# Identity the New Perimeter

Adrian Seccombe

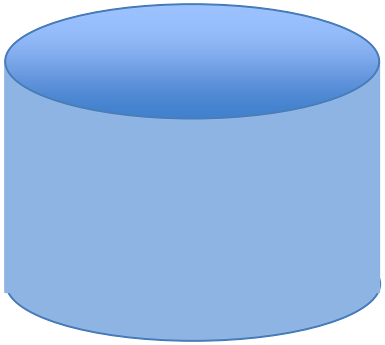
Surrey University

25th March 2010

# Key questions this session will answer

- Which are the key attributes of Cloud Types
- What are some of the key cloud choice drivers?
- Identify primary transformational **SHIFTS** required to enable a secure but collaborative clouds?
- Why does Identity and Access Management have to **SHIFT?**

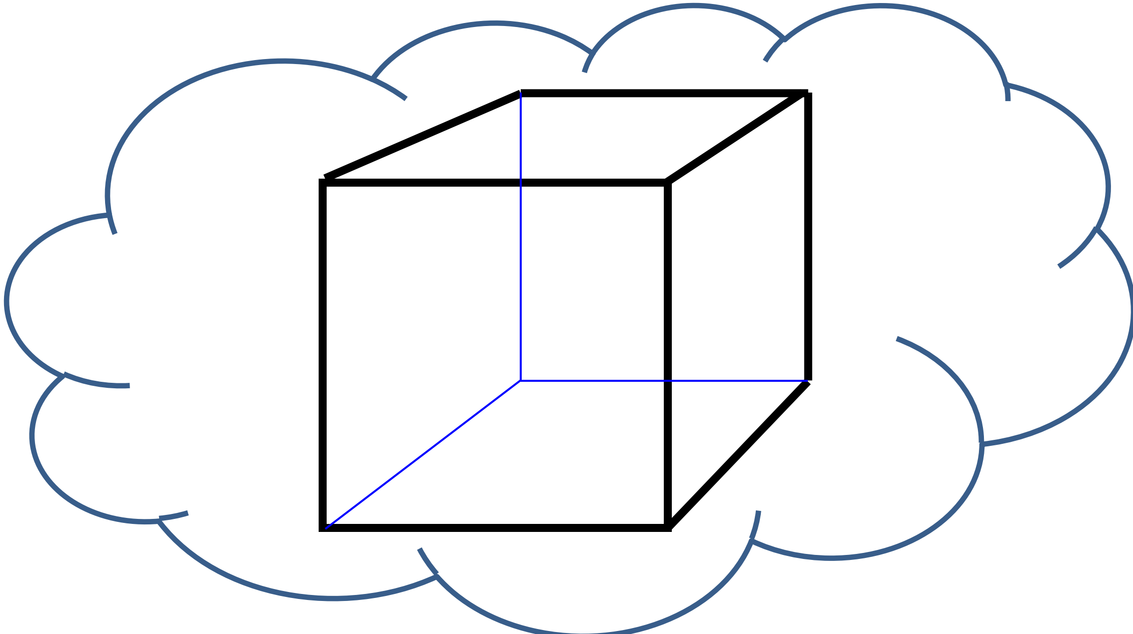
# To Cloud or Not to Cloud?



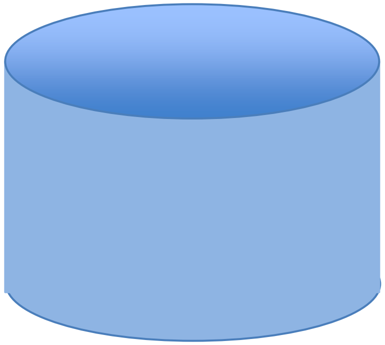
Traditional

“or”

Cloud



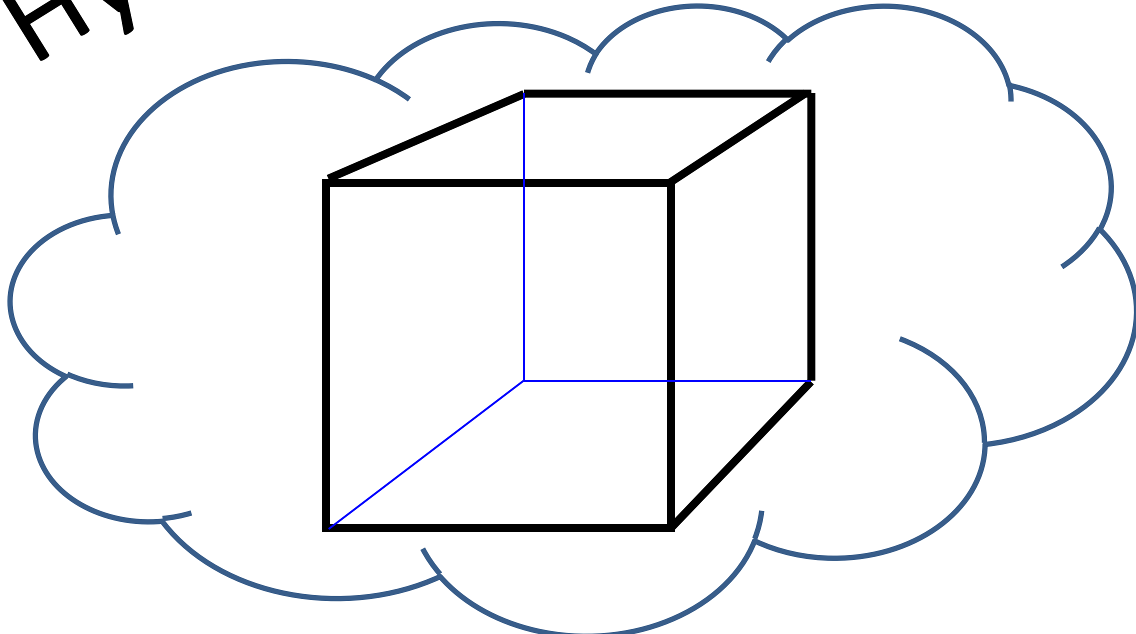
# Let’s get real!



Traditional

We are **all** “Hybrid” already!

