

# Managing Trust-related Policies:

*how did we get here?*

*what's next for researchers?*

*(copyrighted images removed)*

Marianne Winslett

University of Illinois at Urbana-  
Champaign

-- *and colleagues* --





PART 1

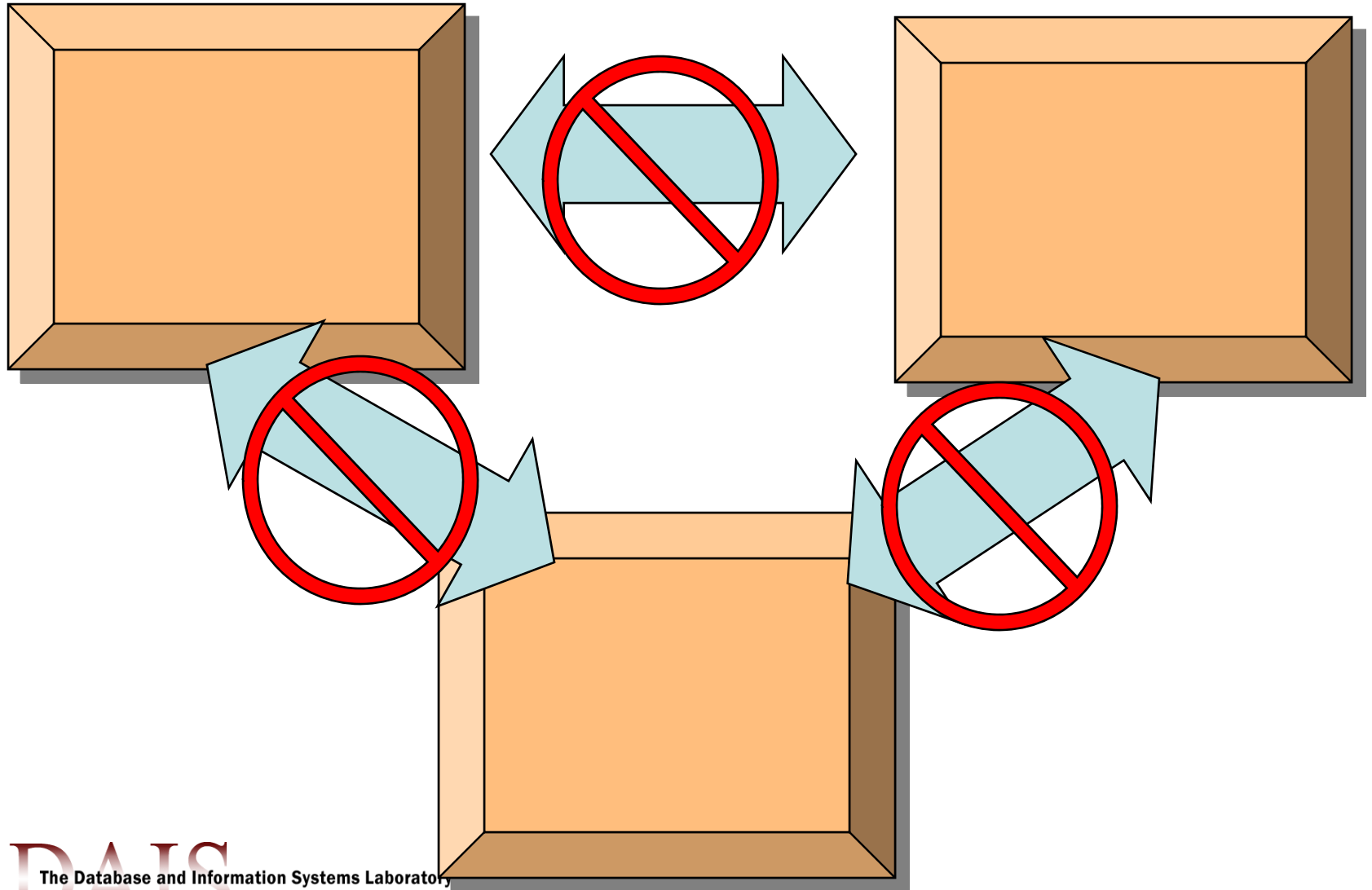
# WHY TRUST-RELATED POLICIES ARE GETTING MORE IMPORTANT



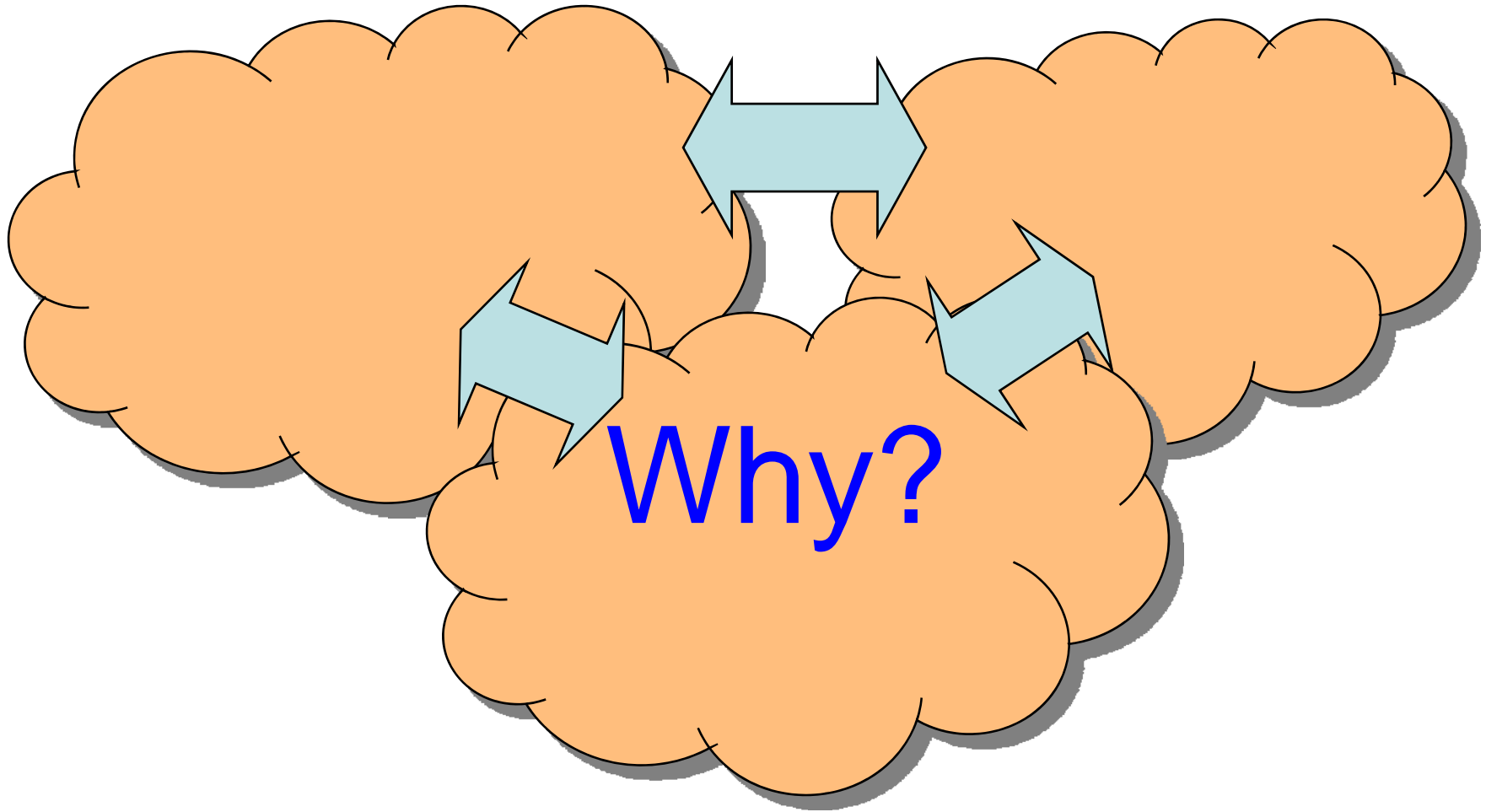
# A tale of two (example) trends



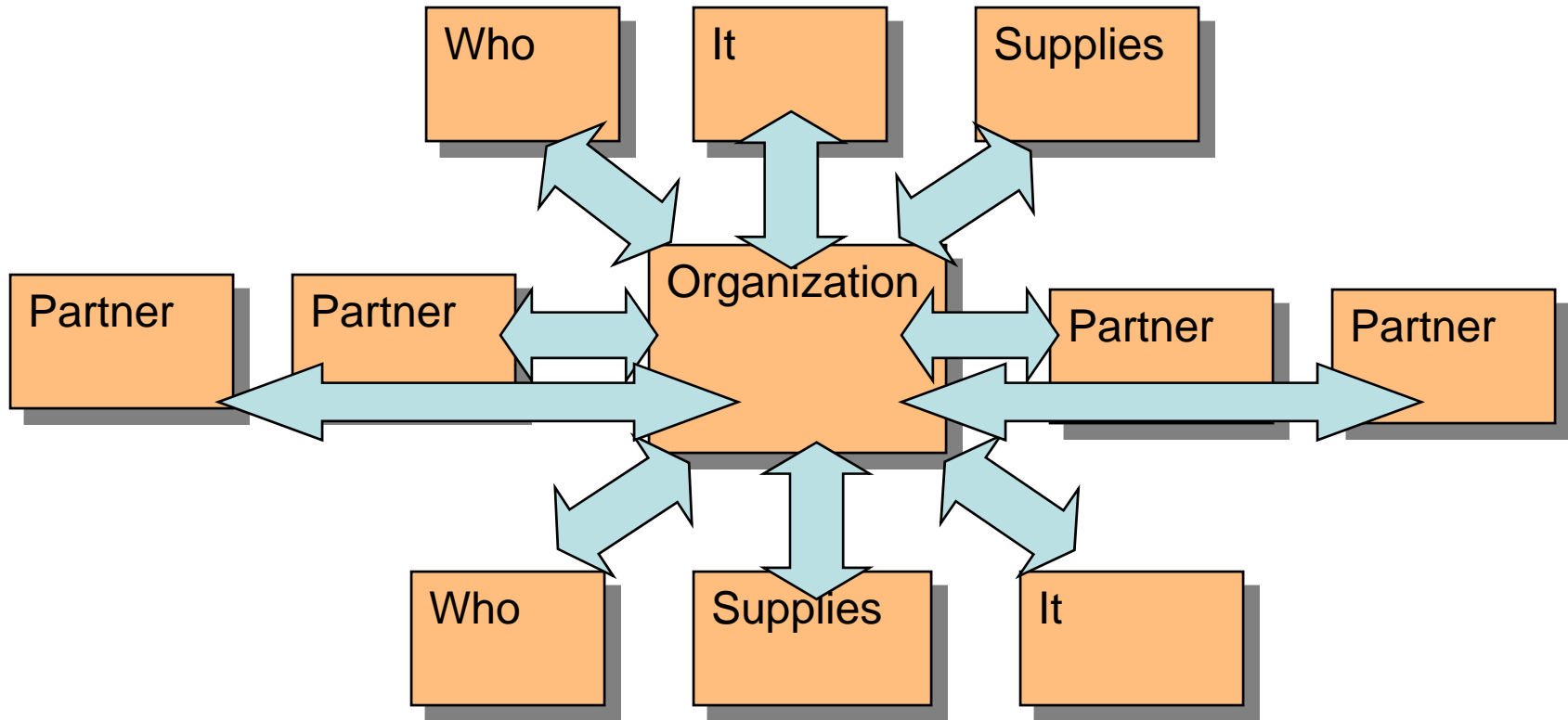
# Organizational boundaries used to be solid



