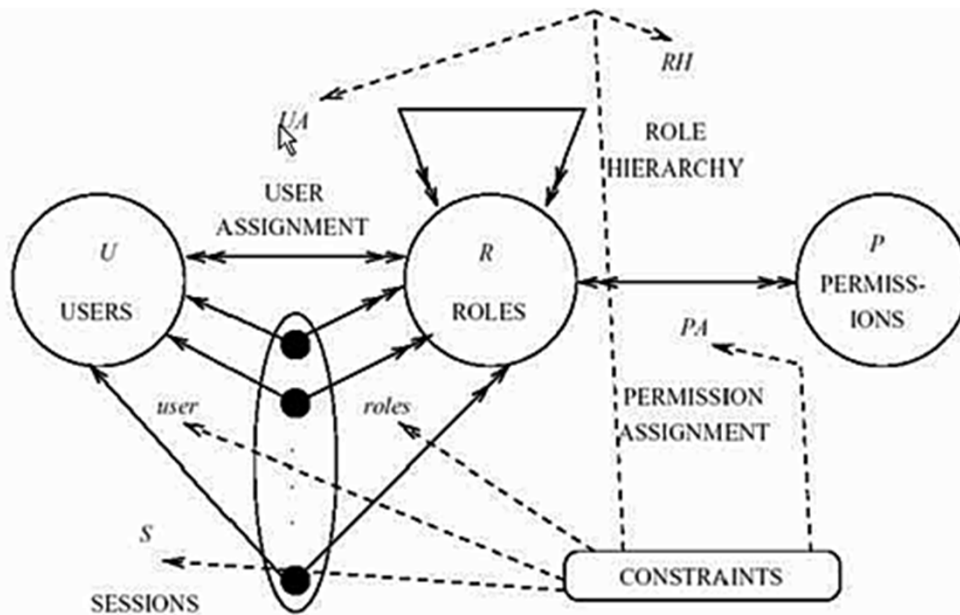


# Role-Based Access Control INCITS CS1 Standards Series



Tim Weil – CISSP, CISA, CRISC  
Security Architect  
Editor – INCITS CS1 RBAC Standards

University of Denver  
Computer Science Colloquium.  
13 Jan 2012

# Table of Contents

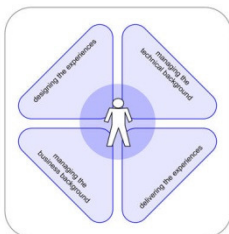
CS1 RBAC - Who

CS1 RBAC - What

CS1 RBAC – Why

CS1 RBAC - How

Use Cases and References



# Info About Tim

- MS Computer Science (Johns Hopkins) - 1990
- Data Processing Professional since 1983
  - Senior [IT Adjective] Engineer
  - Information Assurance Professional (since 1998)
- Implementer of RBAC specifications since 1998
  - NIST
  - INCITS CS1
  - Enterprise Security Management (5-50k users) Implementer
    - Industry Vendor Products (BMC, Beta Systems, IBM)
- IT Security Manager since 2007
  - Booz Allen Hamilton, Federal Agency Contractor (numerous)
  - Raytheon Polar Services
- Author of 3 articles on RBAC standards & 3 ANSI/INCITS standards
- Identity Management Speaker (various conferences)

## **About INCITS**

The InterNational Committee for Information Technology Standards (INCITS) is the forum of choice for developers, producers and users for the creation and maintenance of formal Information and Communication (ICT) technology standards.

INCITS is accredited by, and operate under the rules approved by, the American National Standards Institute (ANSI). These rules are designed to ensure that voluntary standards are developed by the consensus of directly and materially affected interests.

# INCITS – <http://www.incits.org>



## InterNational Committee for Information Technology Standards

Where IT all begins

### Welcome to the InterNational Committee for Information Technology Standards\*

| Search

INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology (Click here to view the INCITS Mission).

Some of these links are password protected (🔒). If you have forgotten your password, please email the staff at [incits@itic.org](mailto:incits@itic.org).

ABOUT INCITS	STANDARDS INFORMATION	NEWS AND EVENTS	INCITS Membership
<ul style="list-style-type: none"> <li>• INCITS Organization</li> <li>• What is INCITS?</li> <li>• INCITS Brochure</li> <li>• Why Participate?</li> <li>• Member Testimonials</li> <li>• INCITS Executive Board Members</li> <li>• Contact Us</li> </ul>	<ul style="list-style-type: none"> <li>• Purchase Standards</li> <li>• Standards</li> <li>• Public Reviews</li> <li>• New Projects</li> <li>• New Published Standards</li> <li>• Publicly Available JTC 1 Standards</li> </ul>	<ul style="list-style-type: none"> <li>• Newsroom: Press Releases</li> <li>• Newsroom: In the News</li> <li>• Best Practices SG Initial Report</li> <li>• Events</li> <li>• Speakers Bureau</li> <li>• Download/Use - INCITS Logo</li> <li>• <b>2008 TC Officers Symposium</b></li> </ul> <p style="text-align: center;">JTC 1 Special Working Group on Accessibility</p>	<ul style="list-style-type: none"> <li>• Obtaining Membership</li> <li>• Online TC Membership Application</li> <li>• Membership Fees</li> <li>• EB Membership Outreach</li> </ul>

# INCITS CS1.1 (2005-2011) was the Role-Based Access Control standards committee under CS1 Cyber Security (<http://cs1.incits.org>)

## INCITS TECHNICAL COMMITTEES


### Languages / Database

- H2 Database
- H3 Computer Graphics & Image Processing
- PL22 Programming Languages

### Media / Education

- L3 Coding of Audio, Picture, Multimedia, and Hypermedia Information
- L8 Metadata
- T3 Open Distributed Processing (ODP)
- V2 Information Technology Access Interfaces
- V36 Information Technology for Learning, Education and Training

### Security / ID

- B10 Identification Cards and Related Devices
- CS1 Cyber Security 
- M1 Biometrics
- T6 Radio Frequency Identification (RFID) Technology

### Storage

- B11 Optical Digital Data Disks
- T10 SCSI Storage Interfaces
- T11 Fibre Channel Interfaces
- 
- T13 ATA Storage Interface

### Information Services / Office / Text

- L1 Geographic Information Systems (GIS)
- L2 Character Sets and Internationalization
- T20 Real Time Locating Systems
- V1 Text Processing: Office and Publishing Systems Interface
- W1 Office Equipment

### INCITS Executive Board Study Groups

- INCITS Study Group on Accessibility
- INCITS Study Group on Security Best Practices 

# NIST RBAC Portal - <http://csrc.nist.gov/rbac>

The screenshot shows a Mozilla Firefox browser window displaying the NIST RBAC Portal. The browser's address bar shows the URL <http://csrc.nist.gov/groups/SNS/rbac/>. The website header includes the NIST logo and the text "National Institute of Standards and Technology Information Technology Laboratory". A search bar labeled "SEARCH CSRC:" is present. Navigation links include "ABOUT", "MISSION", "CONTACT", "STAFF", and "SITE MAP". The main heading reads "Computer Security Division Computer Security Resource Center". A secondary navigation bar lists "CSRC HOME", "GROUPS", "PUBLICATIONS", "DRIVERS", "NEWS & EVENTS", and "ARCHIVE".

The main content area is titled "ROLE BASED ACCESS CONTROL (RBAC) AND ROLE BASED SECURITY". It features a paragraph of introductory text and a list of updates. A light blue arrow points to the first list item: "INCITS RBAC CS1.1 Implementation Standard, ballot resolution meeting held 4/8/08 - new draft in May 08".

On the left side, there is a sidebar menu with the following items:

- Role Based Access Control (selected)
- Current Activities
- Detailed Overview
- Role Engineering & RBAC Standards
- RBAC & Sarbanes-Oxley Compliance
- RBAC Case Studies
- NIST RBAC Patents
- Helpful RBAC Resources
- Contacts
- Frequently Asked Questions (FAQs)

Below the sidebar, there is a section for an "RBAC book" with a cover image and a quote: "A must read." Review from IEEE Computer Society, Security & Privacy. "Overall, this is a great book." Linux Journal. The book is noted as a "2002 Gold Medal for".