Cloud



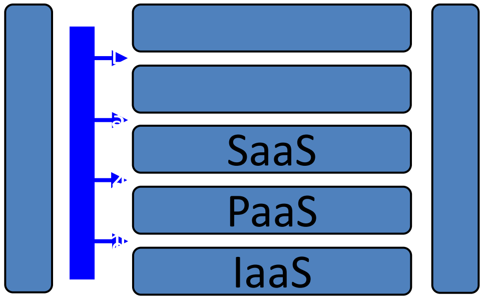
# Unfortunately…

- Our Business Partners are pressing ahead into the clouds, often unaware that they are!
- We are NOT architecting our way into the Clouds
- Seems like we've been here before…
  … remember the early PCs?
- This is where the Jericho Forum Self Assessment Scheme will be able to help you…

# Some Definitions

- **NIST** and the **Jericho Forum** have it wrapped!

**"NNN as a Service"**



**Essential Characteristics:**

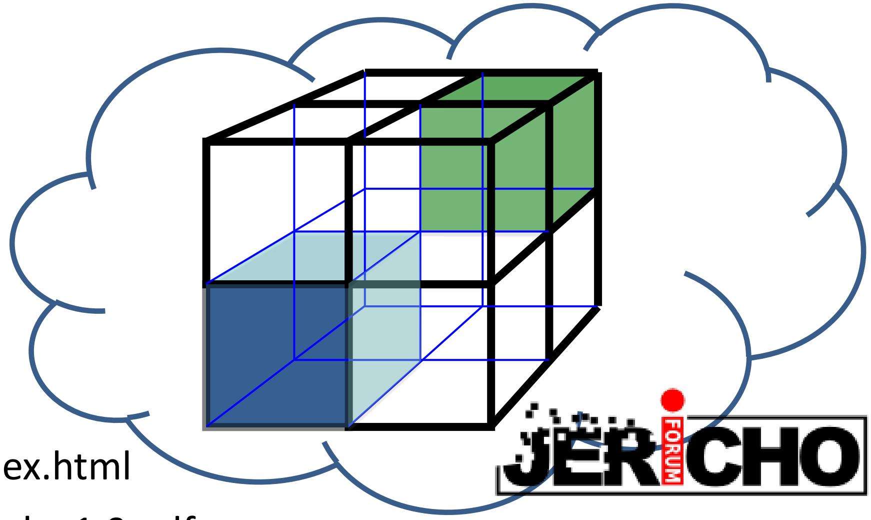
- *On-demand self-service.*
- *Broad network access.*
- *Resource pooling.*
- *Rapid elasticity.*
- *Measured Service.*

**"Deployment Models"**

Public Private

Community Hybrid

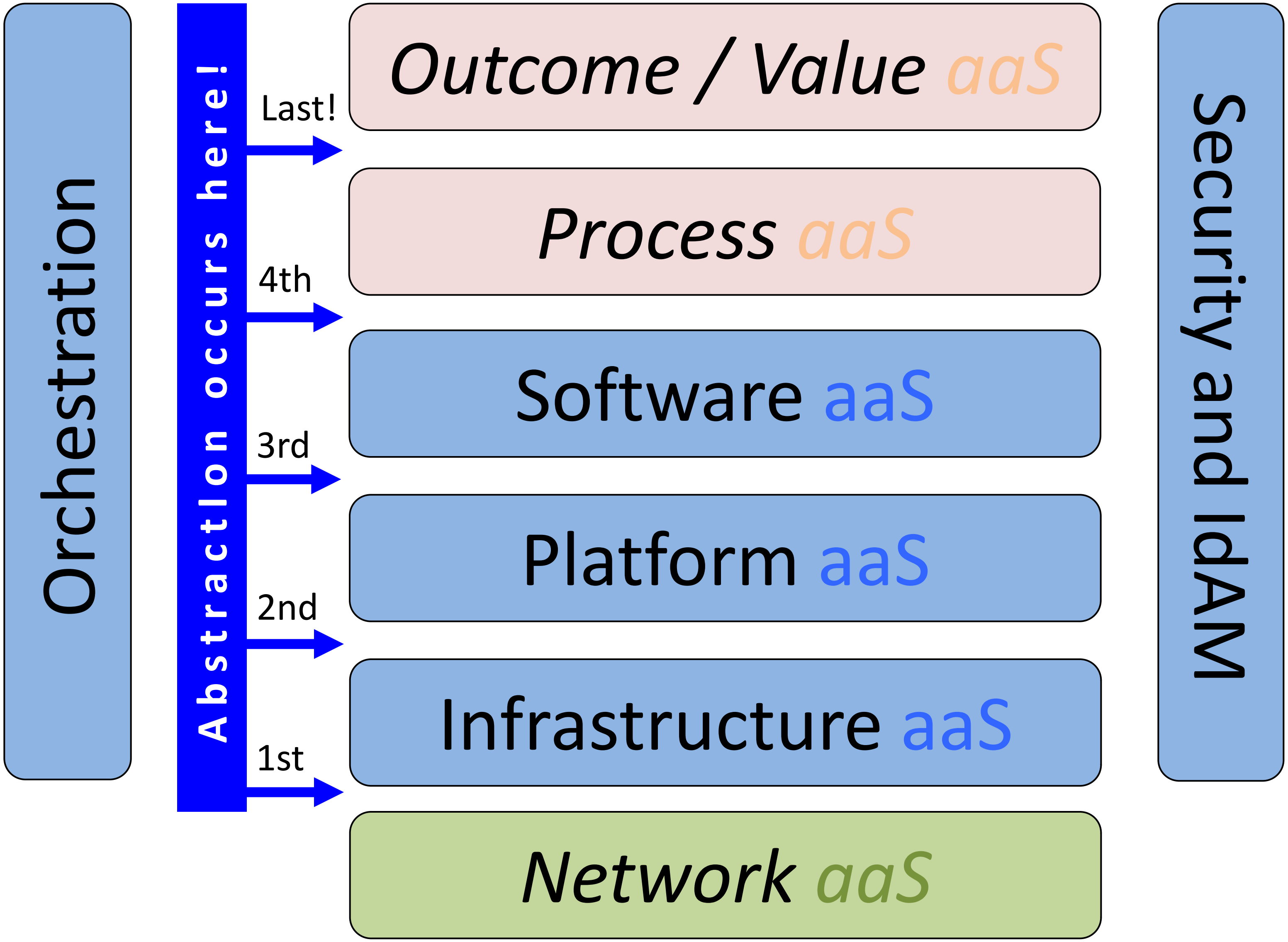
**"Cloud Cube"**



http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

# “NNNNN as a Service”



Orchestration

Abstraction occurs here!