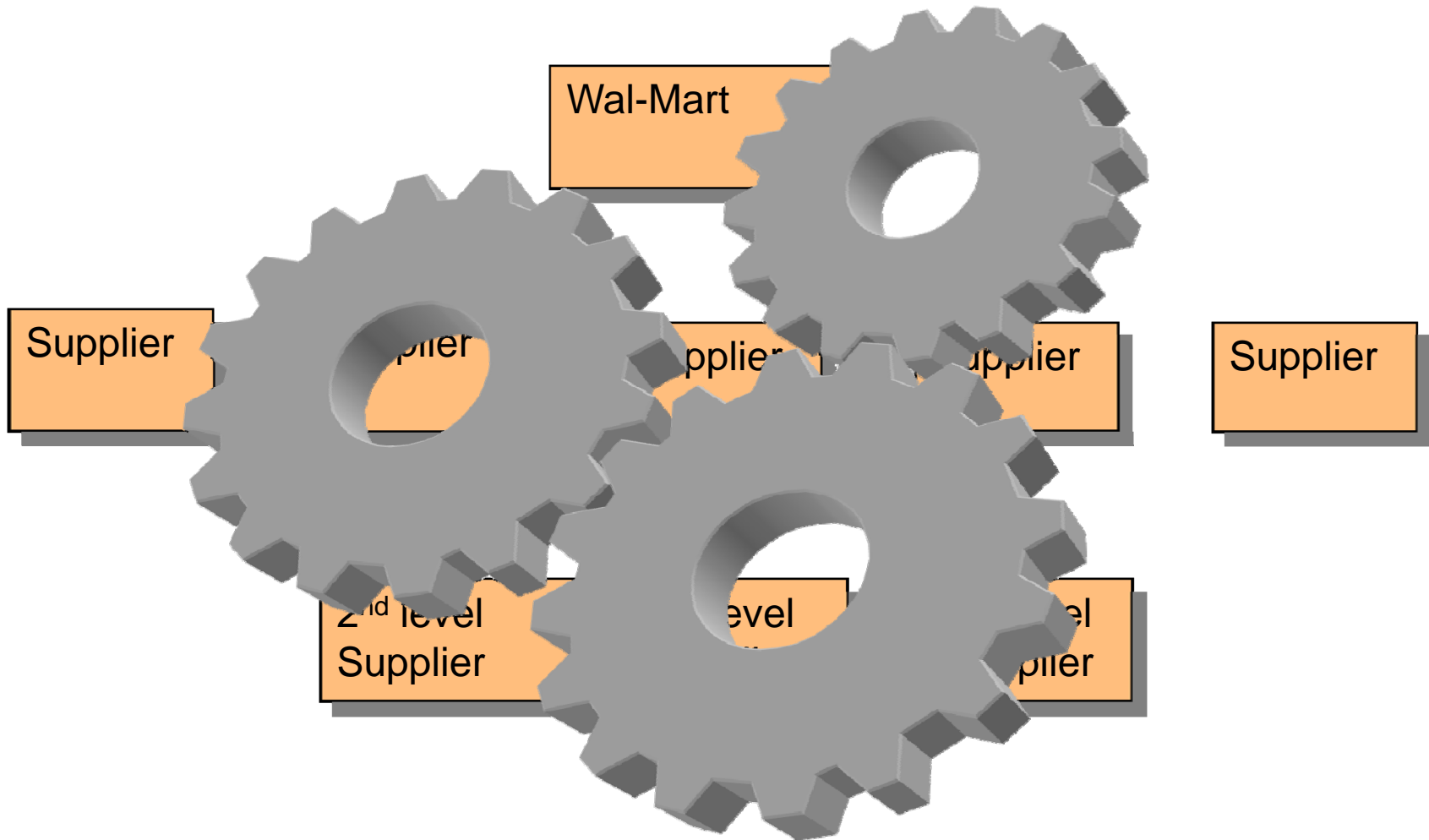
# Now boundaries are fuzzy



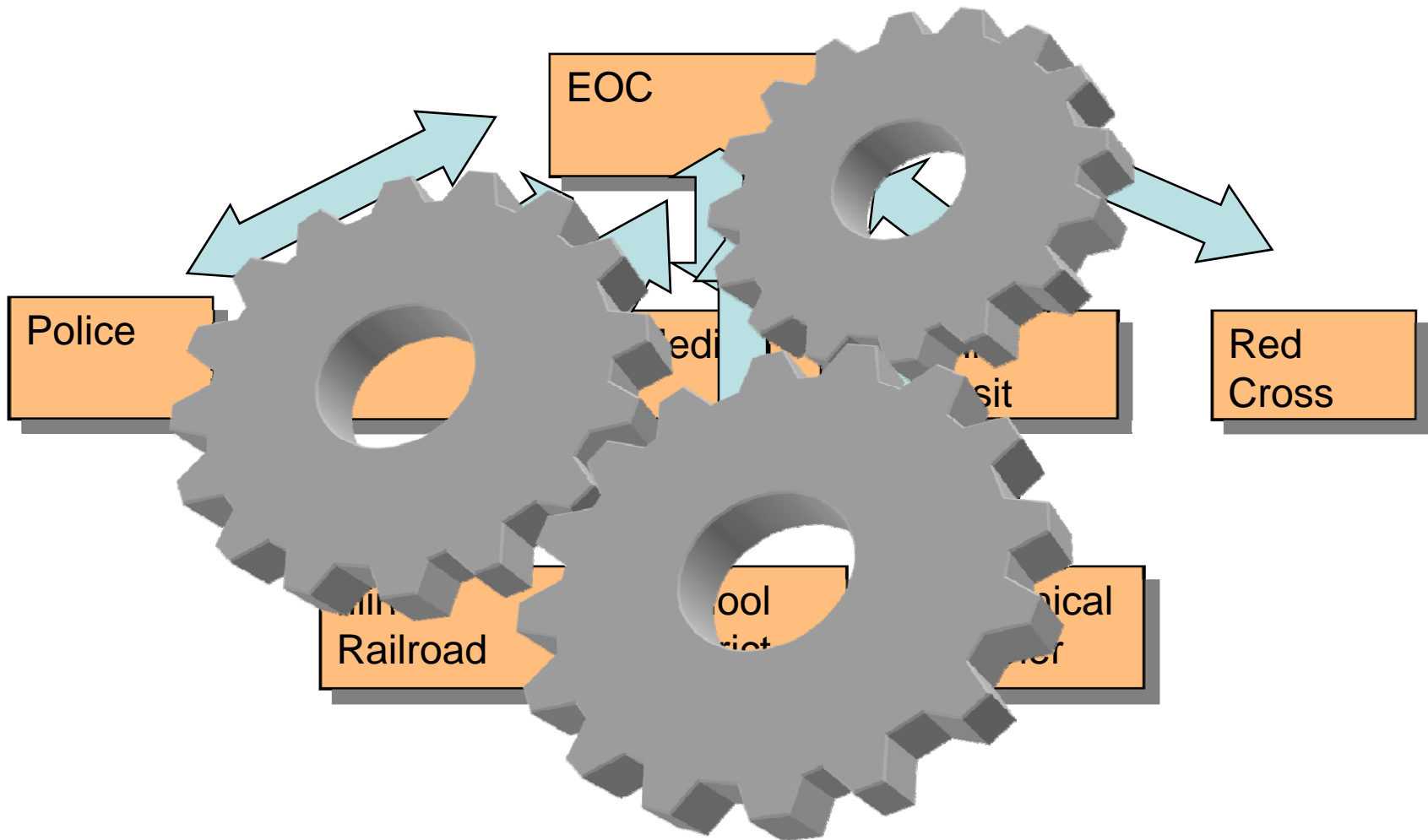
# Competitive pressures are dissolving boundaries