# Table of Contents

CS1 RBAC - Who

CS1 RBAC - What

CS1 RBAC – Why

CS1 RBAC - How

Use Cases and References





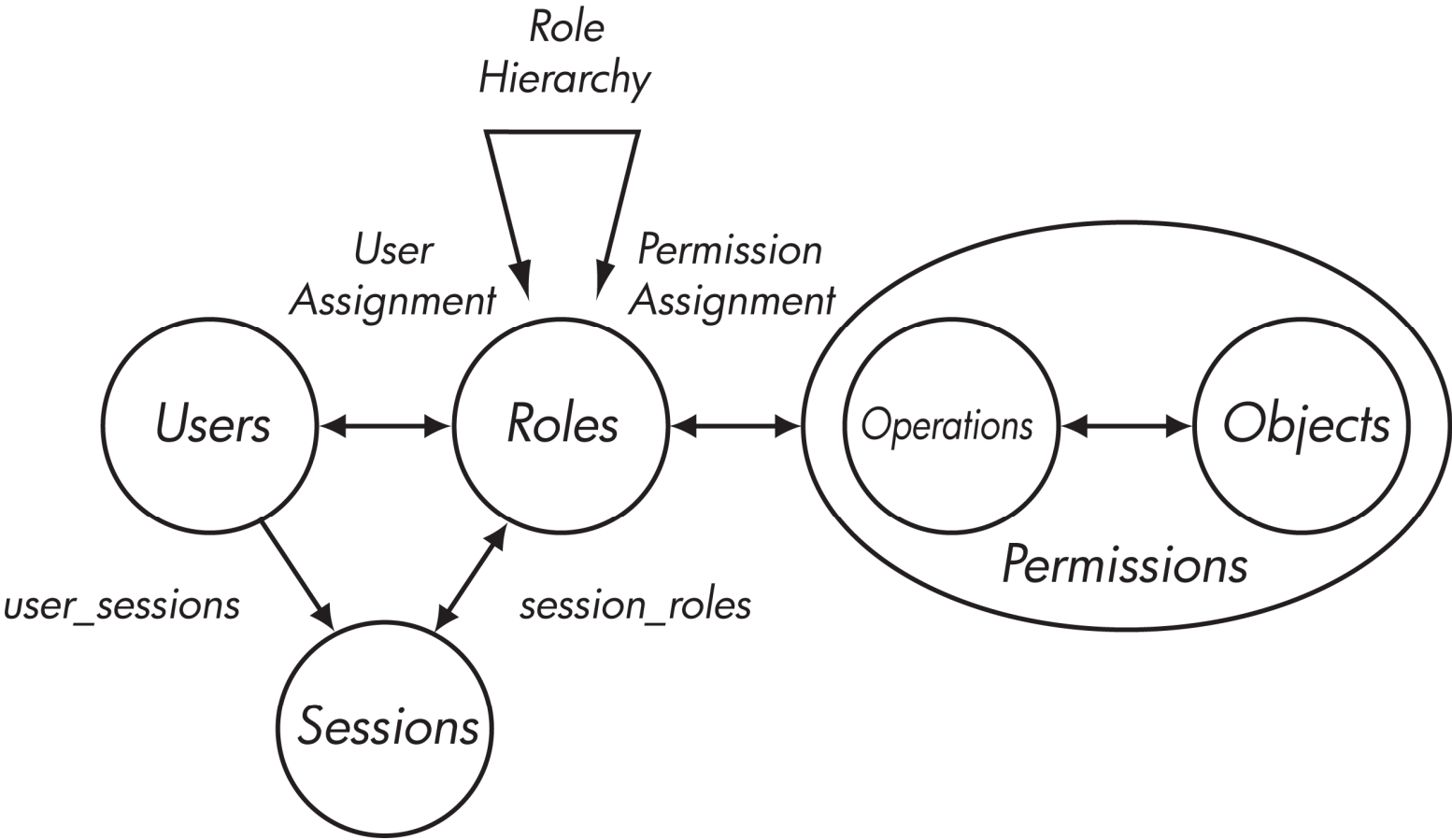
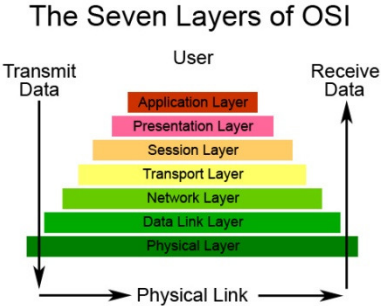
## What do we mean by RBAC?

- Permissions are assigned to roles rather than to individual users
- Users are assigned to roles rather than directly to permissions
- This level of indirection facilitates user-permission management and provides additional security benefits

## Role Definitions

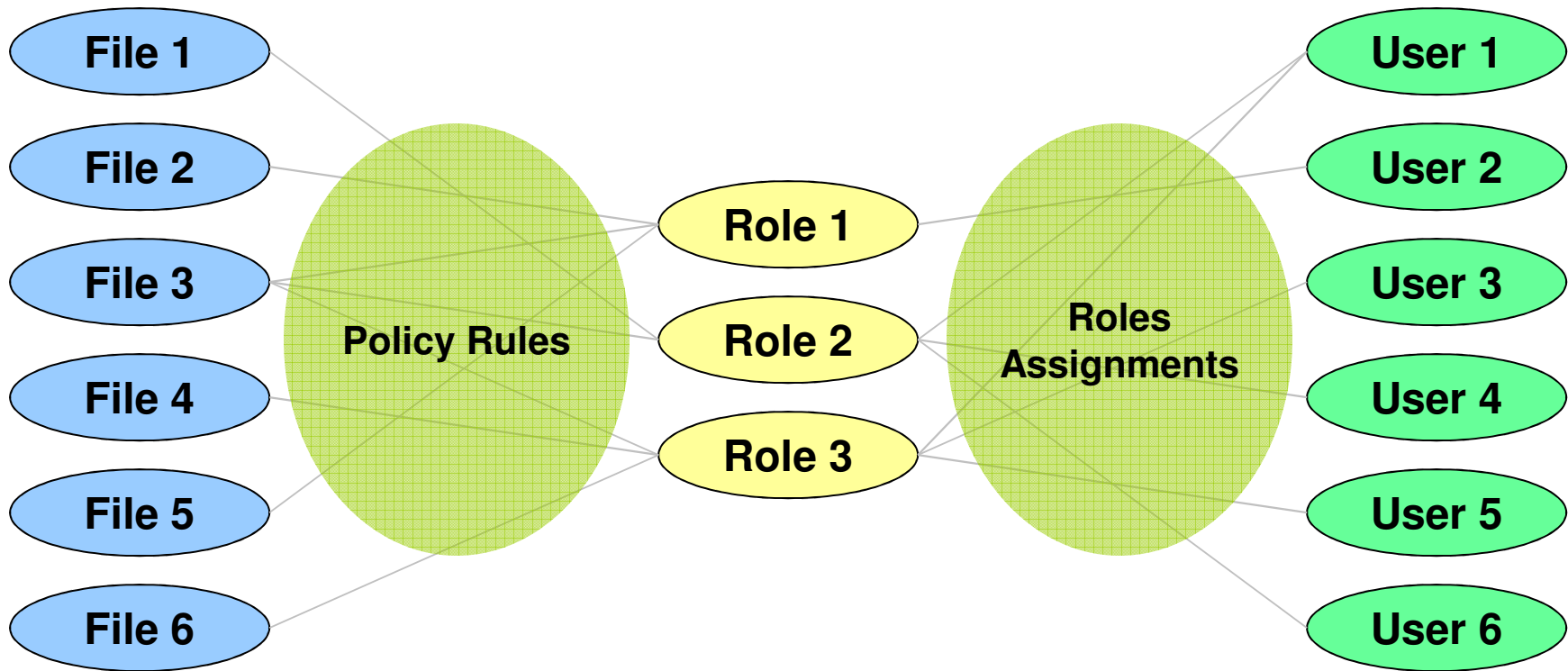
- From the ANSI RBAC standard...
  - A role is a **job function** within the context of an organization, with some associated semantics regarding the authority and responsibility conferred on the subjects to whom the role is assigned
- Roles are often misused to represent things that are not job functions
  - Clearance, Formal access approvals, citizenship
- Role assignments are subject attributes
- Roles are often misinterpreted
  - As entities
  - As a set of privileges

