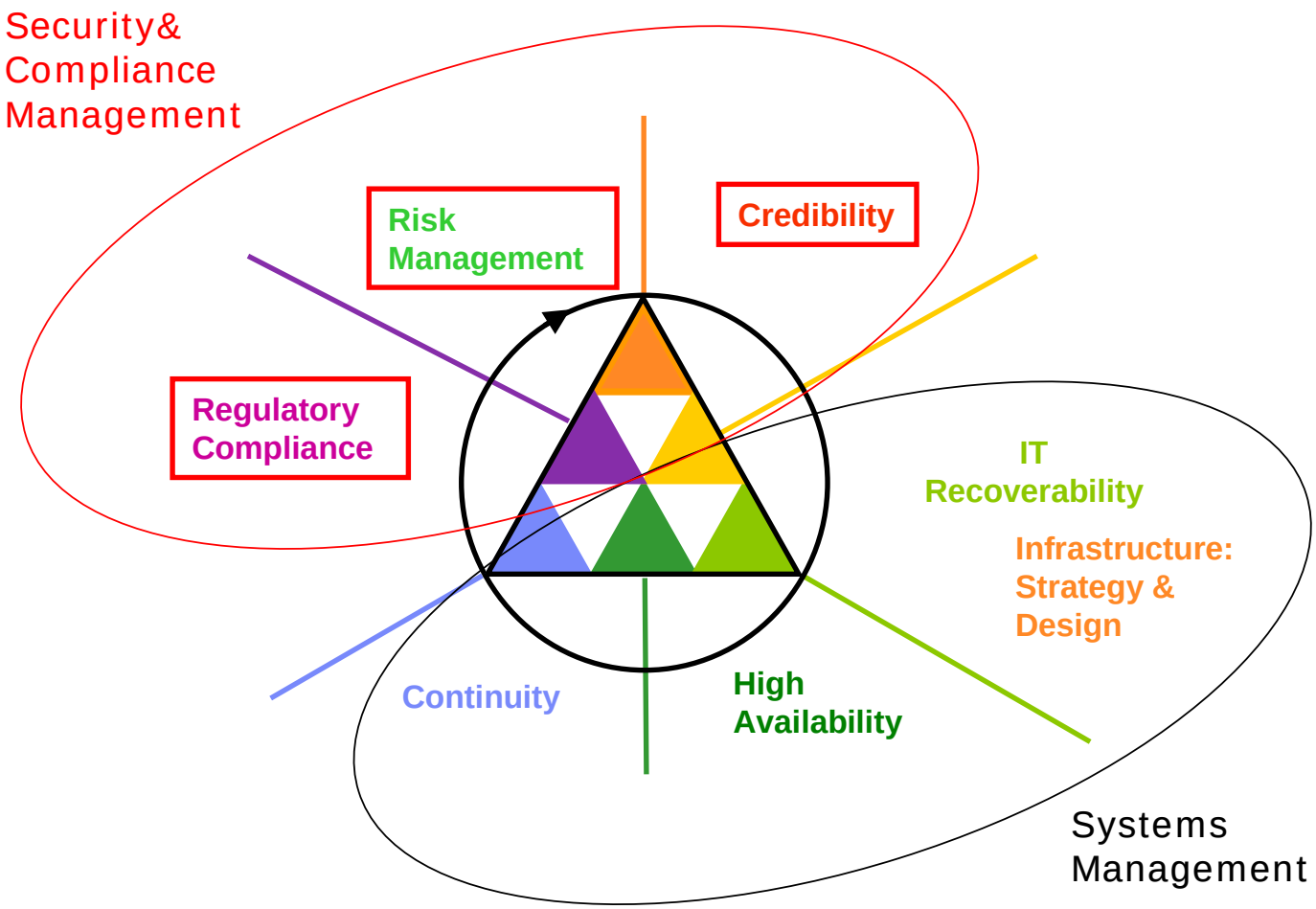


ESB Value Proposition in NCO

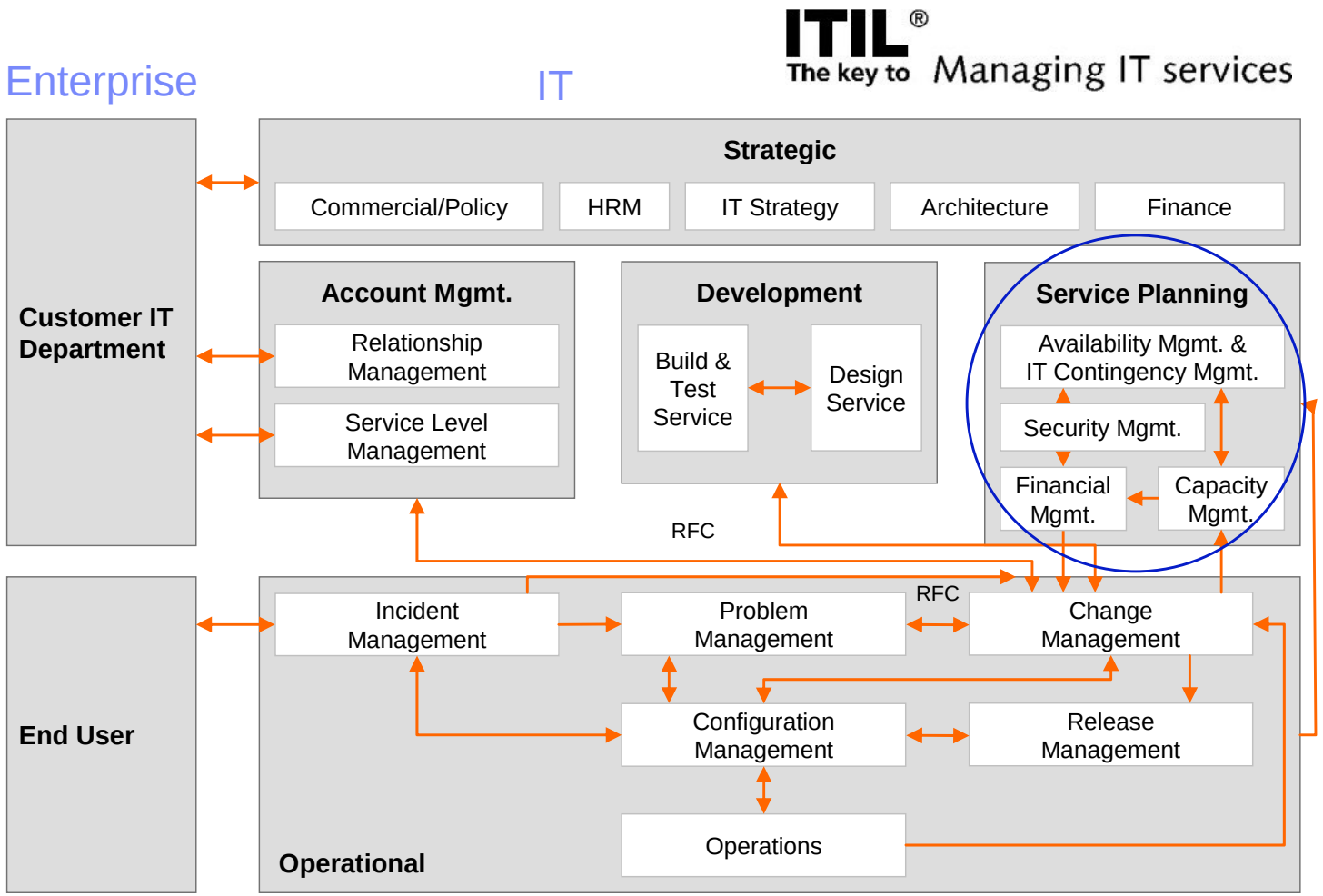


Source: NATO Network Enabled