# Example: supply chains

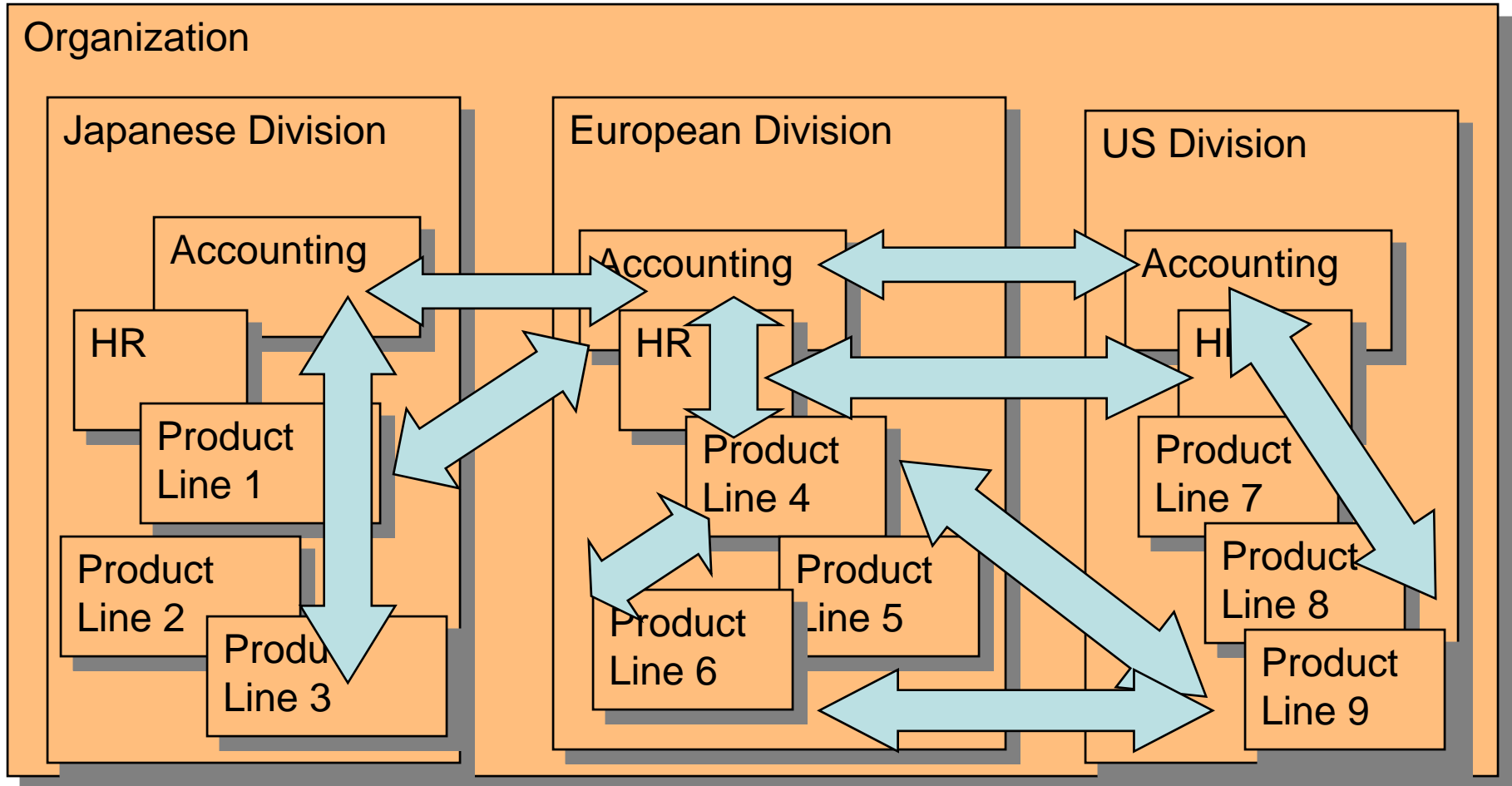


# Example: first responders

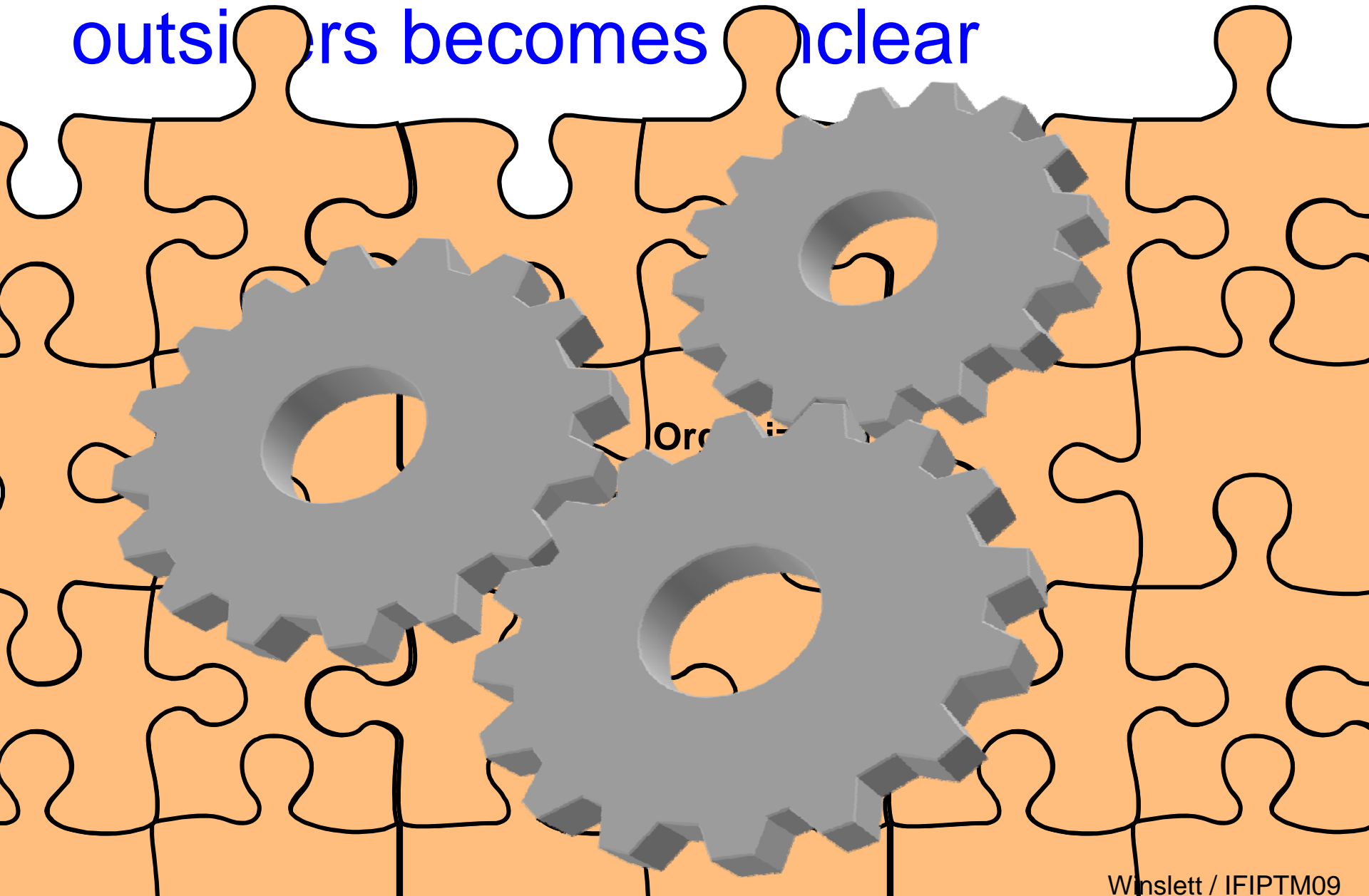




# Example: any large enterprise



# Distinction between insiders and outsiders becomes unclear



# Organizations are also facing new pressures for accountability

GLBA

HIPAA

FERPA

FISMA

OSHA

FDA

SEC Rule 17a-4

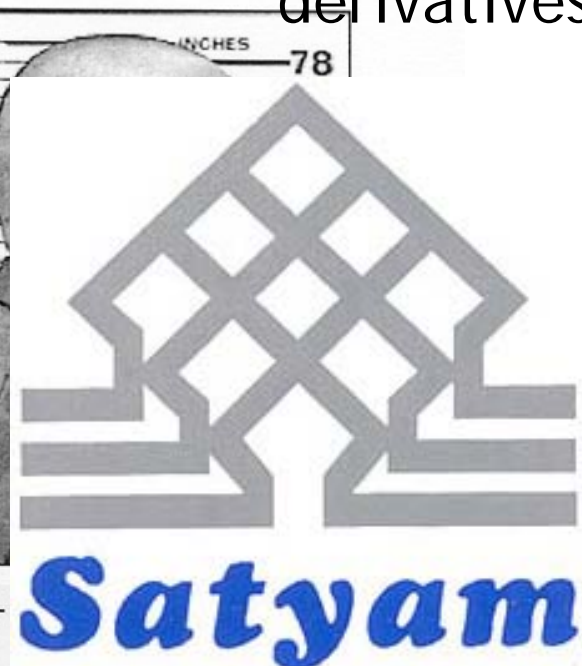
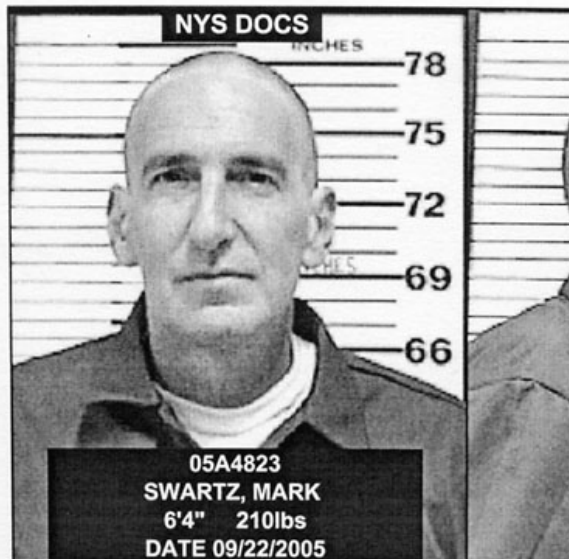
Sarbanes-Oxley



When something really bad happens, the government likes to quickly take action to restore society's trust in its institutions



- FDIC
- Sarbanes-Oxley Act
- Regulating derivatives



Sex - MALE Race - WHITE Hair - BLK/GR Eyes -



# SOX had major repercussions for corporate IT

- Top execs have to sign off on financial reports
- Retain routine business documents for (typically) 7 years, "tamper-proof"

Company	URL	Stock Symbol	Company Type	Price
Bravo Venture Group				

confirm e63537f677f002

File Edit View Message

From: [plone-users-request@lists.sourceforge.net](mailto:plone-users-request@lists.sourceforge.net)  
 Reply-To: [plone-users-request@lists.sourceforge.net](mailto:plone-users-request@lists.sourceforge.net)  
 Subject: confirm e63537f677f0027  
 Date: Sat, 21 Apr 2007 21:14:53

NATIONAL SECURITY COUNCIL  
 WASHINGTON, D.C. 20504

January 25, 2001

INFORMATION

MEMORANDUM FOR CONDOLEEZZA RICE

FROM: RICHARD A. CLARKE

SUBJECT: Presidential Policy Initiative/Review -- The al Qaida Network

*Clarke*  
 Steve asked today that we propose major Presidential policy reviews or initiatives. We urgently need such a Principals level review on the al Qaida network.

Just some Terrorist Group?

As we noted in our briefings for you, al Qaida is not some narrow, little terrorist issue that needs to be included in broader regional policy. Rather, several of our regional policies need to address centrally the transnational challenge to the US and our interests posed by the al Qaida network. By proceeding with separate policy reviews on Central Asia, the GCC, North Africa, etc. we would deal inadequately with the need for a comprehensive multi-regional policy on al Qaida.

al Qaida is the active, organized, major force that is using a distorted version of Islam as its vehicle to achieve two goals:

- to drive the US out of the Muslim world, forcing the withdrawal of our military and economic presence in countries from Morocco to Indonesia;
- to replace moderate, modern, Western regime in Muslim countries with theocracies modeled along the lines of the Taliban.