# NIST RBAC Model



# RBAC Privilege Management

- With RBAC, privileges are managed indirectly through roles



# **RBAC Implementation and Interoperability (RIIS) - 2011**

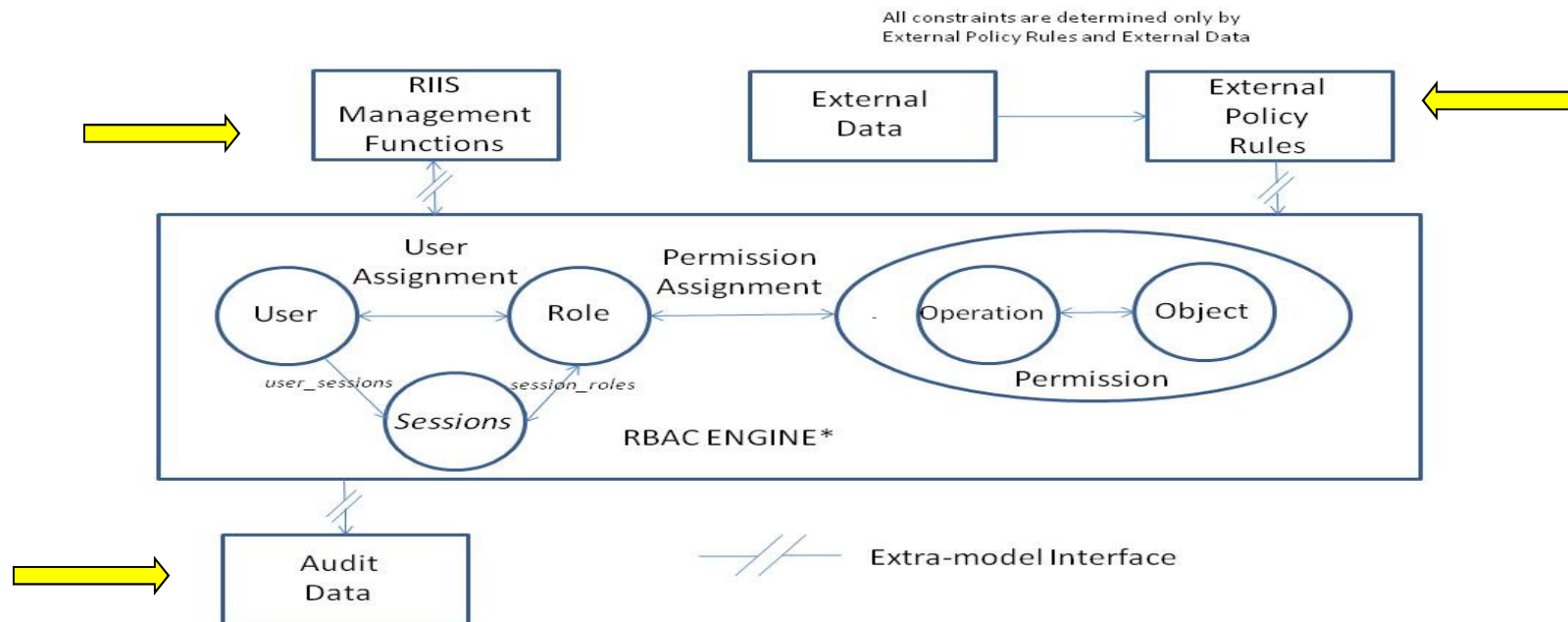
This standard facilitates the Interoperability of RBAC Systems. To meet the need for consistent sets of RBAC components, the RBAC Implementation and Interoperability Standard (RIIS/ ANSI INCITS-459) specifies in greater detail how to design RBAC products to conform to INCITS 359. Published in 2011, this standard can facilitate comparisons among RBAC products, and its interoperability specifications enable translations from one RBAC implementation to another.

## **RBAC Base Standard (ANSI 359-2011) update**

This update to the ANSI 359-2004 standard enhances several RBAC features including granular authorization (support for attributes), real-time policy enforcement, and conformance with the RIIS (ANSI 459-2011) model. In response to comments received over the five-year life of the current RBAC standard (ANSI 359-2004), this enhanced model maintains the advantages of RBAC while providing a mechanism for including attributes in access-control decisions. Publication of this updated standard (RBAC ANSI 359-2011) is expected in 2012.

# RBAC Policy-Enhance Standad (RPE) - 2012

This standard facilitates the use of dynamic constraints with the RBAC model. RBAC Policy-Enhanced standard (RPE provides a framework and functional specifications to handle the relationship between roles and dynamic constraints. The RPE defines the scope and context for role-role, user-role, and attribute sensitive dynamic constraints, which can be implemented in a runtime environment.



\*The RBAC engine controls all access control decisions

The RBAC Policy-Enhanced reference model consists of an RBAC Engine that controls all decisions with interfaces to data and processes external to the RBAC Engine. It contains a representation of core RBAC (INCITS 359) that define its logical components. Core RBAC includes sets of five basic data elements called users (USERS), roles (ROLES), objects (OBS), operations (OPS), and permissions (PRMS). This core RBAC representation includes user assignments, permission assignments, and permissions.

# Table of Contents

CS1 RBAC - Who

CS1 RBAC - What

CS1 RBAC – Why

CS1 RBAC - How

Use Cases and References

# Archie Reed's Secure Identity Management Blog

"Digital ID World Sept 2006: Are NIST Based Roles the Right Answer?"



## Archie Reed's Secure Observations Blog

The focus of this blog is the security space, and identity management in particular. Given time, we will probably take a few off-road expeditions as "shiny things" attract my attention. With the market rapidly evolving this is my take on where we are heading so please, check in, and keep me on my toes.

[Share/Tag this post](#)

» [HP Blogging Code of Conduct](#)

Blog categories: | [All](#)

» [Previous Post](#) » [Next Post](#)

» [Digital ID World Sept 2006: Are NIST Based Roles the Right Answer? #1](#)

Phil and Eric had asked me to sit in on a panel titled "Are NIST Based Roles the Right Answer?" along with Thomas Raeuchle (Prodigen) and Chris Sullivan (Courion). Phil set the premise that he had heard through all his conversations "that in the process of compliance auditing that in the process of auditing compliance data, auditors have come to people and said in order for us to audit the process, instead of auditing the data, [you need] to go role based" and as a result people are getting the order to go role based."

Phil went on to note that "Role based is one of those things that is easy and makes a lot of sense...", however... "[while] it is conceptually simple but it stops right about there, and that actually the process of going to roles tends terrifies those who have done it, and terrifies those who haven't done it even more because they've seen the ones who have done it."

So this was a discussion around why are roles not rolling out like it should?

One issue was that no one wants to roll out something new, so everyone coalesced to the NIST RBAC model. So the question was "Are NIST Based Roles the Right Answer?"