Capabilities Feasibility Study, 2005

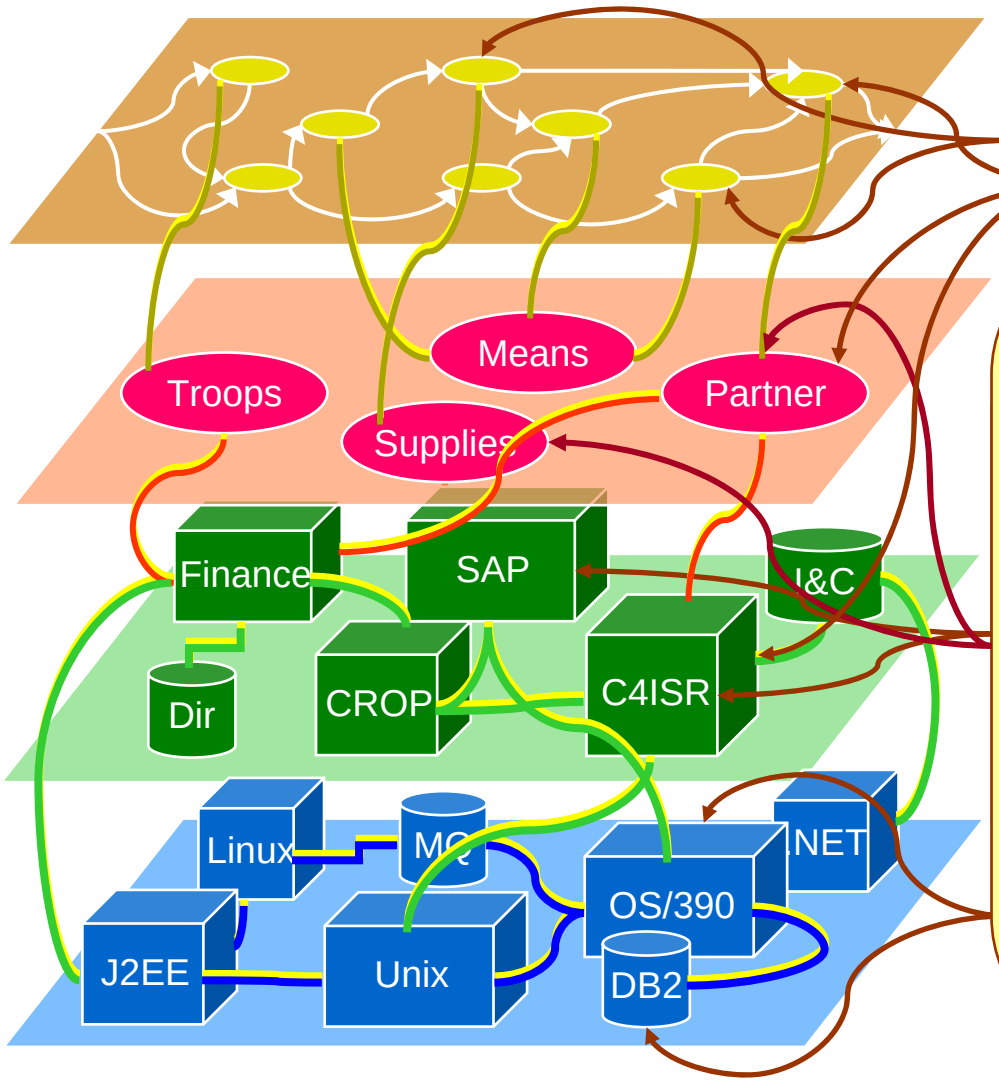
Facets of Security



Networked Era: Running IT as a Business (SOA)