Last!

4th

3rd

2nd

1st

*Outcome / Value aaS*

*Process aaS*

Software aaS

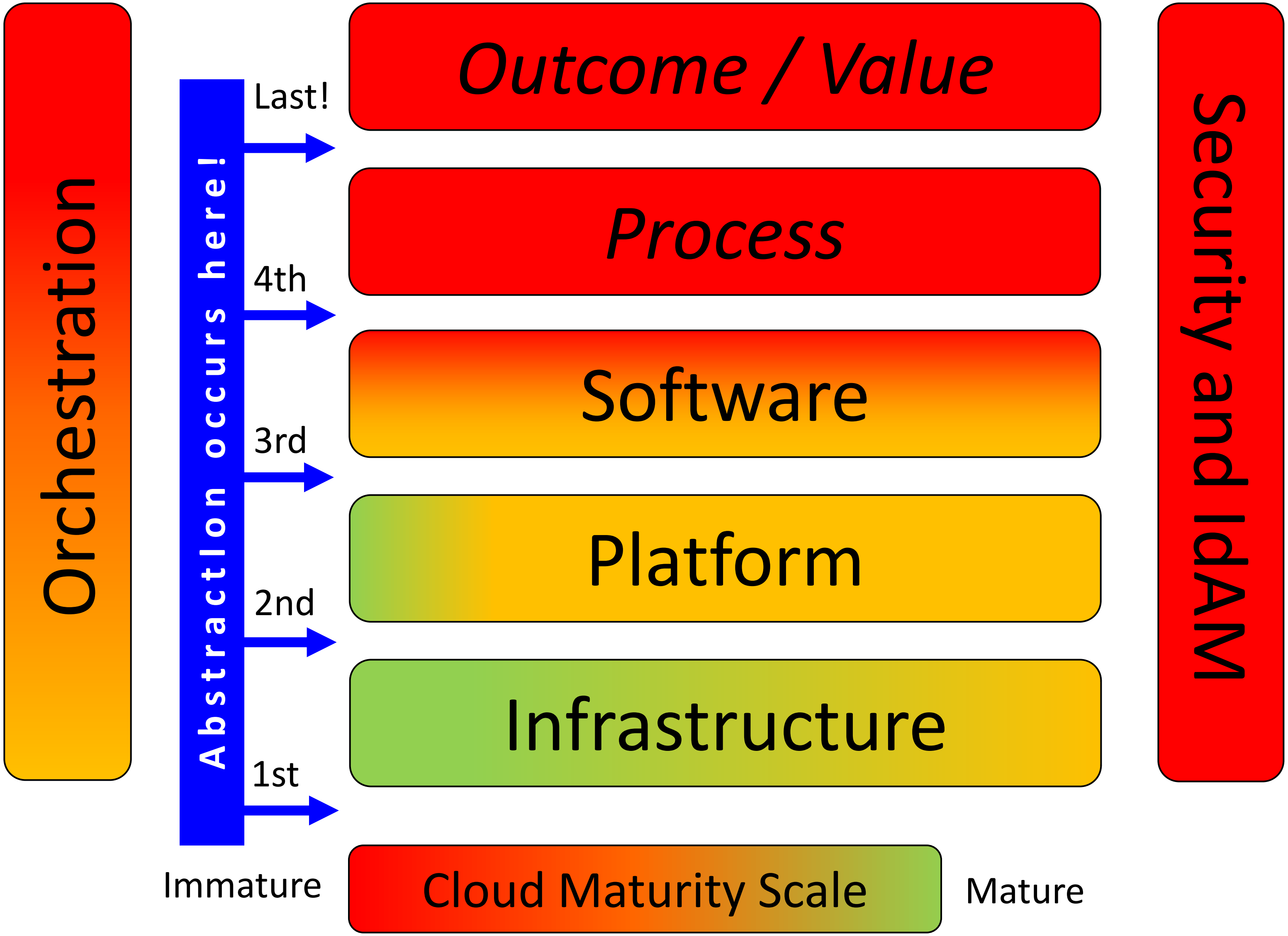
Platform aaS

Infrastructure aaS

*Network aaS*

Security and IdAM

# Maturity of the Cloud Layers



Orchestration

Abstractlon occurs here!

Last!