<a href="#">Apr</a>	<a href="#">May 2008</a>					<a href="#">Jun</a>
S	M	T	W	T	F	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

[RSS](#)

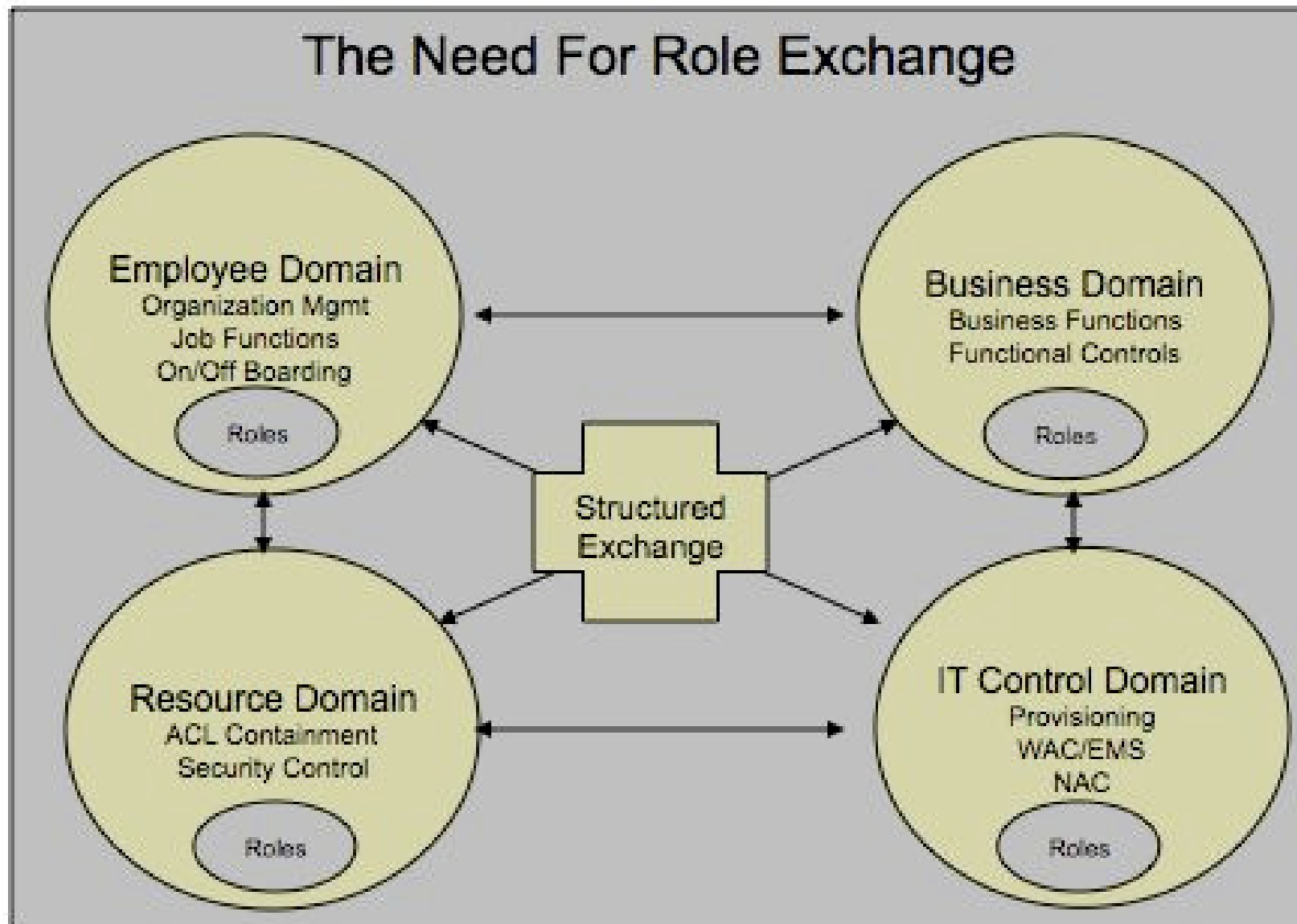
» [HP RSS Feeds](#)

### Recent blog entries

- » [NAC \(Network Access Control\) - Future Directions...](#)
- » [RSA 7-11th Apr - I'll be there, along with the rest of HP's security folks.](#)
- » [NAC \(Network Access Control\) - Some Best Practices #1](#)
- » [NAC \(Network Access Control\) Challenges](#)



# RBAC Interoperability (Enterprise Security Management)





## Health Level 7 (HL7)

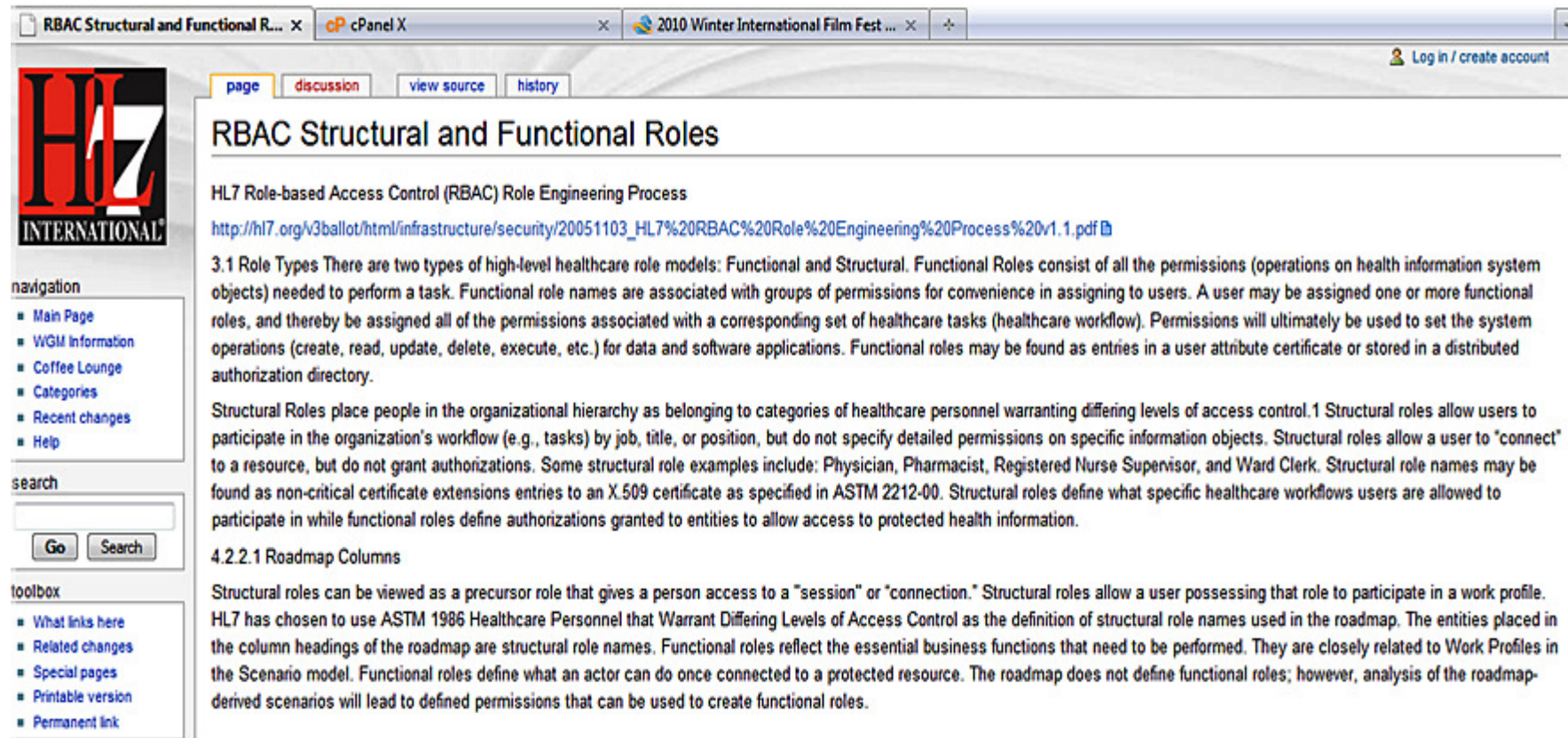
- Healthcare permission catalog
- Healthcare constraint catalog
- Role engineering process
- Evolution from Veterans Administration RBAC Project
  - RBAC Task Group
  - Healthcare Task Group

### HL7 Website

- <http://www.hl7.org>

# HL7 – IT Standards for the Healthcare Community

[http://wiki.hl7.org/index.php?title=RBAC Structural and Functional Roles](http://wiki.hl7.org/index.php?title=RBAC_Structural_and_Functional_Roles)



The screenshot shows a web browser window with three tabs: "RBAC Structural and Functional R...", "cPanel X", and "2010 Winter International Film Fest ...". The page title is "RBAC Structural and Functional Roles". The main content area contains the following text:

HL7 Role-based Access Control (RBAC) Role Engineering Process

[http://hl7.org/v3ballot/html/infrastructure/security/20051103\\_HL7%20RBAC%20Role%20Engineering%20Process%20v1.1.pdf](http://hl7.org/v3ballot/html/infrastructure/security/20051103_HL7%20RBAC%20Role%20Engineering%20Process%20v1.1.pdf)

**3.1 Role Types** There are two types of high-level healthcare role models: Functional and Structural. Functional Roles consist of all the permissions (operations on health information system objects) needed to perform a task. Functional role names are associated with groups of permissions for convenience in assigning to users. A user may be assigned one or more functional roles, and thereby be assigned all of the permissions associated with a corresponding set of healthcare tasks (healthcare workflow). Permissions will ultimately be used to set the system operations (create, read, update, delete, execute, etc.) for data and software applications. Functional roles may be found as entries in a user attribute certificate or stored in a distributed authorization directory.