Managing Different Layers in the SOA Stack



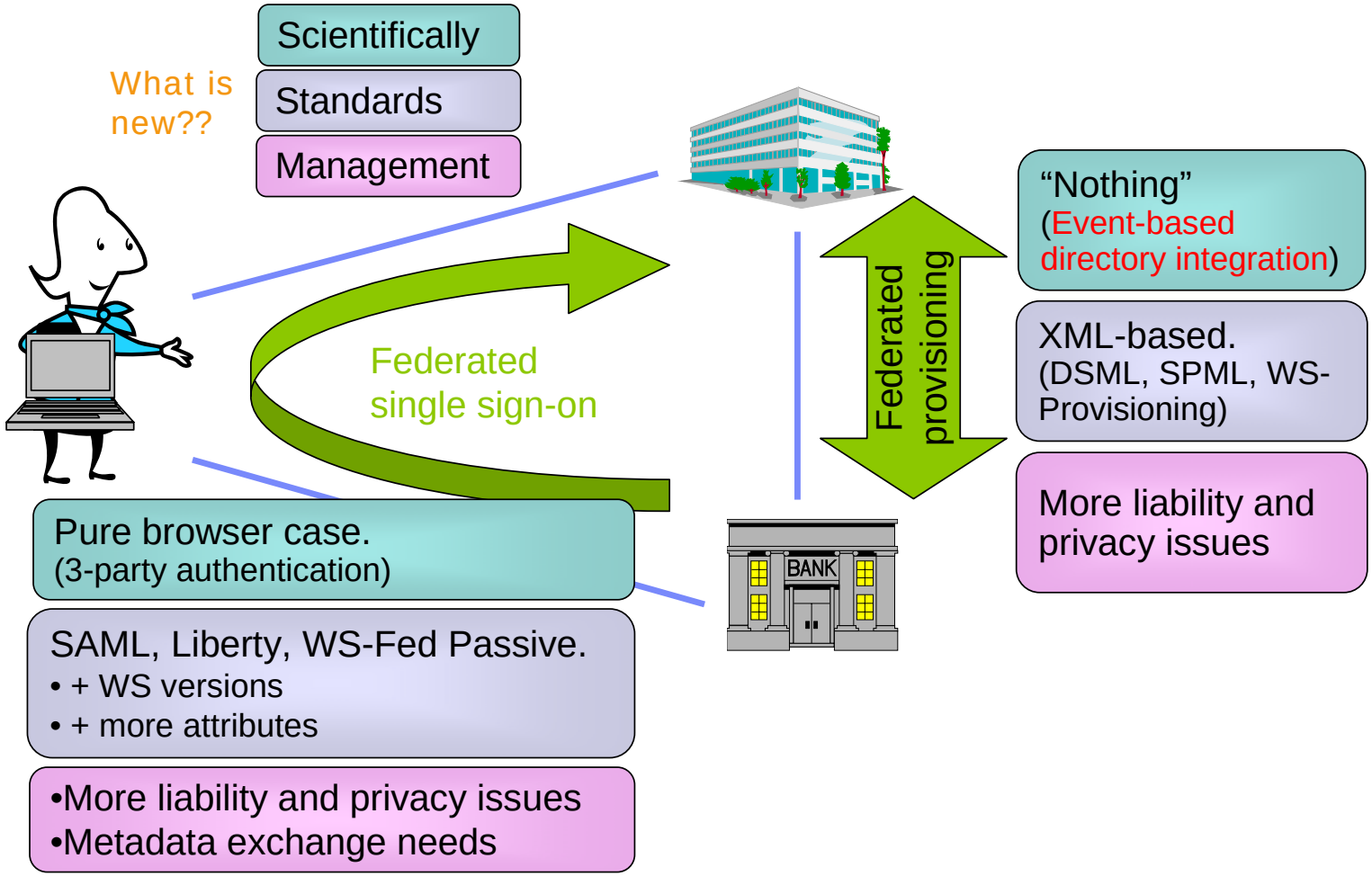
Manage: Service Security

- Consistent authorization across the infrastructure components
- Map identities between various security sub-systems
- Compliance to security policy

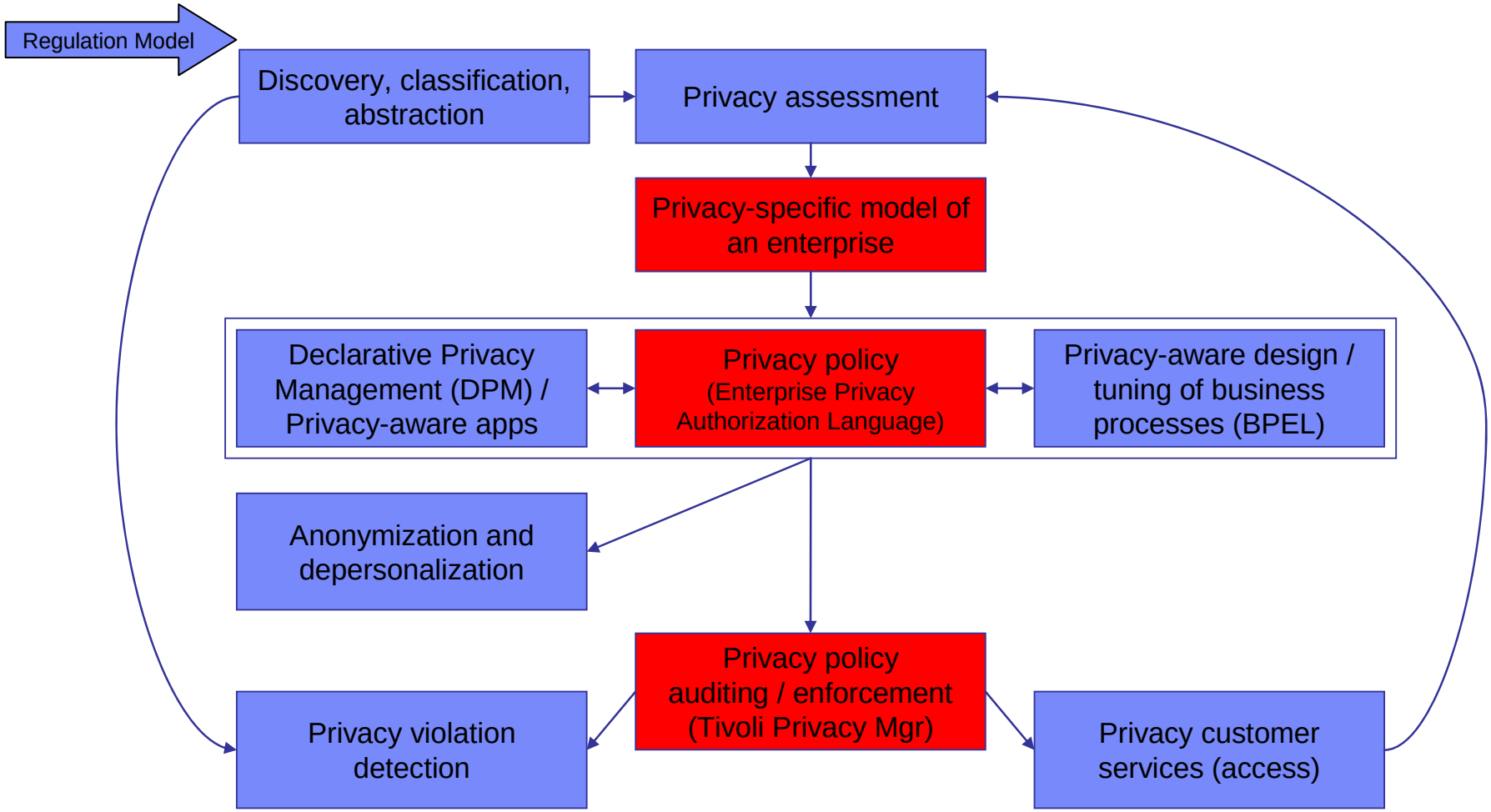
- payload (SOAP/XML), origin, destination, service characteristics
- Problems detected: SLA violations, invalid services, dependency or relationship mismatch
- Control the message flow in the service environment through management mediations like log, filter, and route
- Centralize services management policy
- Set business-related IT goals