4th

3rd

2nd

1st

*Outcome / Value*

*Process*

Software

Platform

Infrastructure

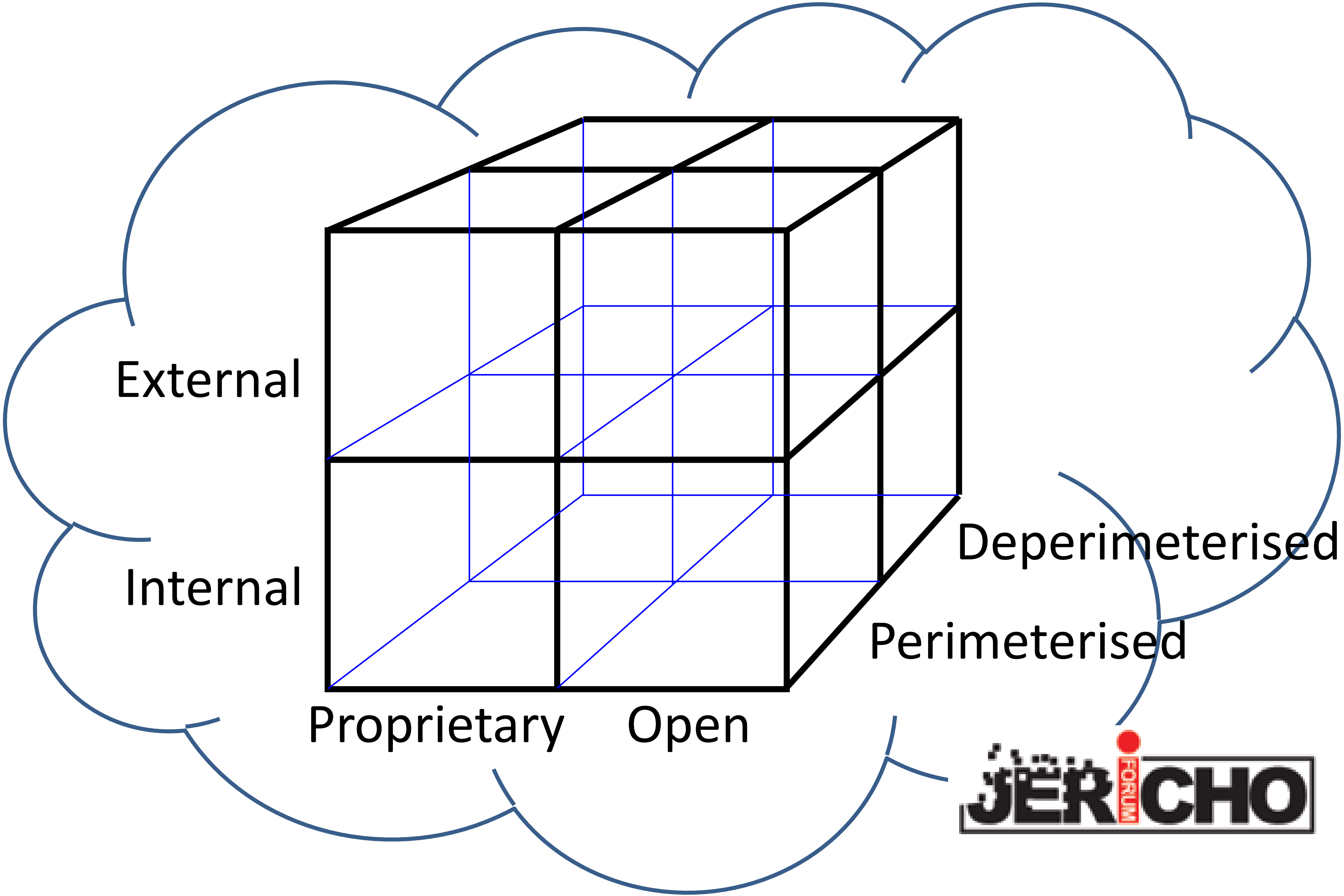
Security and IdAM

Immature

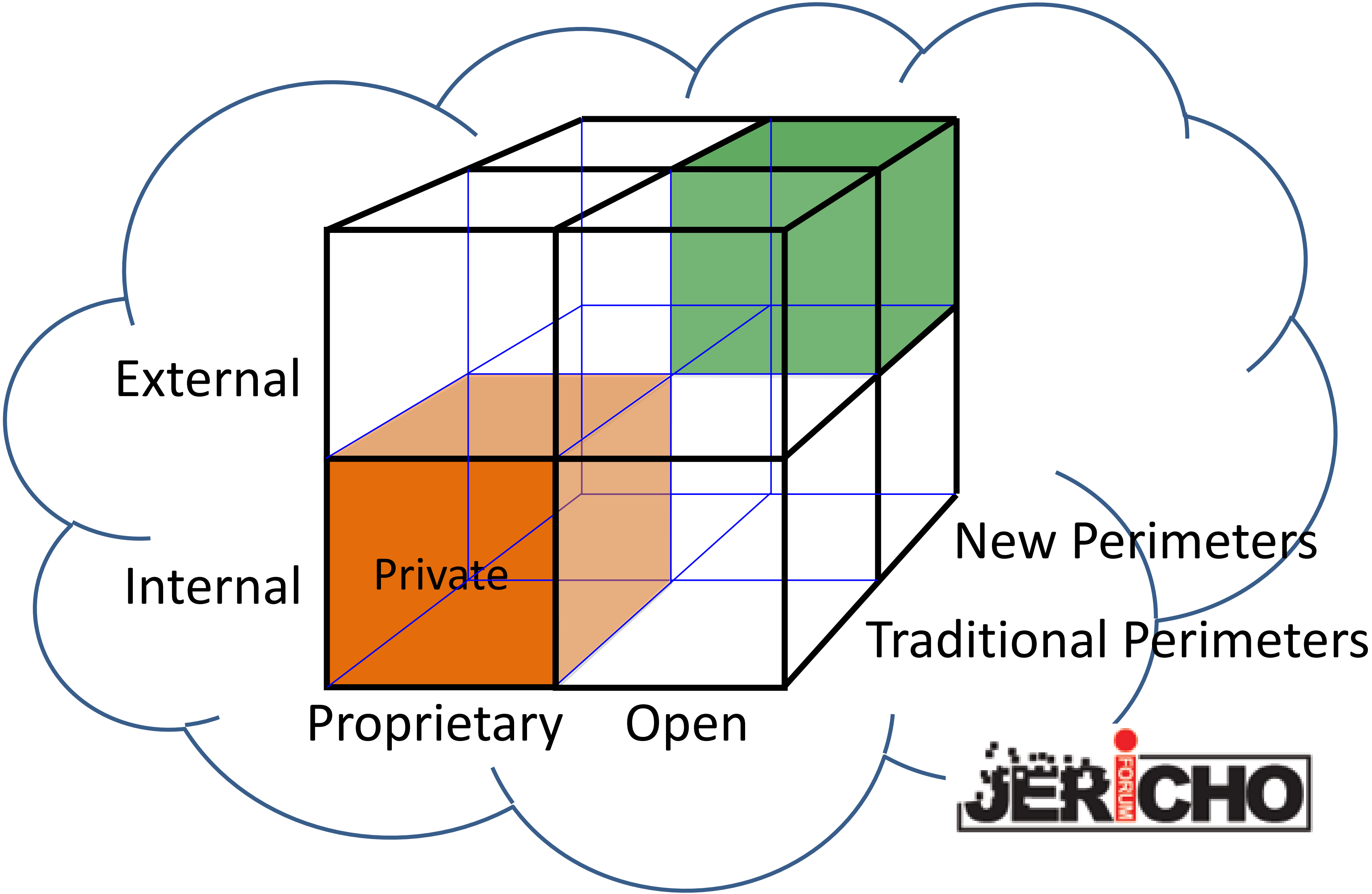
Cloud Maturity Scale

Mature

# The Cloud Cube revisited



# The Cloud Cube revisited



JERICHO FORUM

# Choose the Clouds with care!

- Private Clouds are Silos (Sometimes you need Silos)
- Proprietary Clouds Can Lock You In
- Internal Clouds are a Stop Gap
- Clouds with the Old Perimeters do not enable external collaboration