Structural Roles place people in the organizational hierarchy as belonging to categories of healthcare personnel warranting differing levels of access control. Structural roles allow users to participate in the organization's workflow (e.g., tasks) by job, title, or position, but do not specify detailed permissions on specific information objects. Structural roles allow a user to "connect" to a resource, but do not grant authorizations. Some structural role examples include: Physician, Pharmacist, Registered Nurse Supervisor, and Ward Clerk. Structural role names may be found as non-critical certificate extensions entries to an X.509 certificate as specified in ASTM 2212-00. Structural roles define what specific healthcare workflows users are allowed to participate in while functional roles define authorizations granted to entities to allow access to protected health information.

**4.2.2.1 Roadmap Columns**

Structural roles can be viewed as a precursor role that gives a person access to a "session" or "connection." Structural roles allow a user possessing that role to participate in a work profile. HL7 has chosen to use ASTM 1986 Healthcare Personnel that Warrant Differing Levels of Access Control as the definition of structural role names used in the roadmap. The entities placed in the column headings of the roadmap are structural role names. Functional roles reflect the essential business functions that need to be performed. They are closely related to Work Profiles in the Scenario model. Functional roles define what an actor can do once connected to a protected resource. The roadmap does not define functional roles; however, analysis of the roadmap-derived scenarios will lead to defined permissions that can be used to create functional roles.

The left sidebar contains navigation links: Main Page, WGM Information, Coffee Lounge, Categories, Recent changes, Help. It also has a search box with "Go" and "Search" buttons, and a toolbox with links: What links here, Related changes, Special pages, Printable version, Permanent link.

## **HL7 RBAC Initiatives**

RBAC has a natural fit with many health care applications. Standards are being developed under the HL7 Standards Development Organization. The Department of Veterans Affairs is leading a number of these activities. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates use of RBAC to protect patient information. The HL7 RBAC activities are oriented toward application level systems that are built using the services defined in the general purpose RBAC standards.

# 2010 Economic Analysis of RBAC (RTI NIST Report)

[http://csrc.nist.gov/groups/SNS/rbac/documents/20101219\\_RBAC2\\_Final\\_Report.pdf](http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf)

## Need a way to control network access?

### Government already has it.

---

Role-based authorization has become a standard for protecting large organizations' resources

◦ By William Jackson      ◦ Apr 04, 2011

Role-based access control has saved the U.S. economy more than \$6 billion during the past 16 years, according to a study sponsored by the National Institute of Standards and Technology, and RBAC has become the standard for managing access to IT resources in industry and government.

RBAC was formally proposed by NIST scientists in 1992 and adopted as an industry consensus standard in 2004. A study conducted by RTI International estimated that NIST's work hastened the adoption of the access control scheme and cut development costs, accounting for about \$1 billion of the savings.

"We had no idea where it was going to go," said NIST computer scientist David Ferraiolo, who, along with Rick Kuhn, authored the first formal RBAC model. Now, more than half of all organizations that have more than 500 employees use RBAC for at least some access control, and government agencies routinely use it. "There is no mandate for it," Ferraiolo said. "It is all market driven."

The initial \$2.6 million that NIST spent on RBAC turned out to be a good investment, producing a return of 249 to 1.

# Table of Contents

CS1 RBAC - Who

CS1 RBAC - What

CS1 RBAC – Why

CS1 RBAC - How

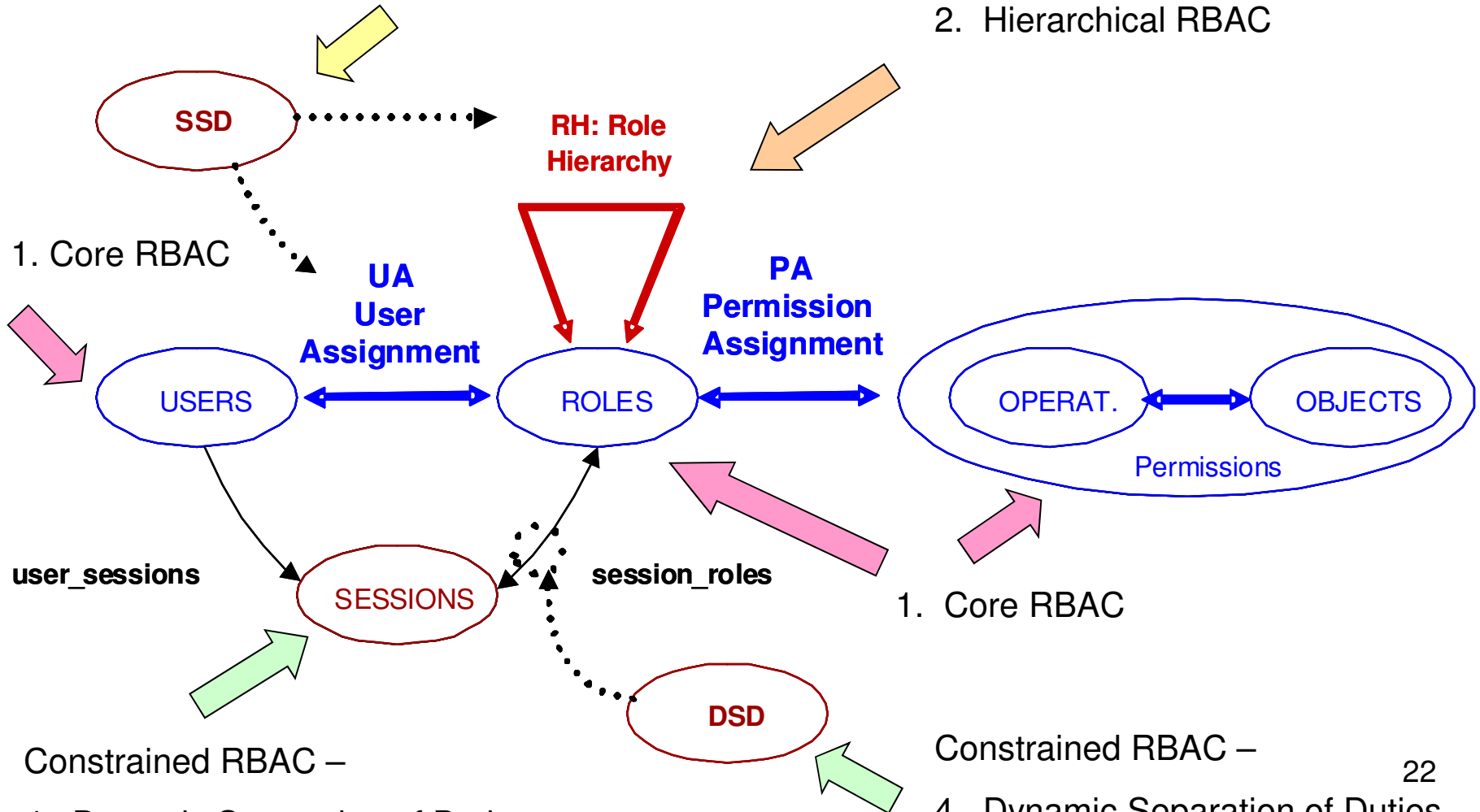
Use Cases and References

# NIST RBAC Model – ANSI INCITS 359 Standard

Constrained RBAC –

3. Static Separation of Duties

2. Hierarchical RBAC



Constrained RBAC –

4. Dynamic Separation of Duties

Constrained RBAC –

4. Dynamic Separation of Duties

# Dynamic Constraints – RBAC Policy-Enhanced Definitions

Dynamic constraints are constraints that take effect at run time. They are distinguished from static constraints, which take effect prior to run time. Dynamic constraints are enforced by access control mechanisms. They act on some components of the RPE Engine namely users and roles. Dynamic constraints are localized to a user session.