AIM IM with davisrefdesk from hmcpherson0893

File Edit View People Help

Text Talk Video Files Invite

Do you know this person? [Report IM Spam](#)

hmcpherson0893 (11:48:52 AM): Hi, I am looking for an article by Bloss called " Cohabiting, Decohabiting, Recohabiting: The Routes Followed by Two Generations of Women." Could you help me?

davisrefdesk (11:49:20 AM): Sure, have you tried looking in any of the Library's databases?

Arial 10 B U a

Search the Web Go Expressions Send

ing list subscription confirm e-Users

ave received a request from our email address, "[plone-users-request@lists.sourceforge.net](mailto:plone-users-request@lists.sourceforge.net)" to be added to this mailing list. The Subject: header intact

<http://lists.sourceforge.net/lists/confirm/e63537f677f0027>

include the following line --  
 add the following line to [plone-users-request@lists.sourceforge.net](mailto:plone-users-request@lists.sourceforge.net)

confirm e63537f677f0027:

that simply sending a 'reply' to this message should work from mail readers, since that usually leaves the Subject: line in the correct form (additional "Re:" text in the Subject: is okay).

Click to open <https://lists.sourceforge.net/lists/confirm/plone-users/e63537f677f0027240c894f6d/>



Bison Gold E	BGEI (NQG)	Explorer	0.50					
Bravo Venture Group	BVG (TSX-V), B9I (XETRA, B, FRA, STR, MUC)	Explorer, Developer	1.440	CAD	0.38/1.98	103128326	01.02.2007	71616880 01.02.2007

# Compliance regulations have teeth: periodic audits, fines, jail terms

SEC Rule 17a-4:

\$1.65M each

Deutsche Bank

Goldman Sachs

Morgan Stanley

Solomon Smith

Barney

U.S. Bancorp



SOX:

Rica Foods CEO \$25K

Deloitte \$1M poor audit

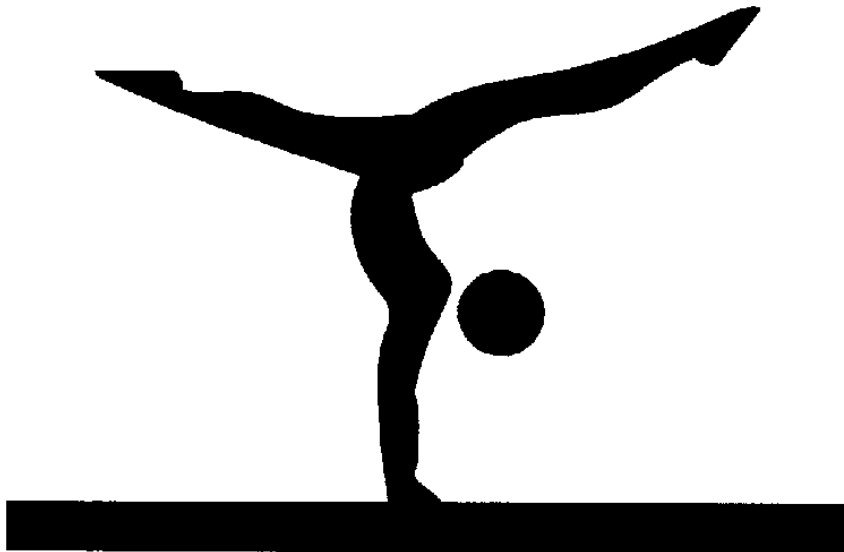


# The government likes to step in for non-corporate scandals as well.



- Video Privacy Protection Act of 1988
- Gramm-Leach-Bliley Act's Financial Privacy Rule
- Health Insurance Portability and Accountability Act (HIPAA)

# E-government records are also at risk for falsification.



How old is your athlete?



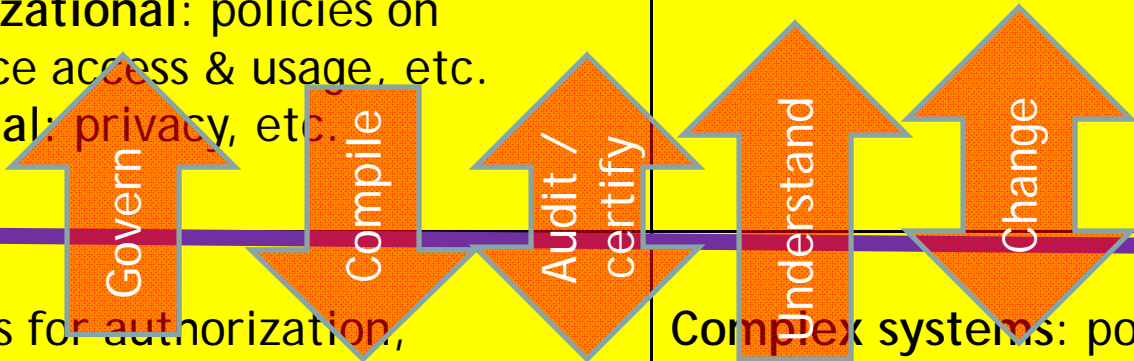


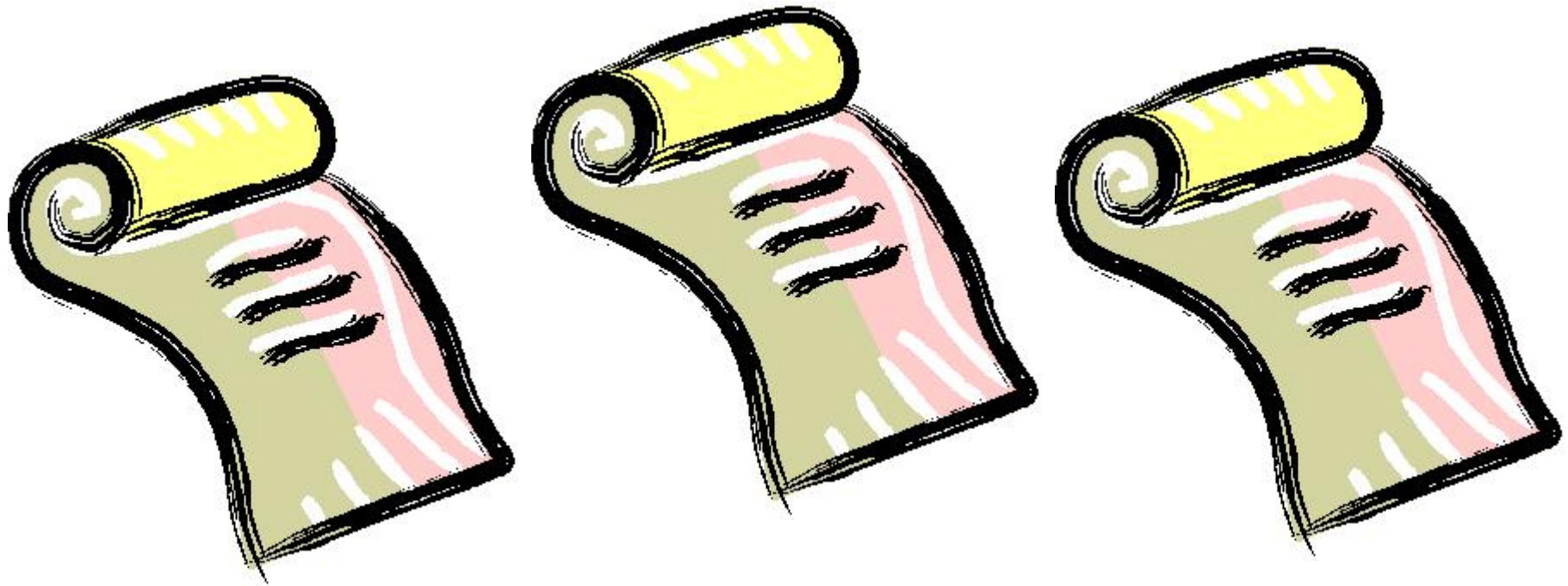
# Accountability includes knowing who can/did do what to your data when



We use policies when our intent is too hard to specify, implement & manage directly.

	Trust-related	Not Trust-related
Intended for humans	<p><b>Not computer-enforceable</b></p> <p><b>Regulatory:</b> Sarbanes-Oxley, SEC Rule 17a-4, HIPAA, FERPA, FISMA, etc.</p> <p><b>Organizational:</b> policies on resource access &amp; usage, etc.</p> <p><b>Personal:</b> privacy, etc.</p>	<p>Regulations and requirements documents in general</p>
Intended for computers	<p>Policies for authorization, authentication, release, privacy, usage, audit, retention, shredding, availability/replication, backup, logging, obligations (e.g., notification) and more...</p> <p><b>Computer-enforceable</b></p>	<p><b>Complex systems:</b> policy-based networking, firewalls, configuration management, ...</p>



