

## Policy Management in a COA

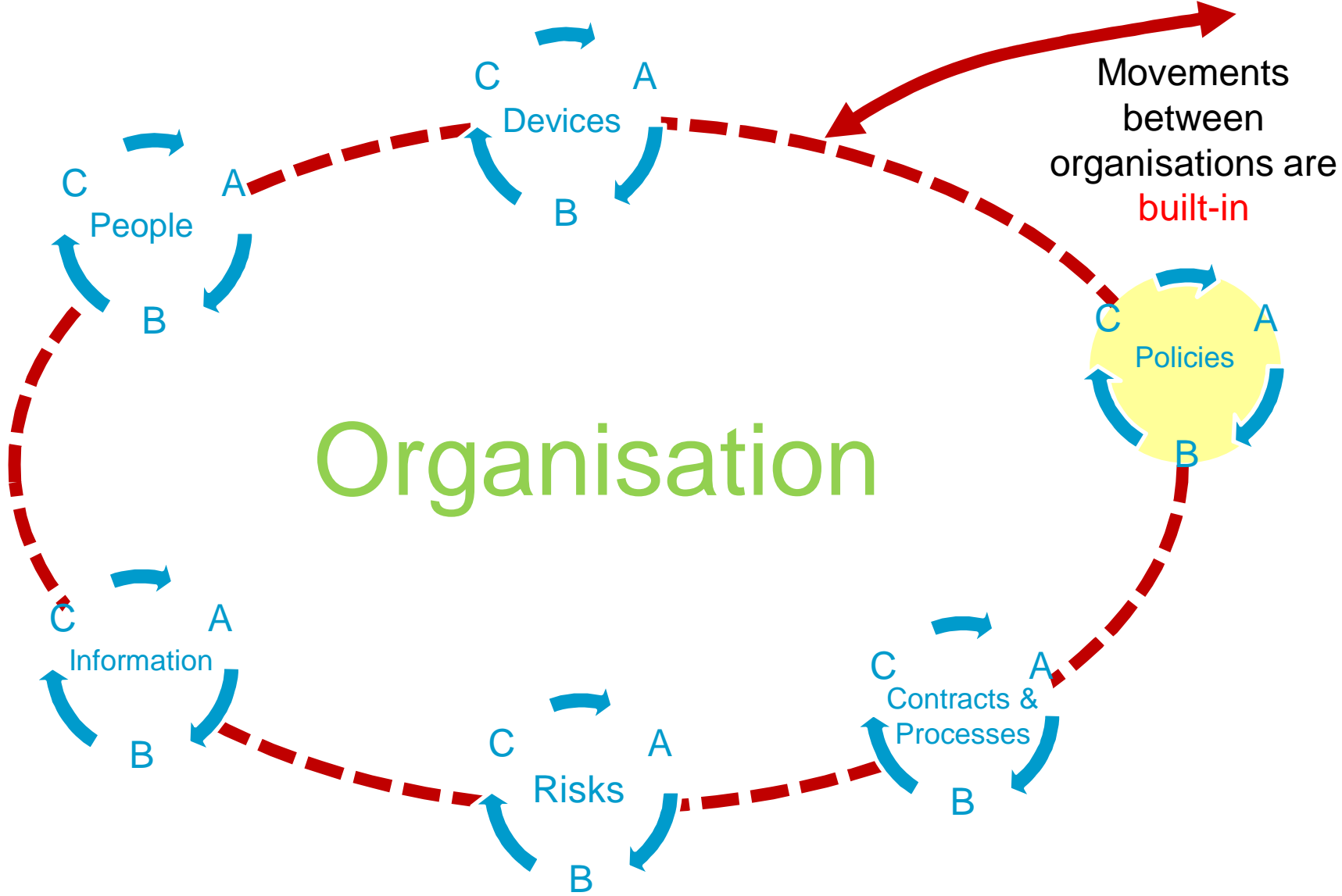
John Arnold

Chief Security Architect, UK

Capgemini



# De-Perimeterised Organisations



## Security Policy - Terminology

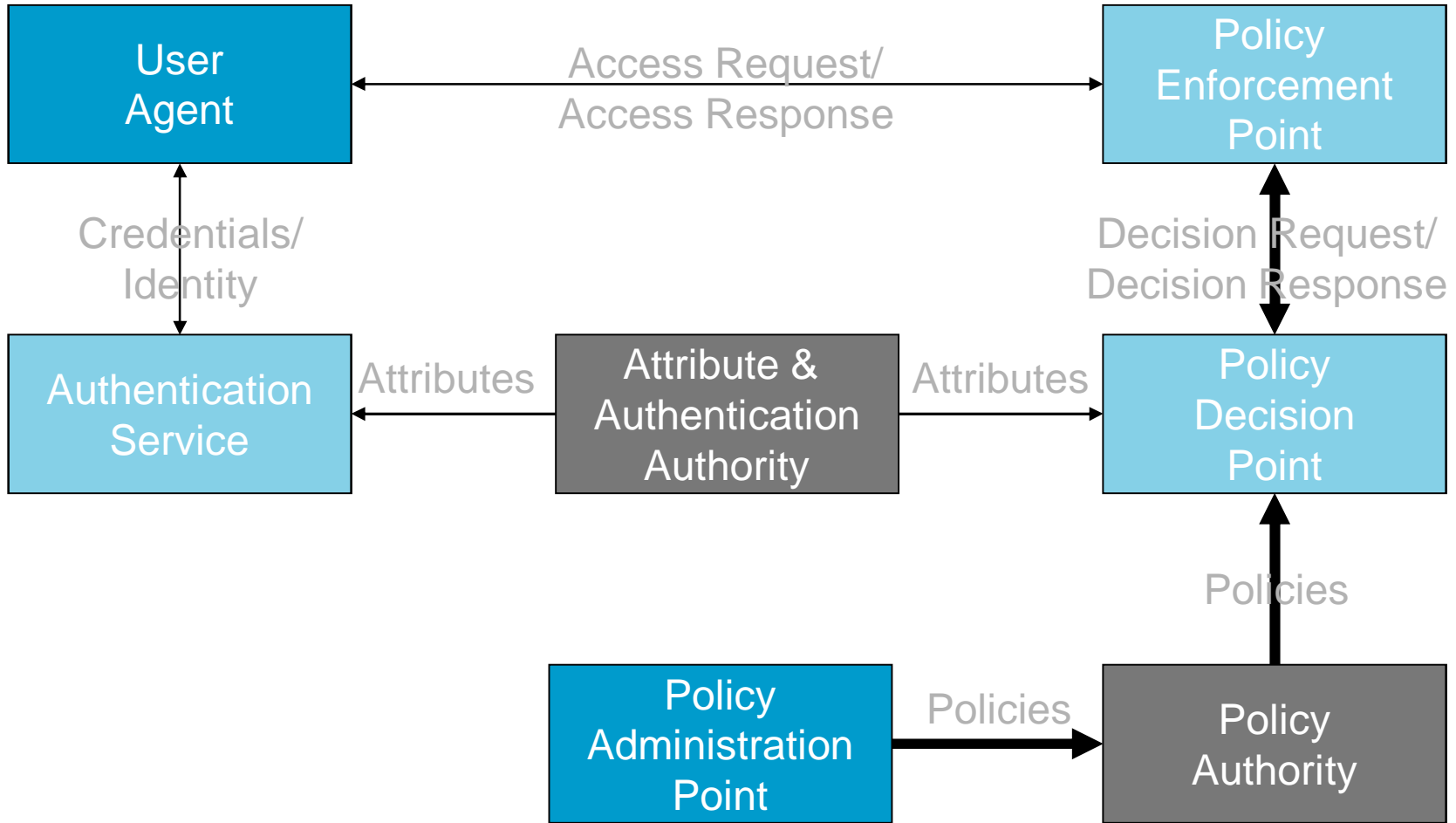
---

- “ A **Human Readable Security Policy** is a security policy that is intended to be interpreted by humans in making security decisions. E.g. a security procedure
- “ A **Machine Readable Security Policy** is a security policy that is intended to be interpreted by computer programs in making security decisions. E.g. an ACL
- “ A **Governance Policy** is a policy that describes how a human or machine readable policy is determined or agreed. E.g. Most ISO27001 security policies.

# Current security policy approaches and the problems with them

Machine readable policies tend to be lists rather than rules	Difficult to change as business needs change.
Machine readable policies are designed to be enforced by infrastructure rather than applications	One size fits all approach; cannot relate policies to business benefit
Machine readable policies not linked to business requirements	Policies do not implement requirements properly and it is not clear how to change them
Application security policies are embedded into application code	May not meet business requirements. Difficult to change as business needs change
Organisations assume their policies are their own	Untrue . where organisations handle information on behalf of someone else, the original information owner is a stakeholder in the policy
Use of ACLs per resource	Enormous number of ACLs to manage

# Handling policies better – a new policy enforcement architecture



## Handling policies better – rich policy language

---

- Replace ACLs by a machine readable policy expressed in a rich policy language
- A rich policy language expresses access decisions in terms of the relevant contract states, e.g. ~~th~~is asset can be accessed by a direct employee of grade 4 and above, or any employee of a joint venture of a particular type~~q~~
- There is a standard for expressing security policies: XACML
- A benefit of using standard security policies . a policy for an asset can be specified once, then actioned by many different organisations as they pass the asset around

## Handling policies better – more realistic governance patterns

---

- Security policy governance is the process whereby security policies are specified, tested and agreed.
- Some common patterns:
  - . Creator control
  - . Subject Control
  - . N-man rule
  - . Content based control
  - . Accountability
  - . Corporate record
- Many information assets have more than one stakeholder and hence more than one policy stakeholder.

## Handling security policies better - security policy as a service

---

- Most organisations aren't capable, or motivated, to develop their own security policies
- It would be better for suitably qualified organisations to specialise in creating standard security policy services to cover areas such as
  - Compliance
  - Hardening
  - Product-specific policies
- This requires standardisation of the policy decision and query language (e.g. XACML) but also of the enforcement hooks to be put into applications.