## **Role-Role (Dynamic)**

- Role-role constraints hold between roles or sets of roles. They can support policies that involve limitations on which combinations of roles may be activated in any user session.

## **User-Role (Dynamic)**

- User-role constraints hold between users and roles. They can support policies that involve limitations on which combinations of roles may be activated by a given user.

## **Attribute-sensitive (Dynamic)**

Attribute-sensitive constraints apply to roles or permissions. They can support policies that involve limitations on which particular roles may be activated or which permissions may be used in a given user session.

## **Time of Day**

- Time of Day constraints control the time at which a role may be activated.

## **Location**

- Location constraints control the user location at which a role may be activated.

## **Purpose of Use**

- Purpose of use constraints specify a reason for requesting a particular access via a role. Examples include privacy, patient consent, and emergency access.

## **User Class**

- User class constraints control the user class that may exercise a given permission

## **Data Value**

- Data value constraints control an access control decision based on data values, e.g., values in a database.

## **Identity Type**

- Identity type constraints use a business decision-making process to determine what the user's role is.

# CS1 RBAC (RIIS) – Implementation Component Model

Component	Fundamental (F)	Organizational (O)	User Limiting – Universal (ULU)	User Limiting – Operational (ULO)
1. Core RBAC	X	X	X	X
2. Hierarchical RBAC		X		
3. Static Separation of Duty (SSD) Relations			X	
4. Dynamic Separation of Duties (DSD) Relations				X

**Fundamental** refers to core RBAC with no hierarchies or constraints;

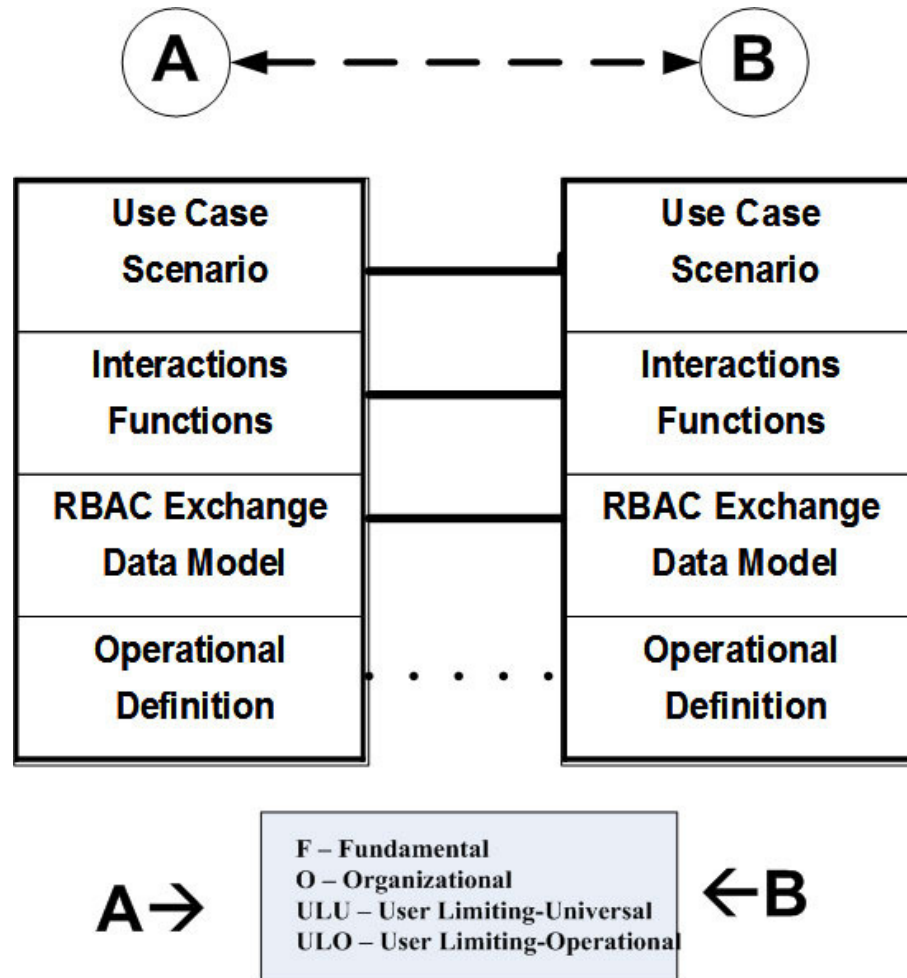
**Organizational** refers to RBAC with role hierarchies,

**User Limiting Universal** refers to RBAC with static constraints

**User Limiting Operational** refers to RBAC with run-time constraints.



# CS1 RIIS Annex –Conceptual Model (Interoperability)



Two Security (or Identity Management) domains are depicted. Within each system, the RIIS interoperability model segments into four areas defined as Use Case Scenarios, Interaction Functions, RBAC Exchange Data Model and Operational Definition

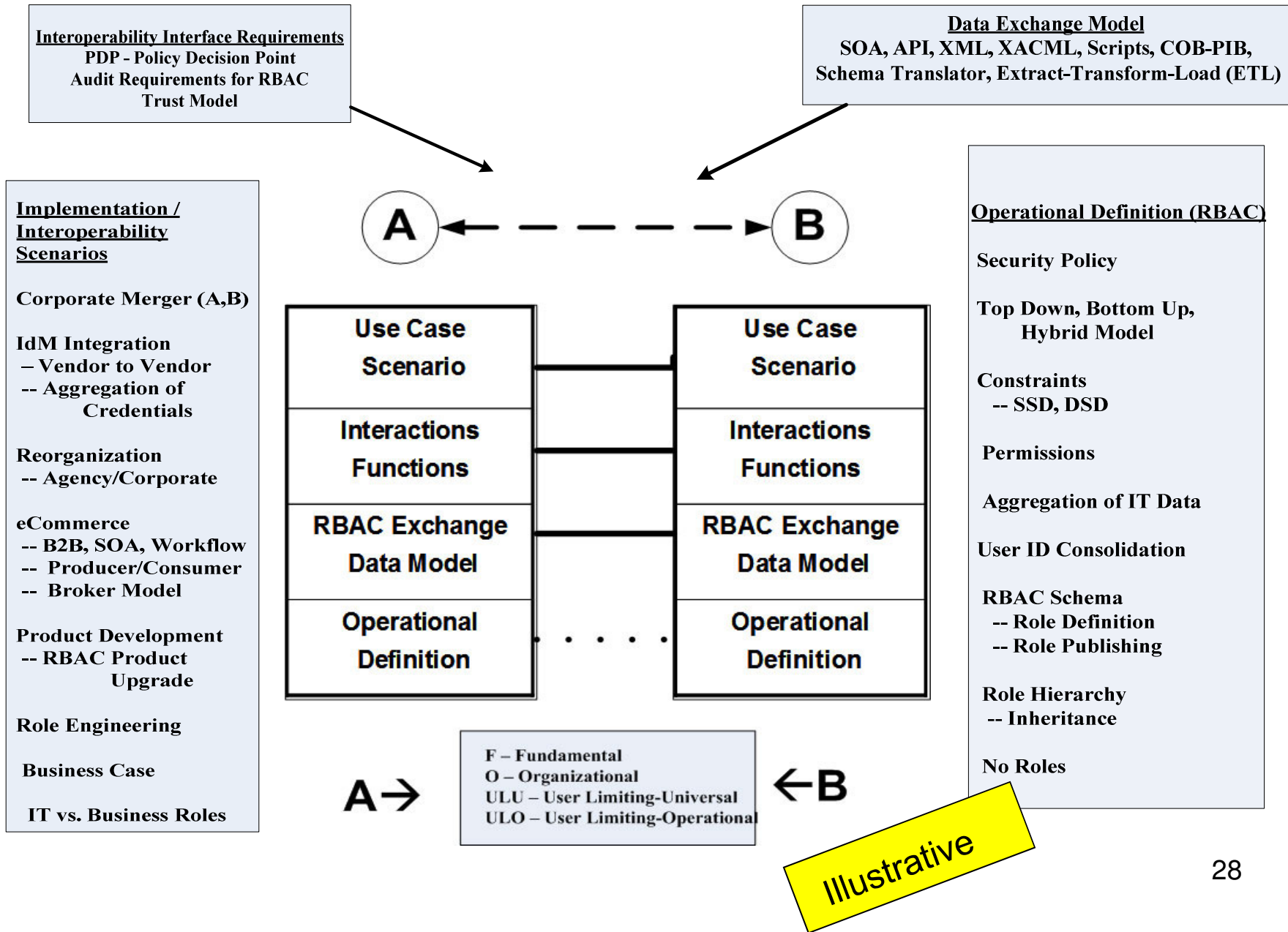
# RBAC Use Case Scenarios and Management Interaction Functions