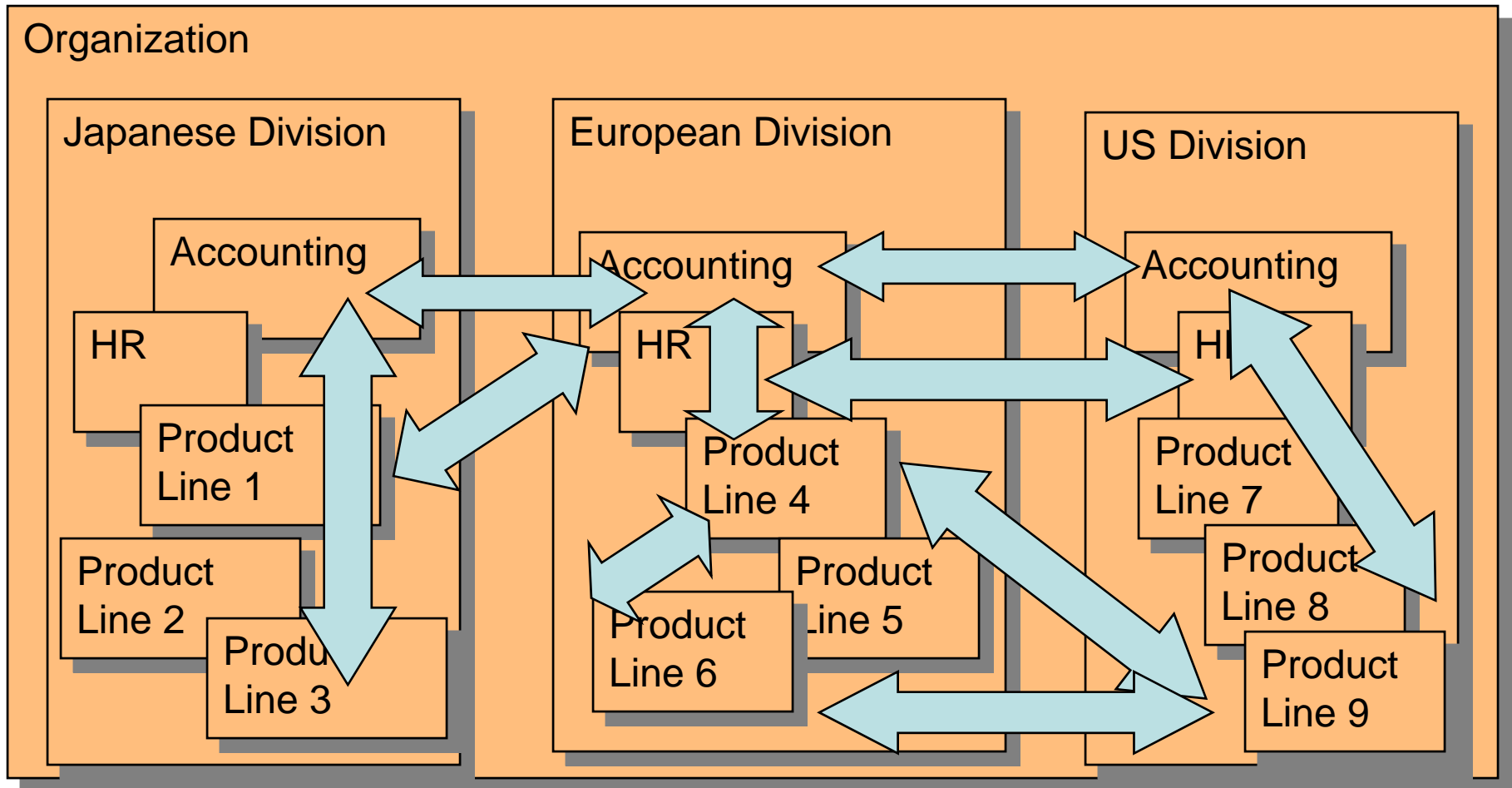


PART 2

# THE RISE OF POLICY-BASED SYSTEMS



# Example: any large enterprise



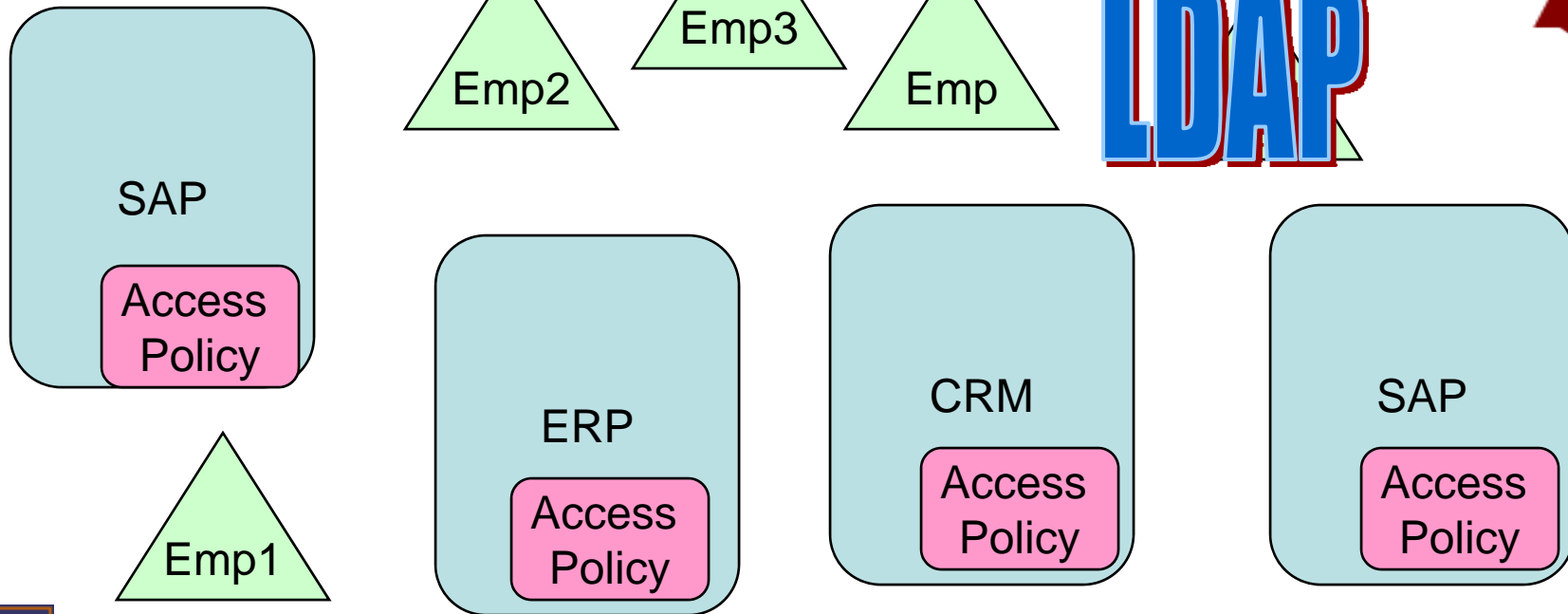
# Industry is taking several steps to meet these needs

Strong authentication (X.509)



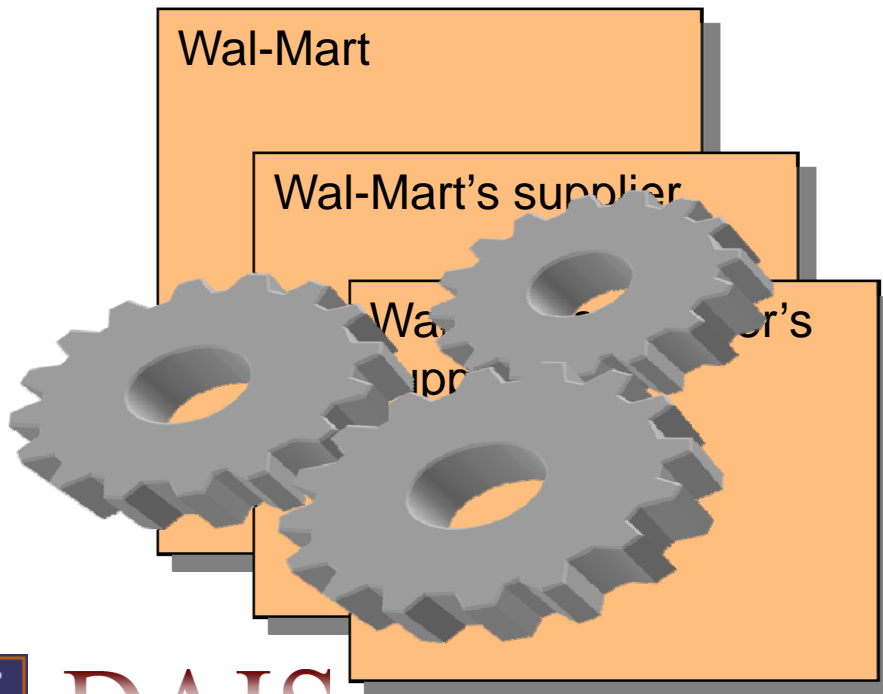
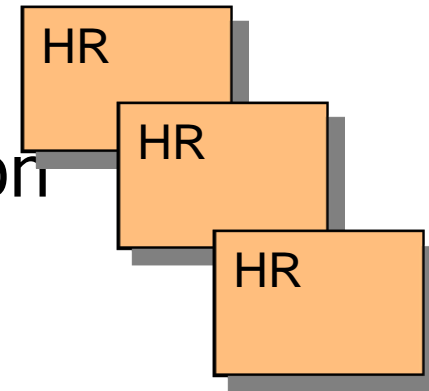
Centralize role definitions, base on attributes

Get access control out of apps (some day)



# So enterprises are moving toward attribute-based access control

- Based off centralized LDAP + X.509
- Avoids inconsistency due to distribution
- Easier to maintain, compared to ACLs



Less insider threat

I claim that policies are becoming more important in other trust-related areas, too.

Firewalls

Routing

How long must we retain this address tuple?

...



# Aren't policy-based trust-related systems a good thing?







# Why this scares me:

Automated  
exploitation of  
policy errors &  
loopholes



# Why this scares me:

Centralized policy-based  
services can be attacked



# Why this scares me:

Understanding policies

Industrial policy languages  
were not intended for  
rigorous analysis or user-  
friendliness