network failures

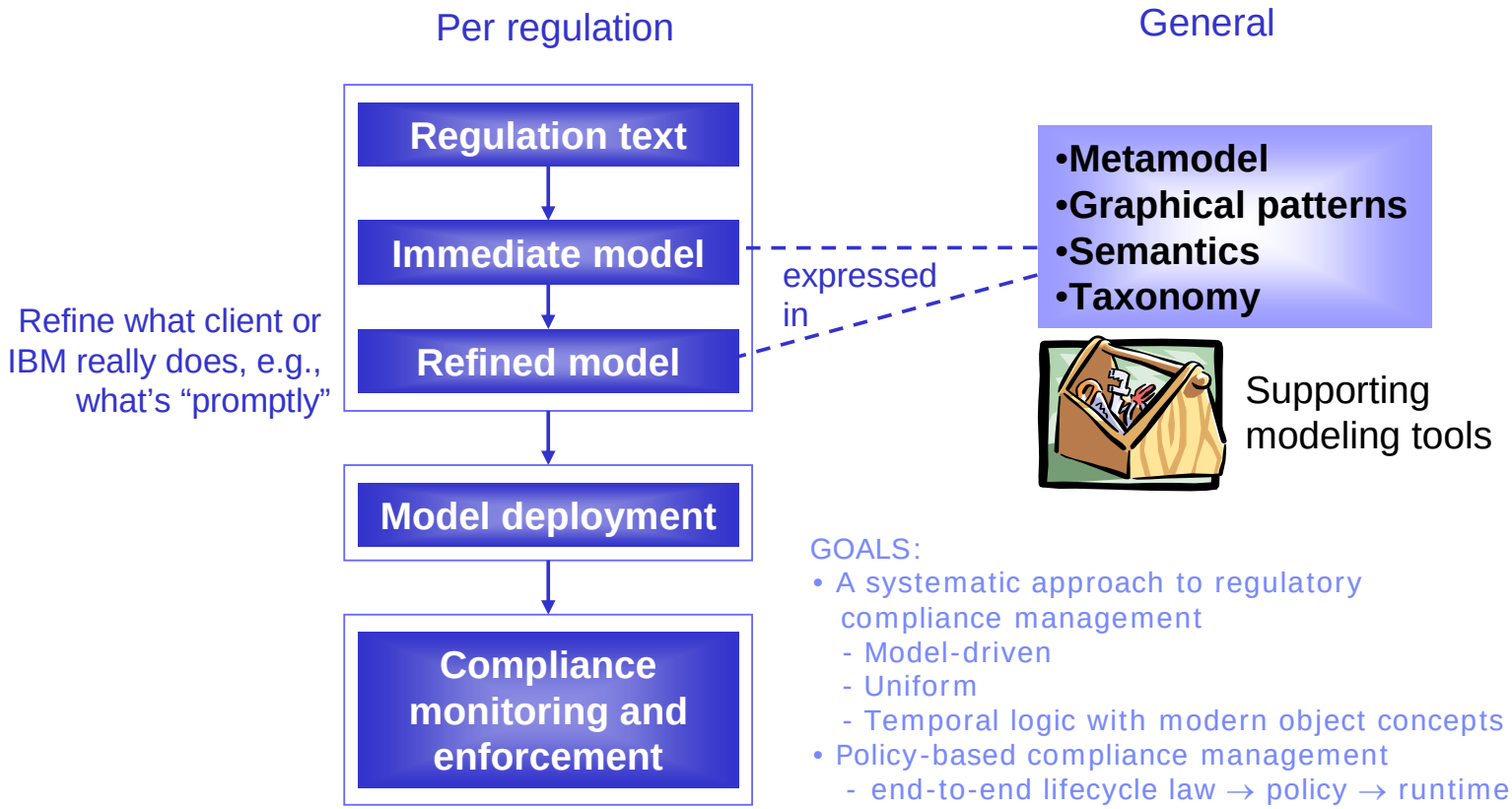
Identity Federation & Regulatory Issues



IBM Enterprise Privacy Architecture



Regulatory Modelling Process …

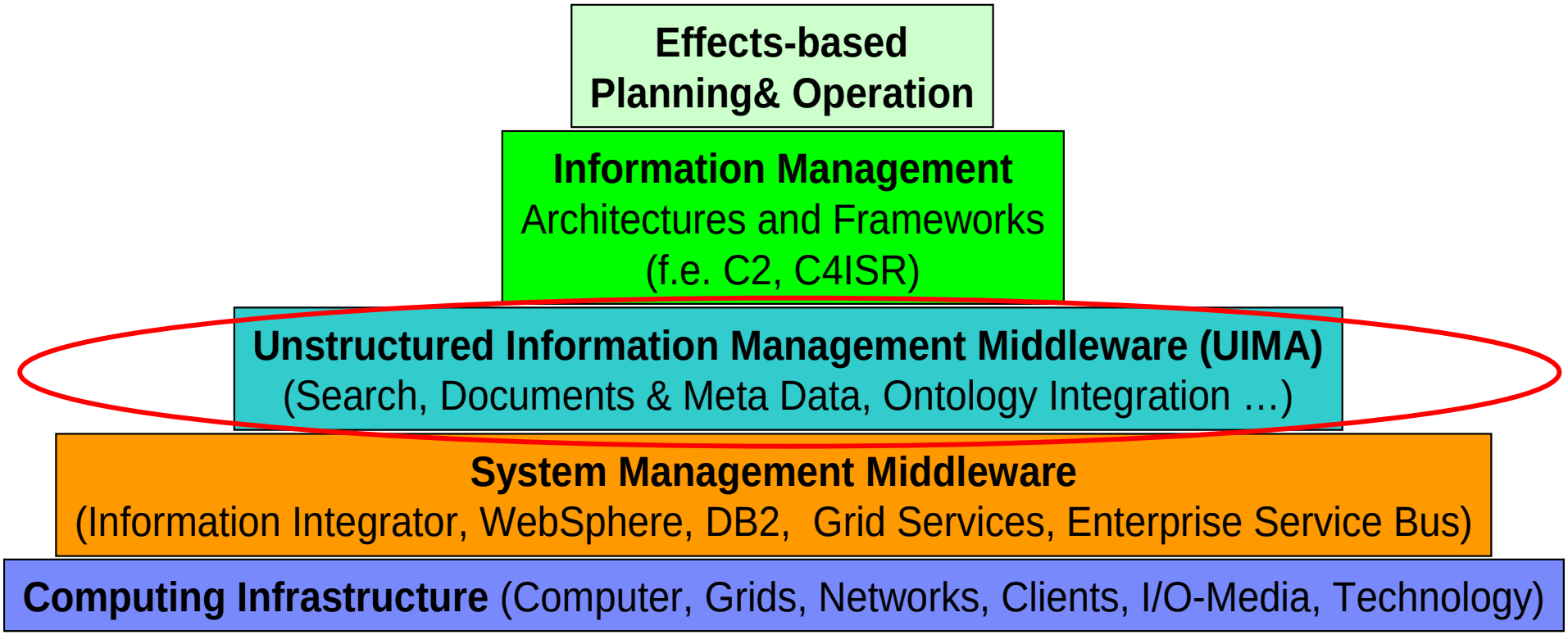


GOALS:
- A systematic approach to regulatory compliance management
  - Model-driven
  - Uniform
  - Temporal logic with modern object concepts
- Policy-based compliance management
  - end-to-end lifecycle law → policy → runtime integration with existing modeling standards (UML2.0, CBM, BOM, IFW)
  - Automated policy deployment
  - Continuous monitoring and enforcement