# The key shifts

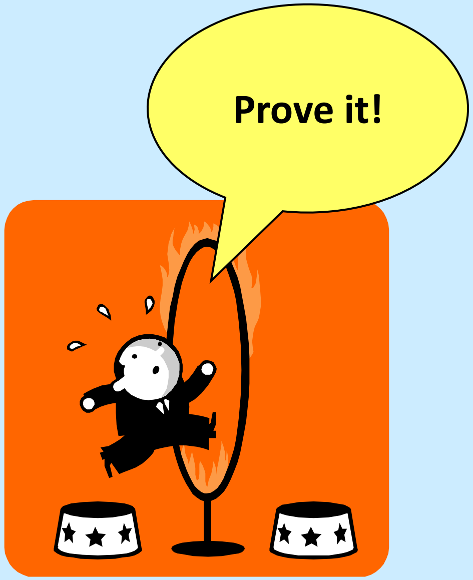
The Identity Shifts

Identity the new Perimeter

# Privilege Management in Ten Words

## Identification

## Authentication



## Authorization

- Identification: The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals

- Authentication: The exchange of information in order to verify the claimed identity of a principal

- **Authorization: The granting of rights, including access, to a principal, by the proper authority**

**Principal: An entity (people, devices, applications, etc.) whose identity can be authenticated**

**Reference: Open Group XDSF (X/Open Distributed Security Framework), ISO 10181-3**

# Did you spot the gap?

Inside the Old Perimeter

- Identify: Who are you?
- Authenticate: You are you

Magic Occurs here!

- Authorise: Have this!

Outside the Old Perimeter

- Principal declares Identity
- Identity Authenticated

Entitlement

- Resource Requested
- Resource Identified
- Resource declares Rules
- Rules verified
- User claims capabilities / attributes
- Claims verified
- Access Control Decision

Identity Shift #1 Resource Centric

# “Identity” Lifecycle of a Resource

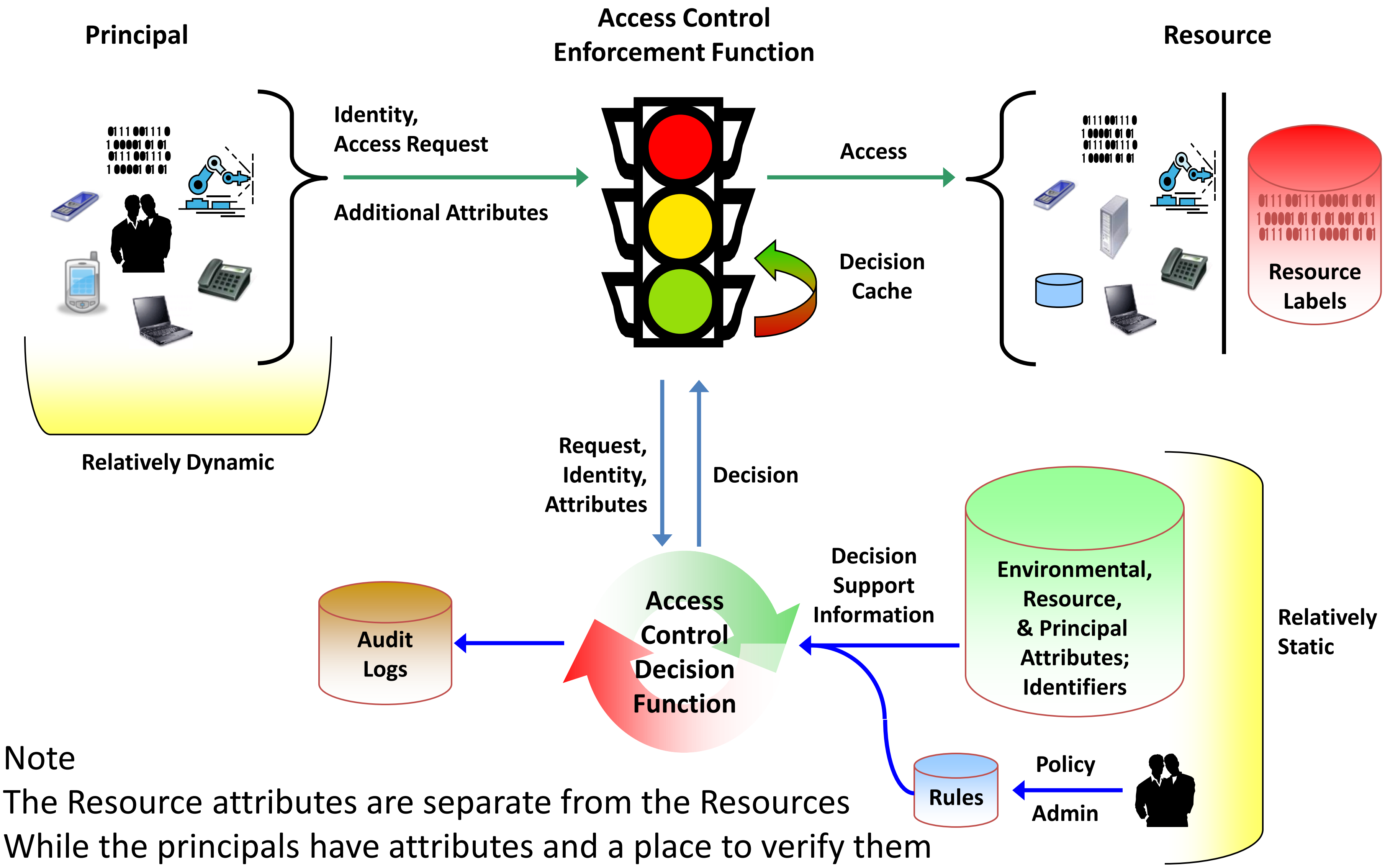
- Create Resource Identity
- Verify Resource Identity
- Set the Access Rules (eg Must be Over 18)
- Enable Rule Authentication
- Entitlement Check (Are you Over 18?)
- Verify Claim
- Evaluate
- Allow Access to Resource