Analysis tools

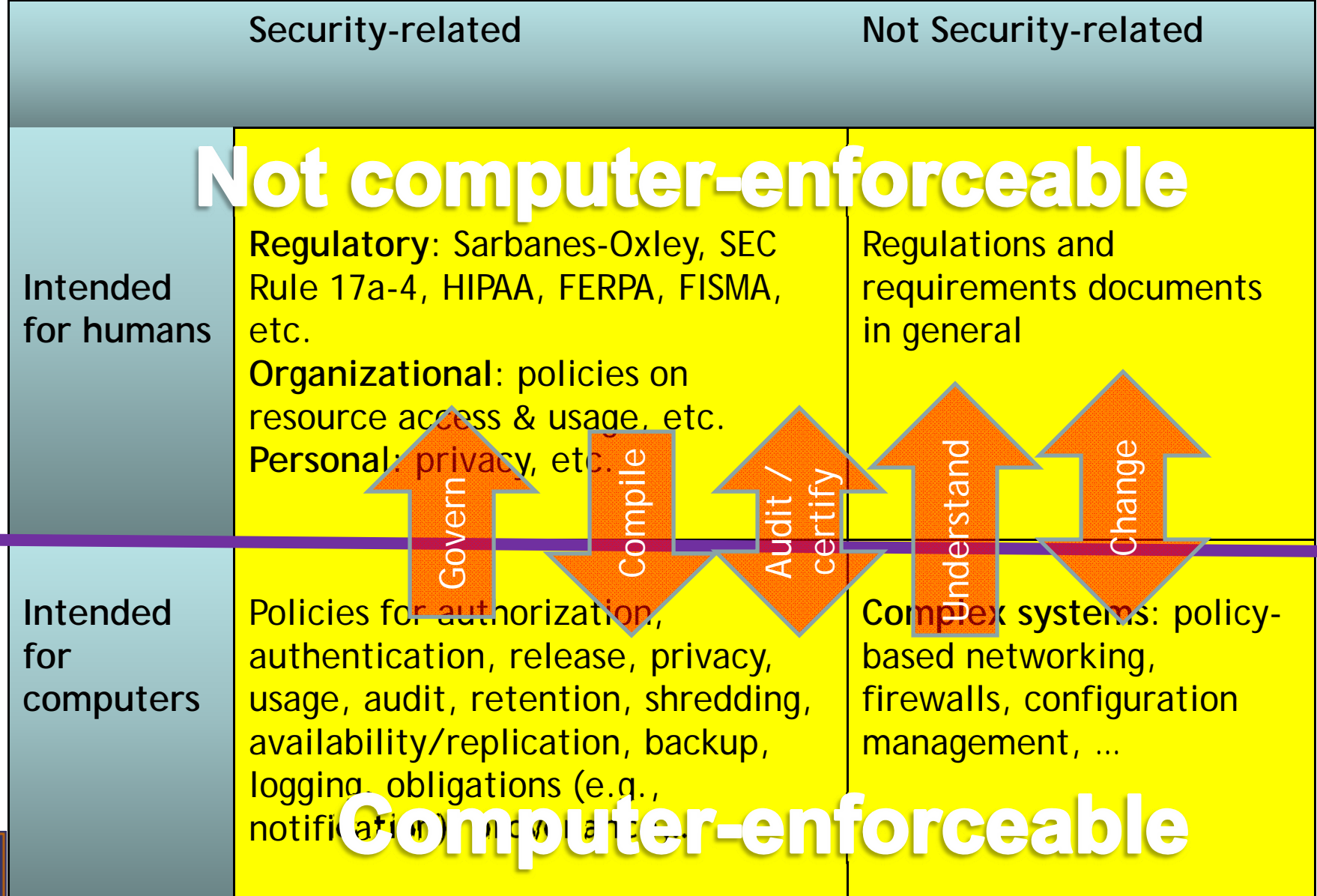


PART 3

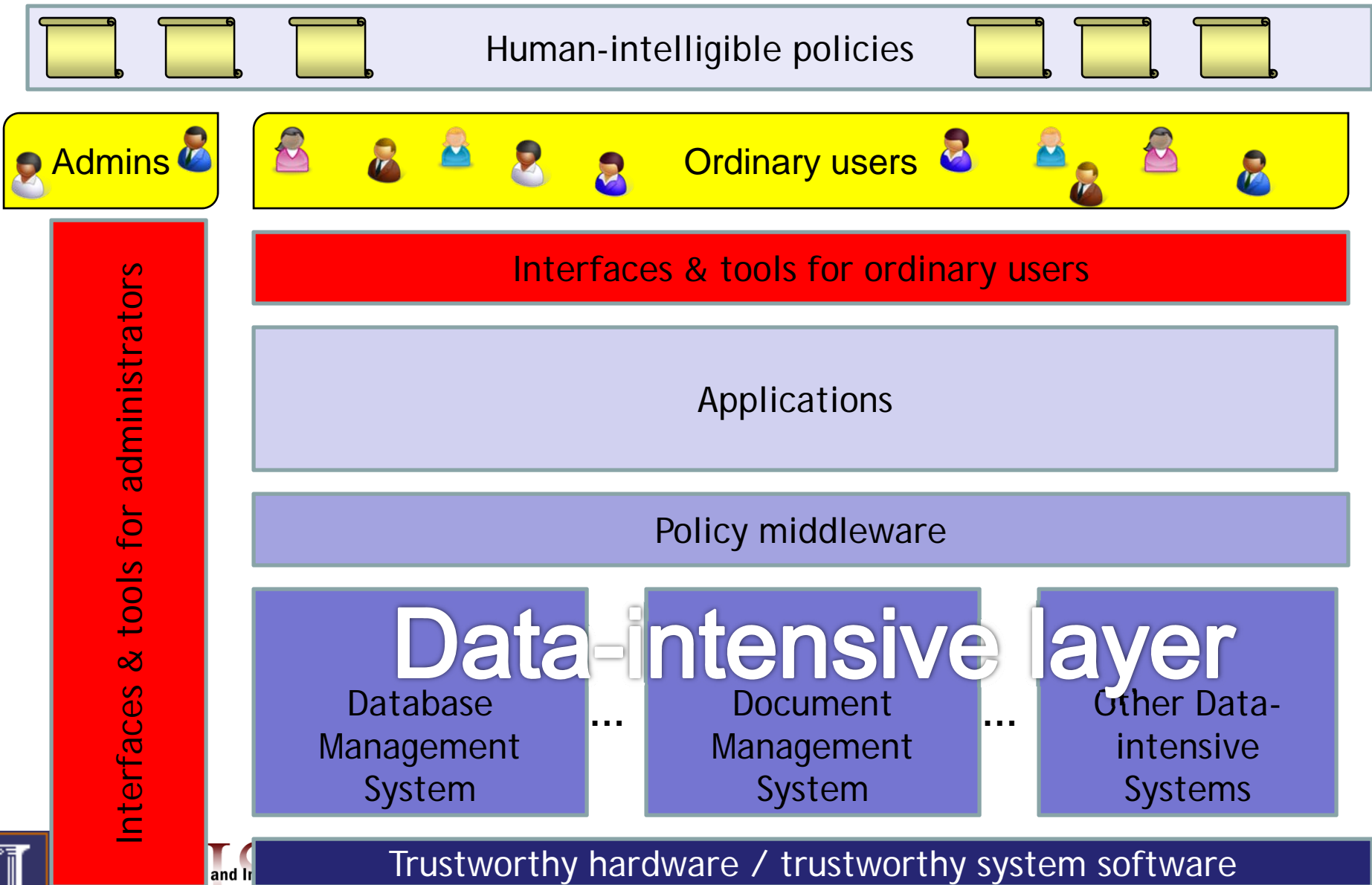
# WHAT CAN WE DO TO HELP?



We use policies when our intent is too hard to specify, implement & manage directly.



# Advances are needed at & between *all levels* of the system.



# We need *easy-to-use* tools for policy admins.

Interfaces & tools for administrators

Understand

Change

- To help them visualize & understand enormous policies
- To analyze large policies
  - Safety and availability questions: Can this user take this action under these conditions?
  - What-if analysis, regression testing for proposed policy changes
  - Explanation of why particular actions were taken
  - Conflict identification & resolution
- Compile policies into actionable enforcement (discussed later)
- Rewrite policies to equivalent form to make them faster, simpler, or meet other goals







# We need **easy-to-use** tools for ordinary users.

## Interfaces & tools for ordinary users

- To manage their own policies: all the tools that system administrators need, but with an interface suitable for them
- For real-time discovery of a system's policies that are relevant to them or to their software agents
- To understand why a particular policy-based action was taken (e.g., their access request was denied), and actionable steps they can take to change that outcome



# We need policy languages, compilation techniques for every situation.



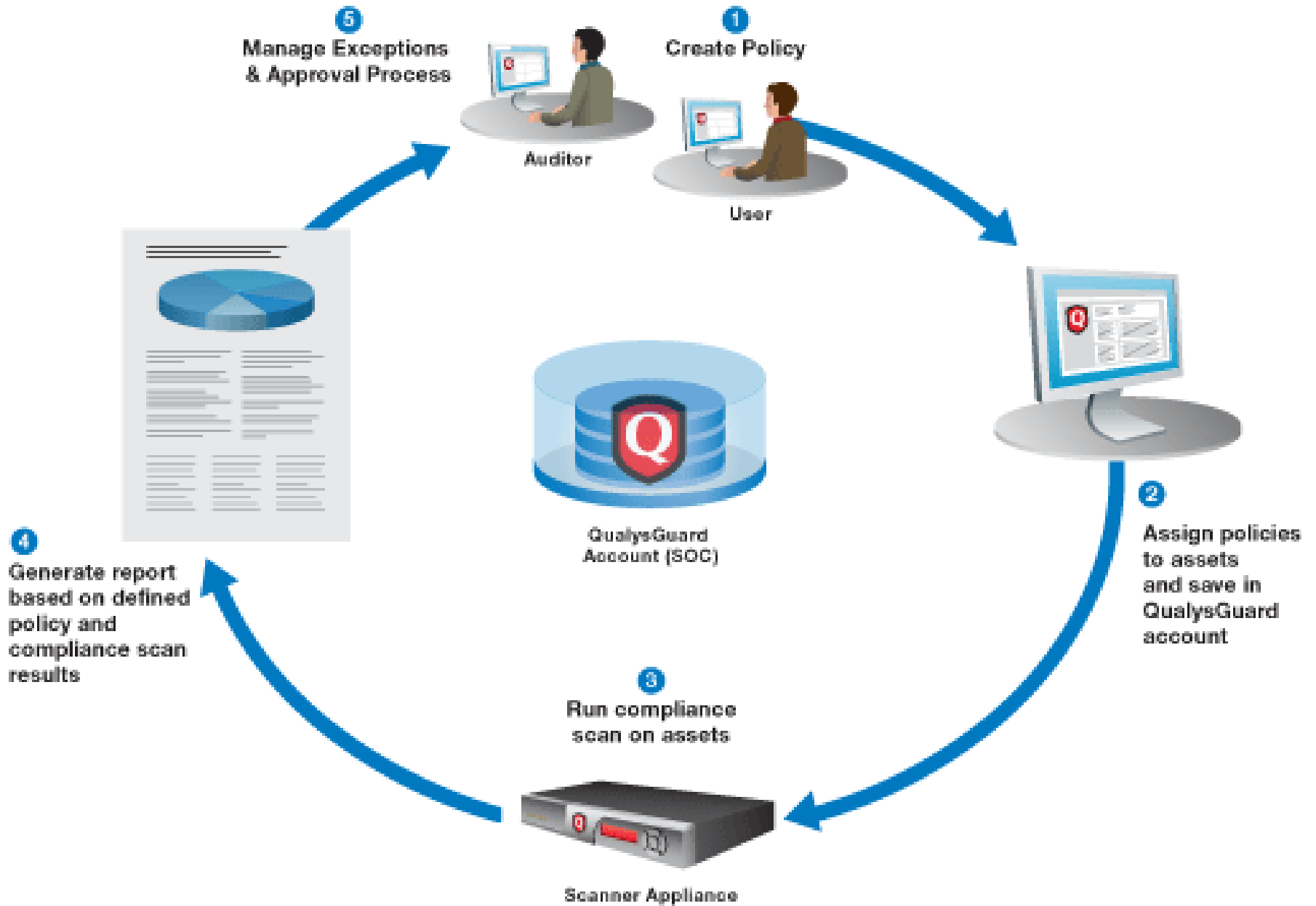
- User-friendly, domain-appropriate languages (SPARQL, workflow)
- Analysis-friendly languages a la Datalog
- Computer-friendly languages a la XACML, WS-POLICY
- Ways to compile a high level language down into actionable enforcement a la SPARCLE
- Bridge gap between policy languages favored by research, industry

(e.g.,  
XACML

vs.