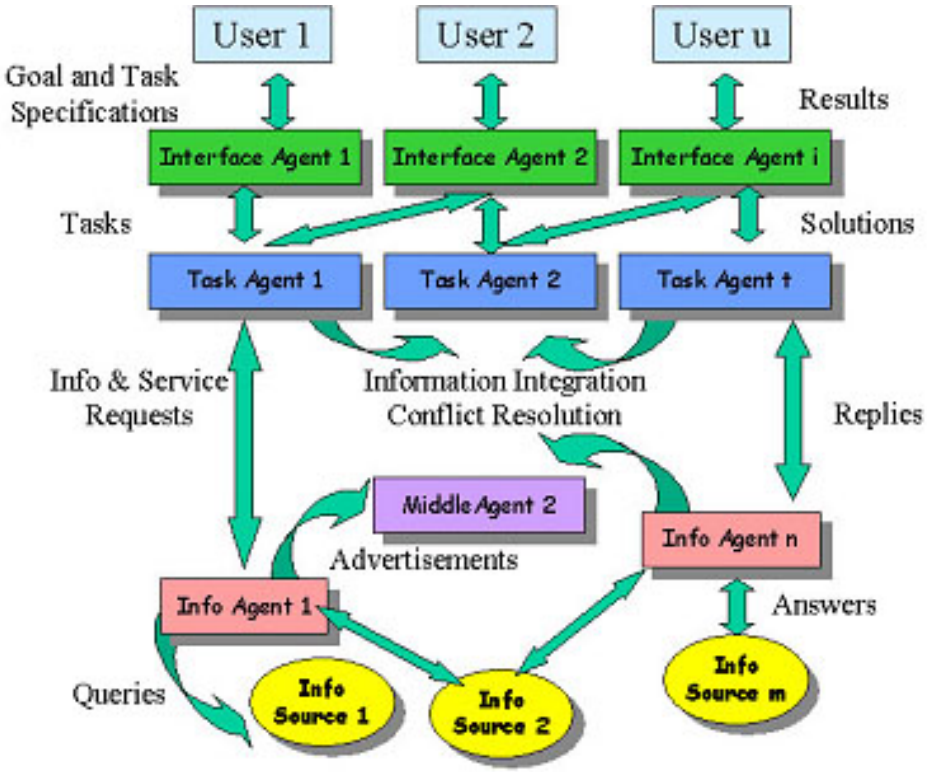
- Recall disclaimer: This is not legal advice by IBM. It is only a technique for tracing requirements and bringing them closer to business process models and IT.

… empowers Policy-Based PKI

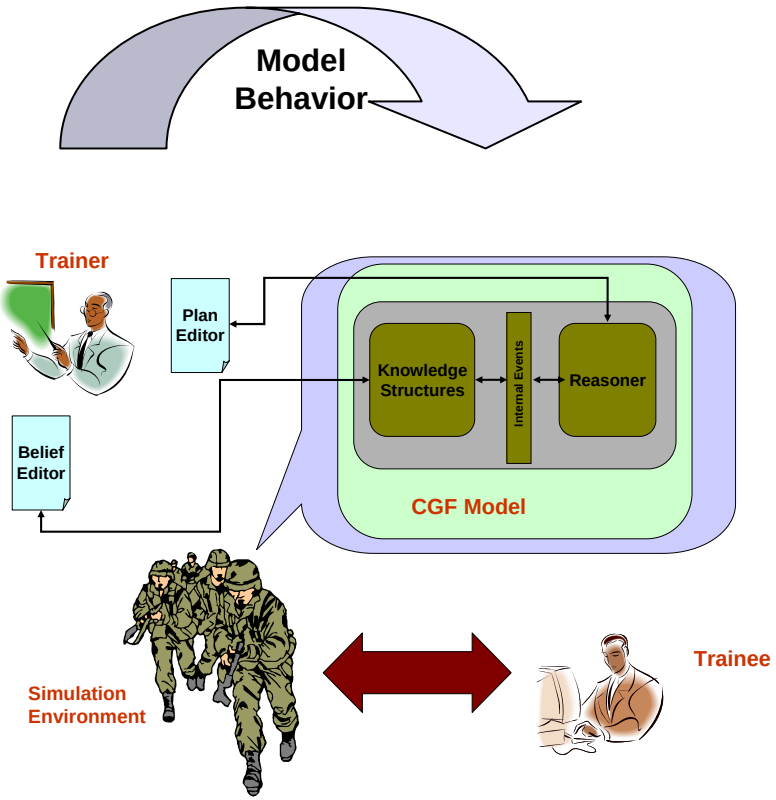
Close up with Semantics: Knowledge Management Framework for EBO