Resource: Service, System, Code, Information

Diagram Courtesy
Steve Whitlock

Asymmetrical

# ISO Authorization Model



Principal

Access Control
Enforcement Function

Resource

Identity,
Access Request

Additional Attributes

Access

Decision
Cache

Resource
Labels

Relatively Dynamic

Request,
Identity,
Attributes

Decision

Decision
Support
Information

Environmental,
Resource,
& Principal
Attributes;
Identifiers

Relatively
Static

Audit
Logs

Access
Control
Decision
Function

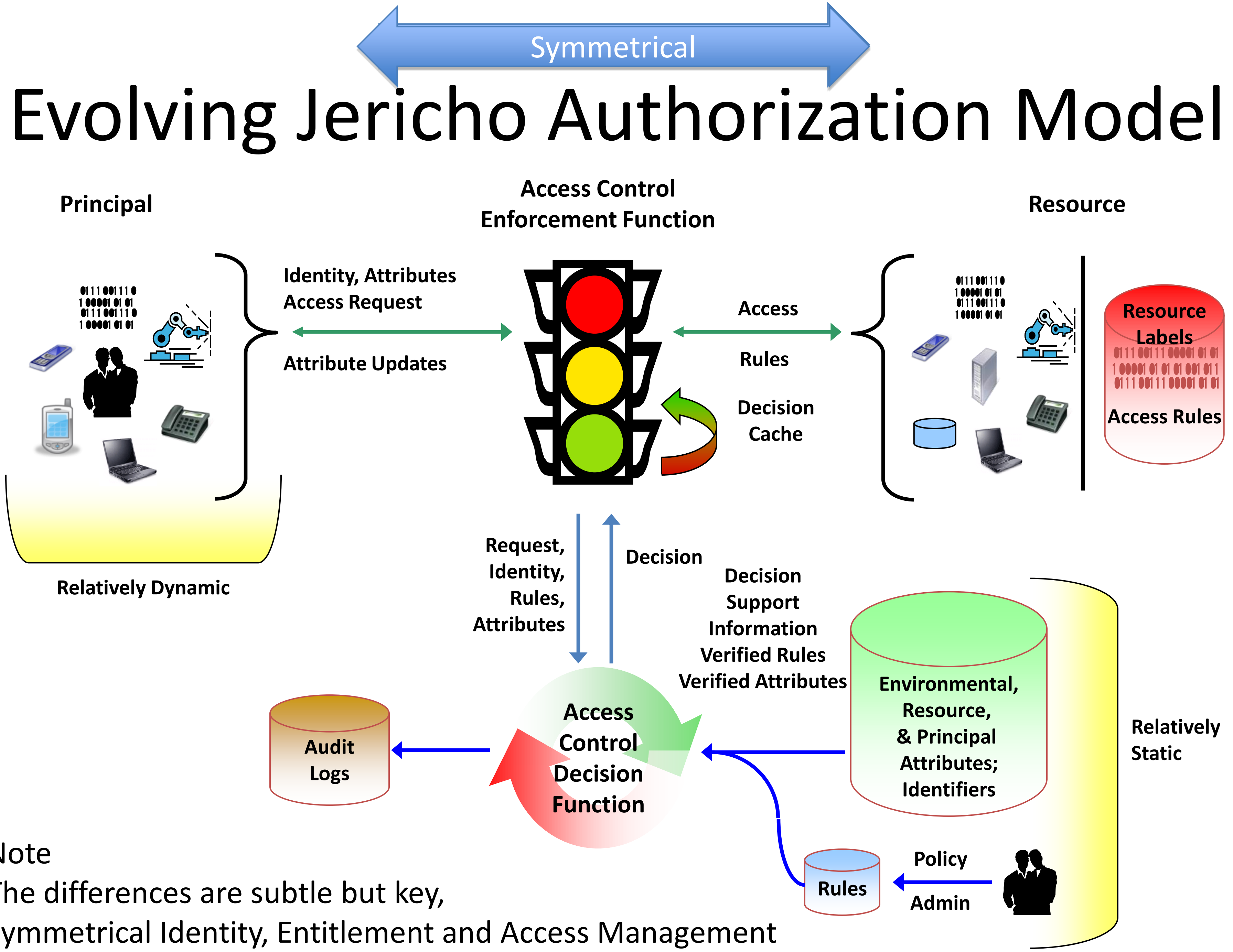
Rules

Policy

Admin

Note
The Resource attributes are separate from the Resources
While the principals have attributes and a place to verify them