Datalog)





SPARCLE is a research prototype of a policy management workbench. SPARCLE allows the polic

# IBM's SPARCLE policy workbench



**Policy Name :** My Bank Policy      **Domain :** Finance      **Created Date:** 2005-07-27  
**Policy Description :** Template for privacy policies in American divisions.      **Last Modified Date :** 2005-07-27

## Example Rule Guide:

**[User Category(ies)] can [Action(s)] [Data Category(ies)] for the purpose(s) of [Purpose(s)] Condition(s)] with [(optional) Obligation(s)].**

1. Customer service reps and tellers can modify or use account numbers or customer name to confirm identity.
2. Loan officers can use credit history or salary to make loan decisions.
3. Marketing reps can use customer mailing address for the purpose of send marketing information if customer has opted-in.



SPARCLE Privacy Policy Workbench - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back - Search - Favorites - Media - Bluetooth

Links Search the Web with Lycos

Address http://localhost:9080/SPARCLES/transform.jsp

Go

Privacy Policy  
Administration  
Change password  
Logout

Original Rule: Customer service reps and tellers can modify or use account numbers or customer name to confirm identity.

Parsed Rule:

1. Customer service reps or tellers can modify use account numbers or customer name to confirm identity.
1. Customer service reps or tellers can modify use account numbers or customer name to confirm identity.
2. Loan officers can use credit history or salary to make loan decisions.
3. Marketing reps can use customer mailing address for the purpose of sending marketing information if customer has opted-in.

Create Rule To create a new rule, click the *Create Rule* button, select the elements of the rule from the categories as desired, and then click *Save Rule* button.

Modify Rule To modify a rule, select the rule to be modified, then select or deselect elements in the appropriate category and when the rule elements appear as desired, click *Modify Rule* button.

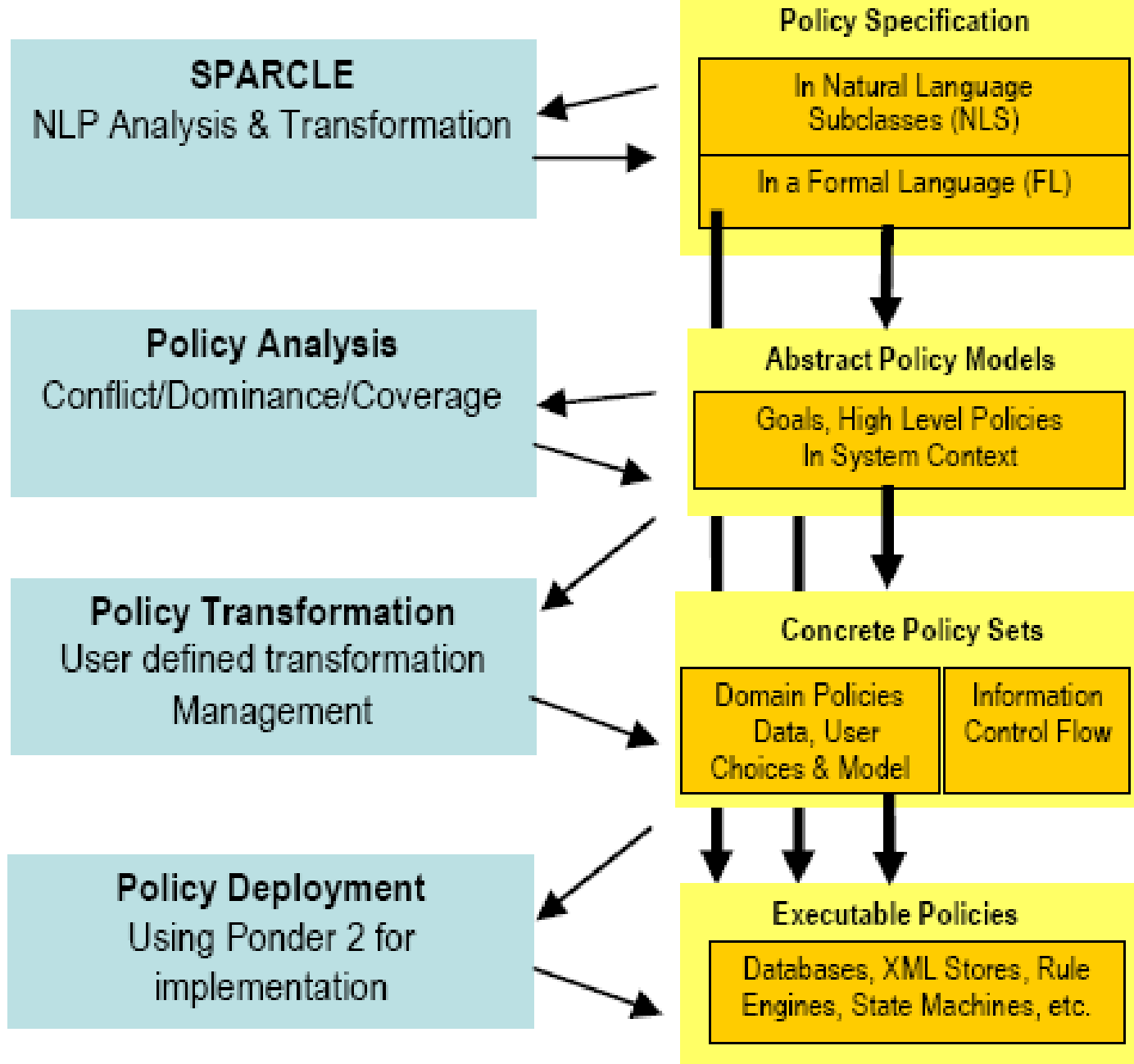
Delete Rule To delete a rule, select a rule and click the *Delete Rule* button.

User Categories	Actions	Data Categories
<input type="checkbox"/> None Selected	<input type="checkbox"/> None Selected	<input type="checkbox"/> None Selected
<input type="checkbox"/> billing reps	<input type="checkbox"/> collect	<input type="checkbox"/> account numbers
<input checked="" type="checkbox"/> customer service reps	<input type="checkbox"/> delete	<input type="checkbox"/> credit card number
<input type="checkbox"/> financial consultants	<input checked="" type="checkbox"/> modify	<input type="checkbox"/> credit history
<input type="checkbox"/> loan officers	<input type="checkbox"/> use	<input type="checkbox"/> customer mailing address
<input type="checkbox"/> marketing reps		<input checked="" type="checkbox"/> customer name

Address Go 73%

“In coordination with IBM Research, IBM Global Business Services (GBS) has used the SPARCLE policy management workbench to help clients with a variety of policy-related issues, ranging from policy definition to policy templates for mandated compliance requirements such as HIPAA and SOX. In addition, GBS clients have used SPARCLE to assist in policy gap analysis, policy conflict resolution and streamlining, and verification of policy consistency.”





From the  
demo by  
Brodie et al.  
in POLICY  
2008

Figure 1. The Components Demonstrated through the Coalition Policy Management Portal.

# We need advances in runtime facilities for policy-based systems

- **Usability:** clean ways to involve the human in the loop as needed, & make their task easy (no 16-digit passwords)
- **Scalability**
  - Fast policy compliance checking at runtime
  - Fast run-time automated resolution of policy conflicts, multiple-choice situations
  - Fast provenance collection, interpretation
- **Sticky policies:** how to ensure enforcement, esp. across organizational boundaries?



# We need user-friendly approaches to help with compliance and audit

*\$250B/year losses due to insiders:  
how to track/undo what they did?*



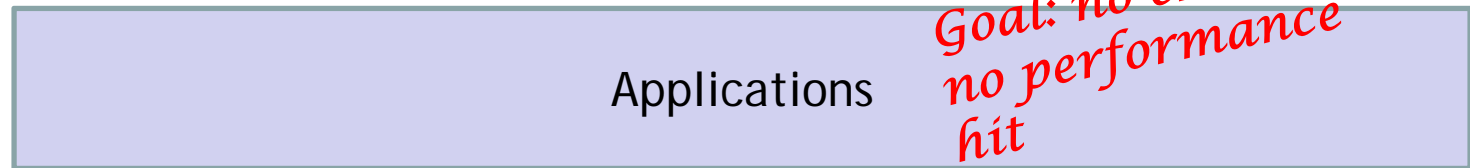
- Prevent non-compliance, when possible
- Automate audit of activity (self-auditing)
- Validate actionable policies against specification
- Evaluate effectiveness of policies against intended high-level goals
- Forensic analysis to identify instances of non-compliance, determine/undo their effects as appropriate (self-healing)

*Concentrate on prevention for long-term, widely deployed policies (e.g., SOX)*

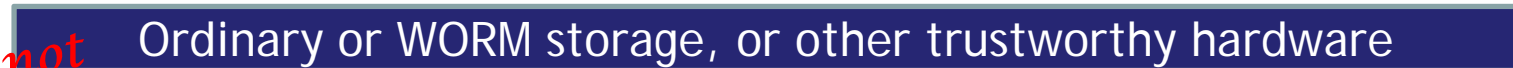
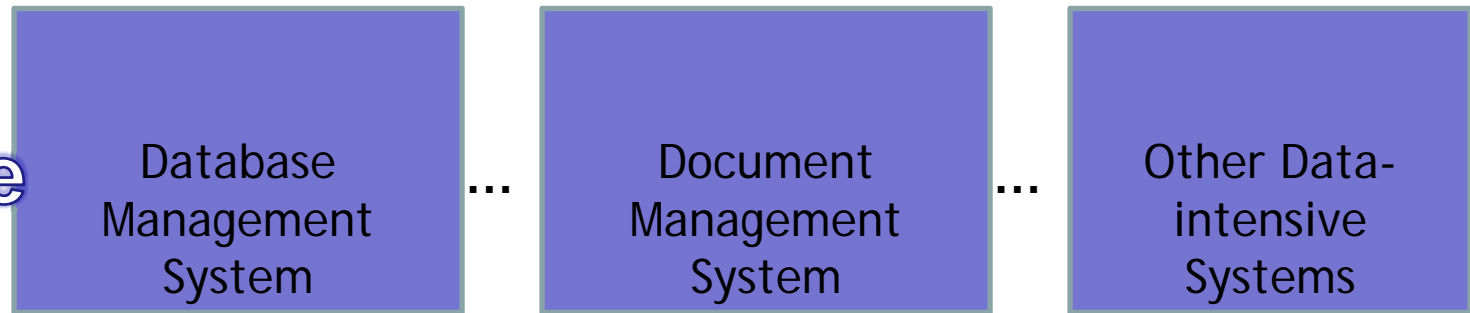