Mobile Software Agents in Simulation & Decision Support

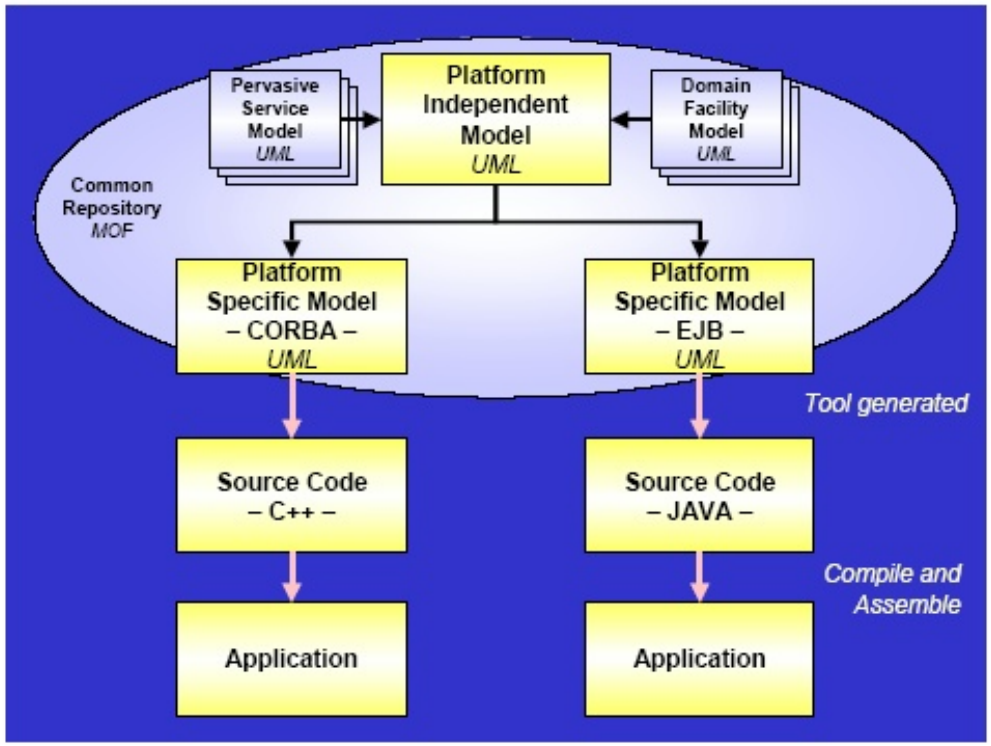


Multi-Agents-System Architecture



CGF = Computer Generated Forces

Model-Driven Architecture & NCO



LCIM	DEVS/HLA	MDA
Level 5 Conceptual Interoperability	*Domain specific Business models, such as DoDAF*	*Domain overarching Repository of PIM*
Level 4 Dynamic/Pragmatic Interoperability	DEVS	PIM
Level 3 Semantic Interoperability	DEVS Reference FOM	PIM PIM-PSM-Mapping
Level 2 Syntactic Interoperability	HLA	PIM-PSM-Mapping PSM
Level 1 Technical Interoperability	*Net standards Web connectivity TCP/IP etc.*	*Repository of PSM describing net/web solutions*

Summary

- Effects-Based Planning and Operation (EBO) shall be enabled through the semantic opening of the information domain.
- An Intelligent Sensor Grid (ISG) lays the foundation via semantic integration and reduction of complexity by virtualizing physical network characteristics.
- Risk management, securing of the network and EBO build on advanced techniques regarding modelling, simulation and analysis. On the resource and component level, technologies and products are plentiful and available today.
- IT-Security and Compliance Management (doctrin enforcement) are mandatory enablers for NCO.
- Model-Driven Development and Architecture (MDA) paves the way to flexible operation planning and execution support.

???