- **Use Case Scenarios (Business Cases Supporting CS1 RBAC)**
  - Company Mergers
    - Integration of Identity Management (IdM) and Security Domains
    - Exchange of RBAC credentials and entitlements
  - IdM Vendor Product Interoperability
    - Provisioning and Role Management applications
    - Aggregation of cross-platform access rights (initial load)
  - eCommerce
    - B2B, Workflow, Cross-Domain Security for SOA
- **CS1 RIIS Management Interaction Functions**
  - A policy language
  - A request/response language (Get/Post Operations)
  - ***26 operations on roles, users, permissions, constraints and inheritance*** as derived from INCITS ANSI-359 (RBAC standard)
  - Examples
    - PostRoleSet, PostUserSet, GetRolePermissions, GetInheritanceRelationship

## Data Exchange Model (XACML RBAC Interface)

- **XACML**: an XML-based OASIS standard that describes:
  - A policy language
  - A request/response language
  - The main three components in XACML are Rule, Policy, and PolicySet
- **XACML RBAC Profile** is used in ANSI 459-2011 (RIIS) as an *example Data Exchange Model*. **XACML RBAC** profile has two main components:
  - Permission PolicySet (PPS)
  - Role PolicySet (RPS).
  - One PPS and one RPS for each defined Role
- **Permission Policy Set (PPS):**
  - defines Policies and Rules needed to the Permissions associated with a certain Role.
  - PPS references can inherit permissions from the more junior role associated with this PPS reference (hierarchical RBAC)
- **Role Policy Set (RPS):**
  - Defines the Role Name
  - Includes only one PPS to associate this Role with its permissions defined in the corresponding PPS.

# Component Features identified in the RBAC Interoperability Requirements



# Table of Contents

CS1 RBAC - Who

CS1 RBAC - What

CS1 RBAC – Why

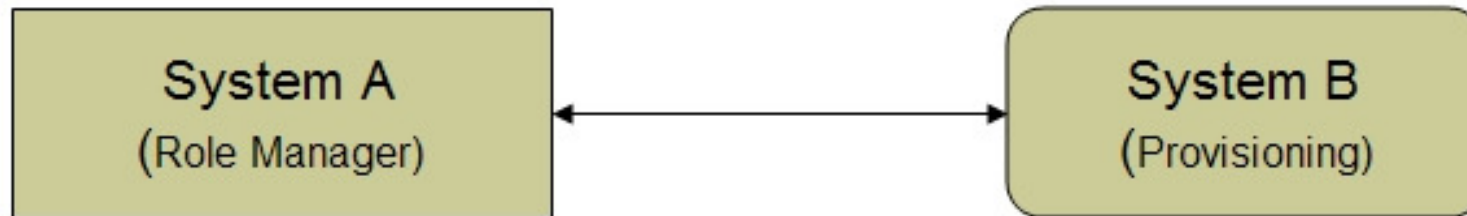
CS1 RBAC - How

Use Cases and References

## Use Case – Continuous Synchronization of External Role Model

### Problem Statement (affecting RBAC)

An enterprise has deployed a Role Management solution (depicted as Systems A) to develop and maintain its role models. As this model changes over time, System A needs to publish these changes out to the operational infrastructure for use and implementation in the user on-board / off-boarding process.



### Scope

One time load (Role Model Provisioning) has occurred

Repeating cycle of synchronization continues in which System A is seen as authoritative over the model used in System B.

### Assumptions

Both systems, denoted System A and System B, are fully RBAC capable.

System A has posed all current configurations to System B and System B is assumed to be in a consistent steady state.

For performance reasons, System A may choose to batch process change notification to System B.

Trust model exists between System A and System B.

System A has a defined Role model and tracks changes make to it in order to relay them to System B

## Use Case – Management Interaction Functions

<b>Interaction Function</b>	<b>Meaning</b>
<b>PostRoleSet</b>	<b>Inform of current set of roles</b>
<b>PostUserSet</b>	<b>Inform of current set of RBAC users</b>
<b>PostUserRoles(user)</b>	<b>Inform of roles currently assigned to a given user</b>
<b>PostUserAssignment(user, role)</b>	<b>Inform of user assignment to a role</b>
<b>PostPermissionAssignment (role,permission)</b>	<b>Inform of permission assignment to a role</b>
<b>PostPermissionSet</b>	<b>Inform of current set of permissions</b>
<b>PostPermissionRoles (permission)</b>	<b>Inform of roles to which a given permission is assigned</b>

## RBAC Data Exchange Model

Extract, Transform and Load (ETL)

Roles Sets, Role Names, User Set, User Assignments,

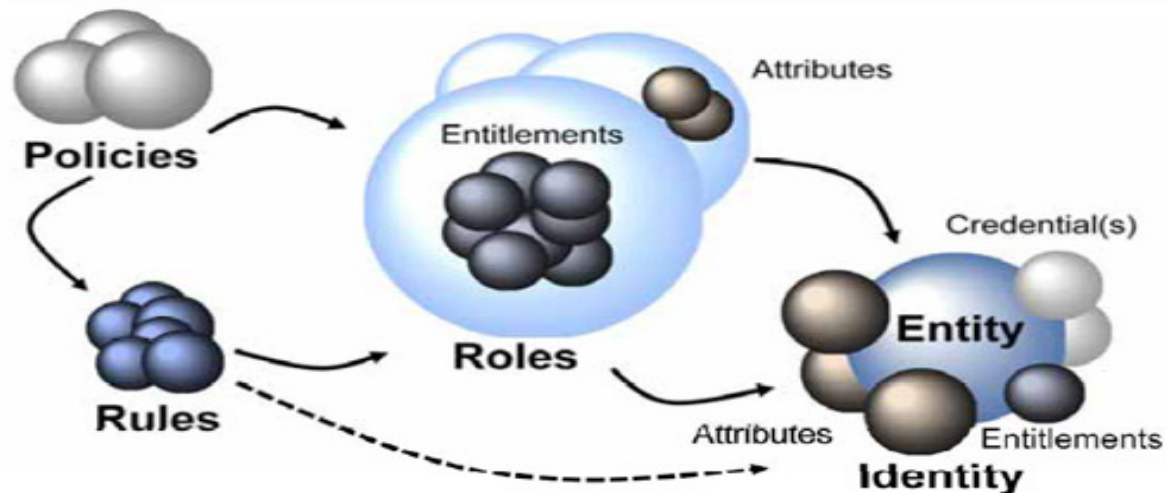
Permission Assignments

# Future Work

- ANSI Publication (359-2011, RPE) standards
- Industry Review (adaptation) of the INCITS RBAC standards
- Software adaptation of the RIIS standard
- Role Engineering Reference Model
- Convergence of xBAC Logical Access Control standards