# Evolving Jericho Authorization Model



Symmetrical

Principal

Access Control Enforcement Function

Resource

Identity, Attributes Access Request

Attribute Updates

Access

Rules

Decision Cache

Resource Labels

Access Rules

Relatively Dynamic

Request, Identity, Rules, Attributes

Decision

Decision Support Information Verified Rules Verified Attributes

Environmental, Resource, & Principal Attributes; Identifiers

Relatively Static

Audit Logs

Access Control Decision Function

Rules

Policy

Admin

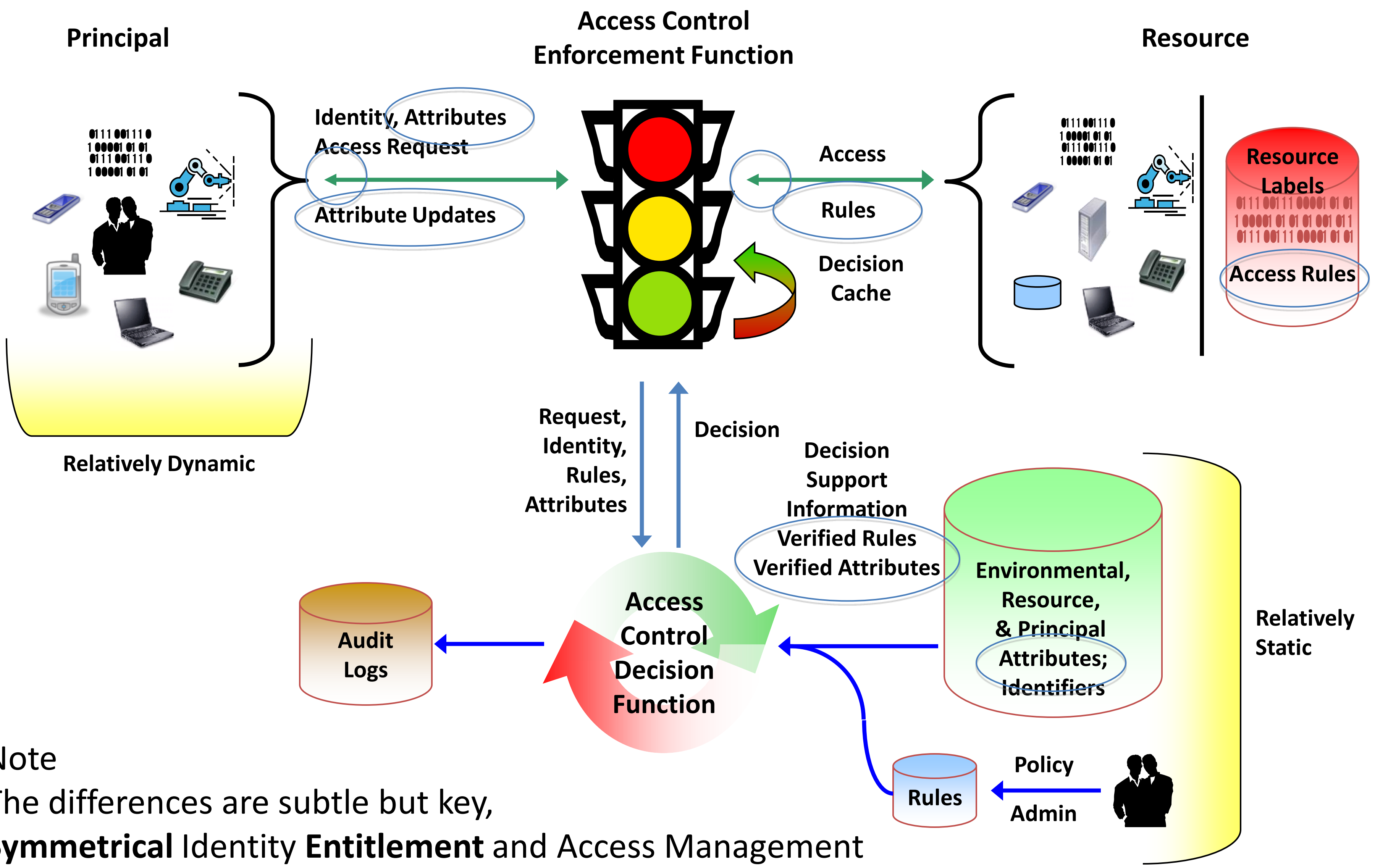
Note

The differences are subtle but key,

Symmetrical Identity, Entitlement and Access Management

Symmetrical

# Evolving Jericho Authorization Model



Principal

Access Control Enforcement Function

Resource

Identity, Attributes

Access Request

Attribute Updates

Access

Rules

Decision Cache

Resource Labels

Access Rules

Relatively Dynamic

Request, Identity, Rules, Attributes

Decision

Decision Support Information

Verified Rules

Verified Attributes

Environmental, Resource, & Principal Attributes; Identifiers

Relatively Static

Audit Logs

Access Control Decision Function

Rules

Policy

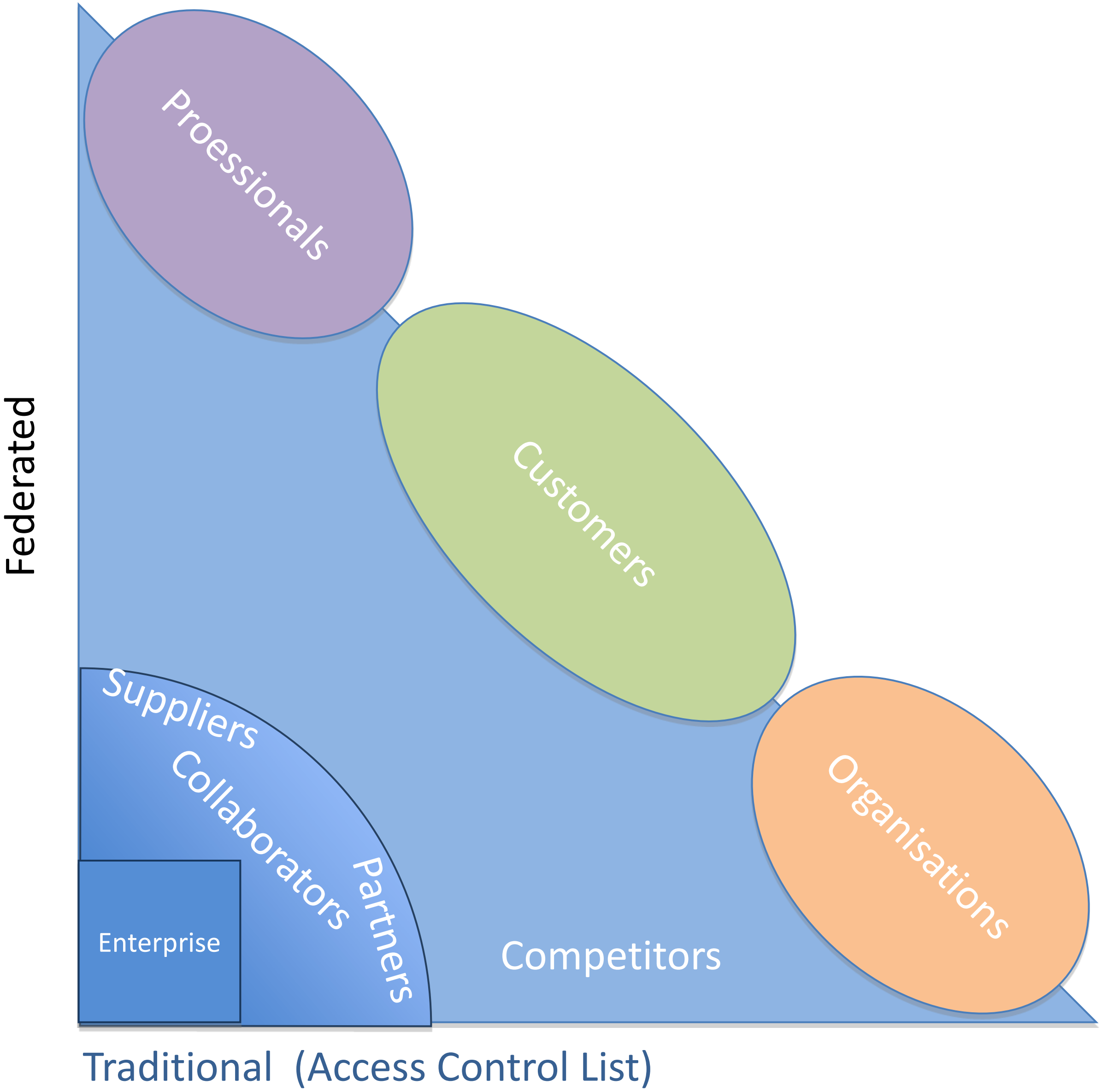
Admin

Note

The differences are subtle but key,