# Example: low-cost high-integrity long-term retention of data, documents, logs for SOX



Data-intensive layer



*Goal: even sysadmins cannot tamper with the data or query answers*

*Goal: Cheap*

## Research challenges:

- Provide trustworthy search, indexing, query answers, & shredding
- Develop/exploit cheap new trustworthy hardware
- Recover from vandalism
- Support fast audits & forensic analysis (what/when/where/how)
- Supporting technology (e.g., de-duplication)

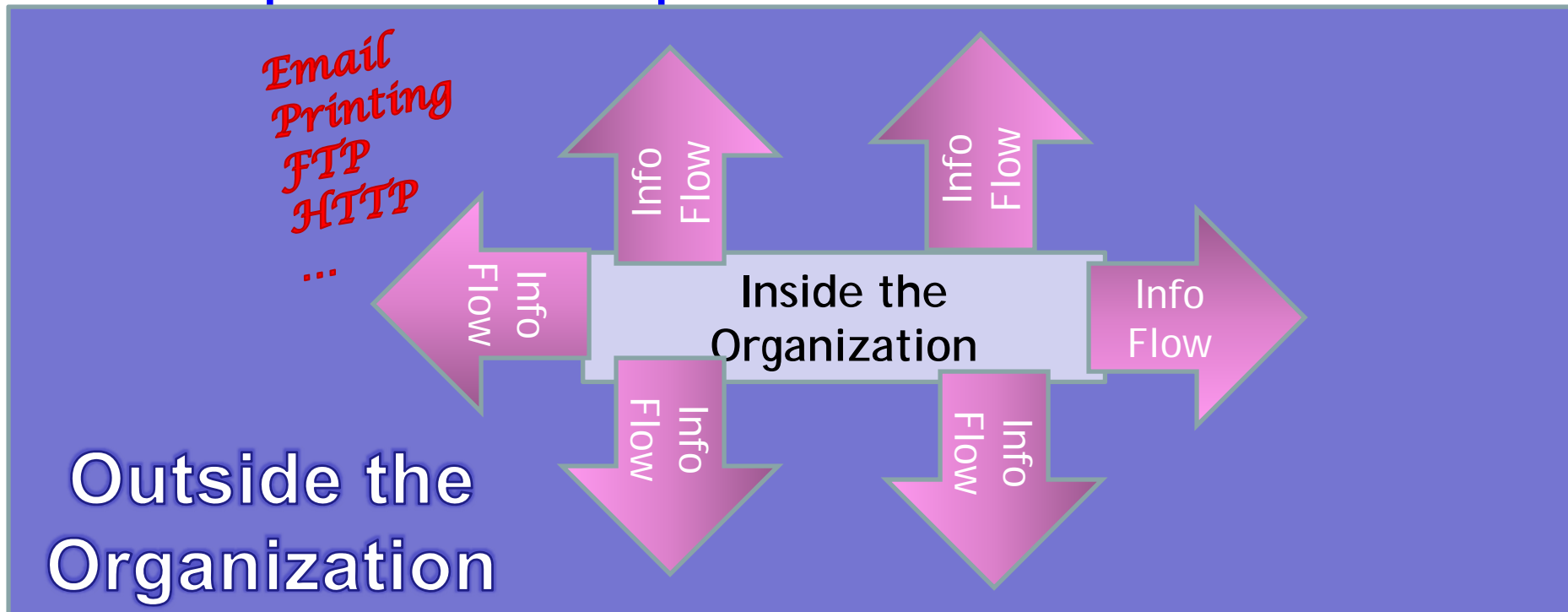


**DAISE**

The DAISE and Information Systems Laboratory

at The University of Illinois at Urbana-Champaign  
Large Scale Information Management

# Example: release policies



## ***Research challenges in controlling release:***

- Fast classification of text, including topic and sentiment identification
- Appropriate handling of encrypted content, tables, figures, images, speech, ...
- How to deal with use of outside resources: gmail, clouds, ... (often adopted because security is not usable)





**DAIS**

**The Database and Information Systems Laboratory**

at The University of Illinois at Urbana-Champaign  
*Large Scale Information Management*

# Example: auditing cloud SLA compliance

My Data and Services

The Cloud

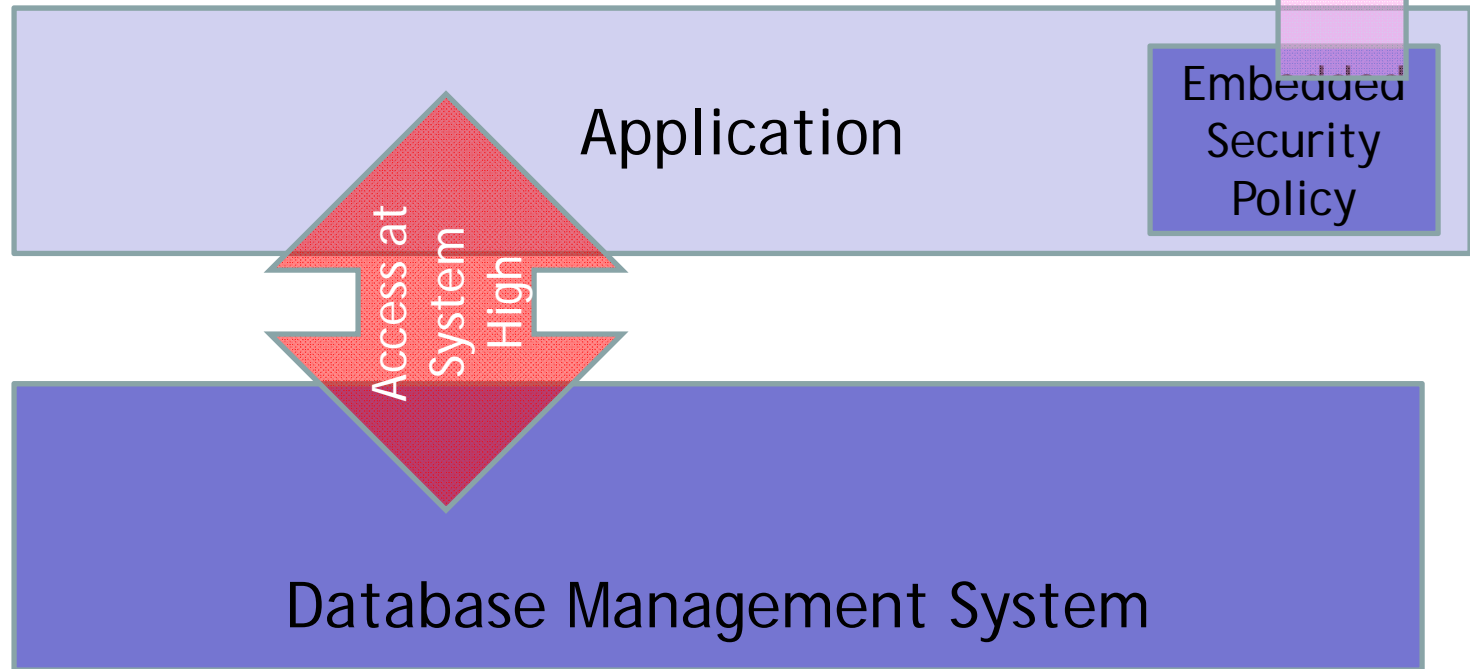
## ***Research / usability issues:***

- Where is my data and how is it being stored?  
(determines regulations, compliance, (sticky) policies to comply with)
- What cloud promises are amenable to user verification, and how can we perform that verification?



# Example: finer-grained policies for DB access

*Trend: pull out, centralize embedded policies*



**Goal:**  
*data-, app-, & user-  
 dependent control over  
 access to each DB cell, to  
 make DB self-protecting*

## **Research challenges:**

- Appropriate semantics for policies
- Acceptable performance hit at run time
- Usability
- Sticky policies based on, e.g., data provenance



# Example: modern organizations employ *risk management*

Assess risks to the organization's mission

## **Research issues:**

- How to evaluate policy effectiveness in reducing risk

Devise policies to bound the risk at acceptable levels

Review the effectiveness of the policies

- How to reflect risks directly in policies (e.g., variants of risk-based access control)



There are many interesting research issues in regulatory compliance beyond SOX, SEC Rule 17a-4, & HIPAA.

## Methodology:

- Understand the regulation and *how it is currently enforced*
- Understand what threats the regulation targets
- Translate those threats into IT-level threats
- Devise novel low-cost IT to address those threats
- *Tech transfer*: Convince policymakers to require its use

**Example potential targets:** e-govt vital statistics (birth, death, marriage, voter, etc.); stronger assurances for FERPA, GLBA, FISMA at minimal cost



# SOX targets CFOs tampering with the info that goes into quarterly reports. Translate that to IT threats:

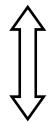


*Commit Record*



Alice

**Trustworthy**

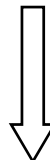


*Regret*



Adversary

**Bribed Superuser**



*Query*



Bob



*Integrity Check*



Auditor

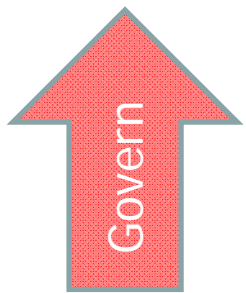
**Trustworthy**





# IT governance means knowing what your assets and policies are.

- Industry sells tools for asset discovery; *what are the open IT-level problems?*
- Policy discovery: how to extract policies embedded in legacy software?
- Role engineering/mining/discovery: how to mine roles from activity logs?
- Permission provisioning: how to assign permissions to new users?
- Can we use cutting-edge info integration techniques to *understand* the information that we find (e.g., determine the meaning of schemas, find PII)?



In conclusion: there's a lot of interesting research to do in policy-based systems.