## The "Atomic Elements" of Identity and Access Governance

---

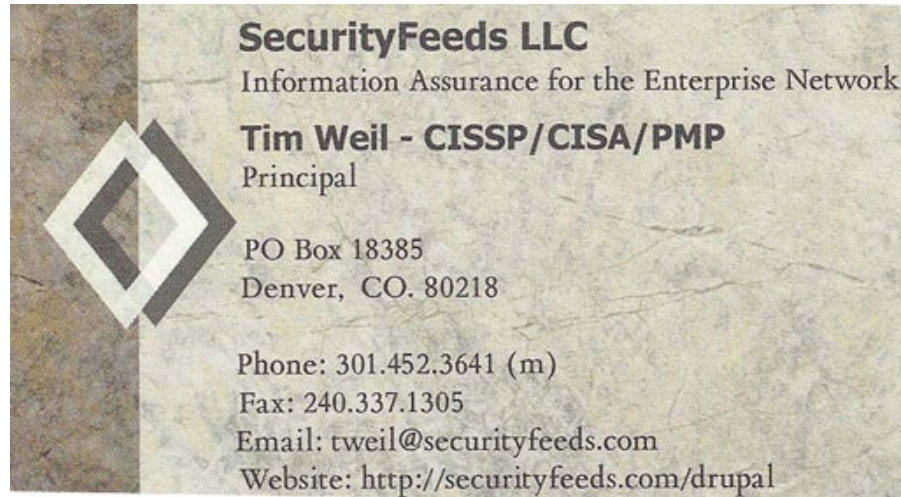


*"The two most common elements in the universe are hydrogen and stupidity." — Harlan Ellison*

**Gartner**



# Thank you for joining us!



- Ed Coyne –
- CS1 RBAC Editor
- HPTI
  - 703-375-2530
  - [ecoyne@hpti.com](mailto:ecoyne@hpti.com)
- INCITS – [incits.org](http://incits.org)

- **Draft Copy of the CS1 (RIIS) Standard**

<http://csrc.ncsl.nist.gov/groups/SNS/rbac/documents/draft-rbac-implementation-std-v01.pdf>

- **Call for CS1 RBAC Use Case Development**

<http://csrc.nist.gov/groups/SNS/rbac/documents/rbac-use-cases.html>

- **How to Join CS1 RBAC Working Group**

<http://csrc.nist.gov/rbac/how-to-join-CS1.1.pdf> or  
contact Lynn Barra at [lbarra@itic.org](mailto:lbarra@itic.org)).



## Questions and Backup Slides



# CS1 RBAC – Management Interaction Functions (1 of 2)

Interaction Function	Meaning	Options
PostRoleSet	Inform of current set of roles	F, O, ULU, ULO
GetRoleSet	Obtain current set of roles	F, O, ULU, ULO
PostRoleName(rolename)	Inform of a new role name	F, O, ULU, ULO
GetRoleName(rolename)	Obtain new role name	F, O, ULU, ULO
PostUserSet	Inform of current set of RBAC users	F, O, ULU, ULO
GetUserSet	Obtain current set of RBAC users	F, O, ULU, ULO
PostRoleUsers(role name)	Inform of users currently assigned to a given role	F, O, ULU, ULO
GetRoleUsers(rolename)	Obtain users currently assigned to a given role	F, O, ULU, ULO
PostUserRoles(user)	Inform of roles currently assigned to a given user	F, O, ULU, ULO
GetUserRoles(user)	Obtain roles currently assigned to a given user	F, O, ULU, ULO
PostUserAssignment(user, role)	Inform of user assignment to a role	F, O, ULU, ULO
GetUserAssignment(user, role)	Obtain user assignment to a role	F, O, ULU, ULO
PostPermissionAssignment (role,permission)	Inform of permission assignment to a role	F, O, ULU, ULO
GetPermissionAssignment (role,permission)	Obtain permission assignment to a role	F, O, ULU, ULO
PostPermissionSet	Inform of current set of permissions	F, O, ULU, ULO
GetPermissionSet	Obtain current set of permissions	F, O, ULU, ULO

# **CS1 RBAC – Management Interaction Functions (2 of 2)**

<b>Interaction Function</b>	<b>Meaning</b>	<b>Options</b>
<b>PostRolePermissions(role)</b>	<b>Inform of permissions currently assigned to a given role</b>	<b>F, O, ULU, ULO</b>
<b>GetRolePermissions(role)</b>	<b>Obtain permissions currently assigned to a given role</b>	<b>F, O, ULU, ULO</b>
<b>PostPermissionRoles (permission)</b>	<b>Inform of roles to which a given permission is assigned</b>	<b>F, O, ULU, ULO</b>
<b>GetPermissionRoles (permission)</b>	<b>Obtain roles to which a given permission is assigned</b>	<b>F, O, ULU, ULO</b>
<b>PostUserAssignmentConstraintStatic (user,role)</b>	<b>Inform of a given user’s static assignment constraint</b>	<b>ULU</b>
<b>GetUserAssignmentConstraintStatic (user,role)</b>	<b>Obtain a given user’s static assignment constraint</b>	<b>ULU</b>
<b>PostUserAssignmentConstraintDynamic (user,role)</b>	<b>Inform of a given user’s dynamic assignment constraint</b>	<b>ULO</b>
<b>GetUserAssignmentConstraintDynamic (user,role)</b>	<b>Obtain a given user’s dynamic assignment constraint</b>	<b>ULO</b>
<b>PostInheritanceRelationship (role,role)</b>	<b>Inform of an inheritance relationship between two given roles</b>	<b>O</b>
<b>GetInheritanceRelationship (role,role)</b>	<b>Obtain an inheritance relationship between two given roles</b>	<b>O</b>

## **CS1 – RBAC Standards and Related Publications**

- ***Role Engineering: Methods and Standards*** - Edward J. Coyne, Timothy R. Weil, D. Richard Kuhn (2011) , IT Professional (Nov/Dec 2011) Vol 13 no. 6 p. 54-57 = Online available [IT Professional \(Nov/Dec 2011\) Vol 13 no. 6](#)
- ***Adding Attributes to Role-Based Access Control***, E. Coyne, R. Kuhn, T. Weil (2010) IEEE Computer (June) 43 (6) p. 3 – Online available [IEEE Computer \(2010\) - Volume 43 Issue 5](#)
- ***ANSI/INCITS 459-2011 - Information Technology - Requirements for the Implementation and Interoperability of Role Based Access Control*** - Edward J. Coyne, D. Richard Kuhn, Timothy R. Weil (2011) p. 27 - Online available - [ANSI/INCITS 459-2011 \(RIIS Standard\)](#)
- ***An RBAC Implementation and Interoperability Standard: The INCITS Cyber Security 1.1 Model*** - Ed Coyne, Tim Weil (2008) IEEE Security and Privacy 6 (1), p. 4 – Online available [IEEE Security & Privacy \(2008\) - Volume 6 Issue 1](#)

## CS1 – RBAC Standards – Citations & Reference Material

In our line of work, they say the number of citations (references) validates the strength of the argument (read technical paper). Our efforts have now been quoted numerous times –

- SANS White Paper– ***Extending Role-Based Access Control***, J. Michael Butler, April, 2011, pg 18 – Online Available – [SANS Analyst Program White Paper](#)
- ***The Privacy and Security Gaps in Health Information Exchanges***, American Health Information Management Association (AHIMA) and Healthcare Information and Management Systems Society (HIMSS), April 2011, pg 31 – Online available - [White Paper by the AHIMA/HIMSS HIE Privacy & Security Joint Work Group](#)
- K.D. Gordon et al., “***Accounting Data Security at JEA Using Role-Based Access Controls***,” University of North Florida, 2011, Online Available [Accounting Security Data at JEA Using RBAC](#)
- National Institute of Standards, Computer Division Computer Security Resource Center, [NIST RBAC Portal](#)
- National Institute of Standards – [RBAC Case Studies](#)

## ABAC vs RBAC vs (xBAC) – The Industry Debate

The Identity Management debates on ‘which access control models’ fit the needs of business and industry is a lively discussion among vendors, analysts and developers of robust Enterprise Security Management solutions –

- Axiomatics – [White Papers on ABAC, XACML, Contrast with RBAC Solutions](#)
- IdmWorks – [The Tie Ins of ABAC, RBAC, RaDAC and SAML](#)
- Identropy – [A Practical Look at Role Management](#)
- Identropy – [A Role Management Primer](#)
- Alan H. Karp, Harry Haury, Michael H. Davis, ***From ABAC to ZBAC: The Evolution of Access Control Models*** HP Laboratories, Online available [HPL-2009-30](#)