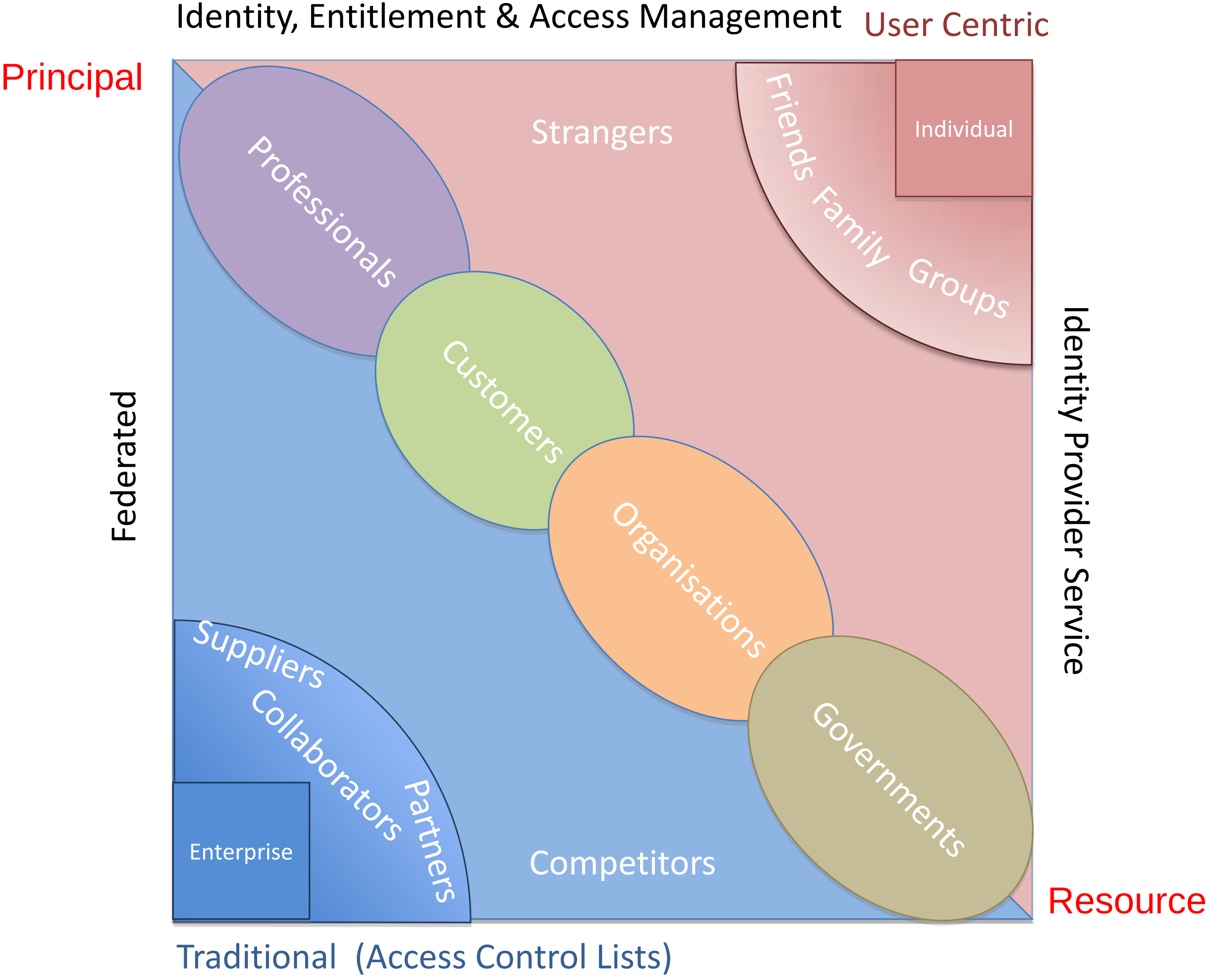
**Symmetrical** Identity **Entitlement** and Access Management

# Identity Shift #2



# Identity Shift #2

Identity, Entitlement & Access Management



# “Identity” Lifecycle of a Principal

- Create Identity
- Verify Identity
- Stake Claims (Set Identity Capabilities / Attributes)
- Verify Claims
- Use / Present Identity
- Authenticate Identity
- Request Resource
- State required Capability or Attribute (Claims)
- Authenticate Claims

# Identity is the key to the Clouds

| Old Frame | New Frame |
|---|---|
| • Enterprise Centric | • Principal Centric |
| • Access Control List | • Resource Centric |
| • Directory Server | • Rules Based Access |
| • Authentication Svcs | • Authentication Routing |

An ACTION for you ,to enable your **SHIFT**:
Get your architects defining and / or divining
the Access Rules that apply to YOUR resources.
Hint: Keep them Simple!

# And finally

- It's really all about the new perimeter…..
- ….the Identity Perimeter
- What are we Human’s or Ostriches?
- We have been complacent for too long!
- We need to bolster our defences at the same time as redesigning them.
- How best can we do that?

JERICHO FORUM

SELF ASSESSMENT SCHEME

“I see no Clouds”