Workshop: The Role of Roles in Compliance
A Practical Approach

2008-04-25, 16:00-17:30, Track: Workshop IV

- Dr. Horst Walther, Kuppinger Cole + Partner
- Dr. Ron Rymon, Eurekify
- Dr. Martin Kuhlmann, Omada
- Kevin Cunningham, SailPoint
- Darren Rolls, Sailpoint
- Peter Weierich, Voelcker Informatik
- Melvis Hadzic, Oracle

Forum am Deutschen Museum
Museumsinsel 1 • 80538 München
Phone: +49 89211 25170 • Fax: +49 89211 25165
Web: http://www.forumamdeutschenmuseum.de

The Role of Roles in Compliance

- Enterprise role management is quickly becoming a critical technology for enabling organizations to verify and enforce regulatory policies and to audit the effectiveness of internal controls over user access.
- But due to complexity and marketplace confusion, many companies struggle to find an approach that delivers practical and timely results.
- This workshop is designed to help technical leaders adopt a pragmatic strategy for managing roles as part of a successful governance, risk management, and compliance initiative.
- SailPoint's Chief Technology Officer, Darran Rolls, will provide an in-depth look at role management concepts and technologies.
- And, he'll offer recommendations that can help organizations achieve practical benefits with roles. Points of discussion include:
  - Introduction: What is role management?
  - Business drivers and use cases for role management
  - Where do roles fit in the world of compliance?
  - How do compliance roles relate to provisioning roles?
  - How useful is the NIST RBAC model?
  - Real-world deployment issues:
  - Engaging the business user in the process
  - Achieving flexibility, usability, and ease of deployment
  - Role model interoperability
  - Future directions for role concepts and technologies
- Workshop participants will gain the theoretical and practical knowledge they need to develop clear action plans for tackling role management in their organizations and to determine the most appropriate approach for the needs of their identity infrastructure and compliance objectives.

agenda

- Introduction: What is role management?
- Business drivers and use cases for role management
- Where do roles fit in the world of compliance?
- How do compliance roles relate to provisioning roles?
- How useful is the NIST RBAC model?
- Real-world deployment issues:
- Engaging the business user in the process
- Achieving flexibility, usability, and ease of deployment
- Role model interoperability
- Future directions for role concepts and technologies

Introduction

What is role management?

- Role management & compliance
- Dimensions – not only Roles
- How to find roles
- Where crafting roles is worthwhile
- Centrally or locally

Role Management & compliance

two arbitrary examples

- Segregation of Duties
  - ISO17799 10.1.3
  - COBIT 4.0 PO4.11
- Access control
  - ISO17799 11.5
  - COBIT 4.0 AI2.3

Segregation of Duties

Compliance requirements to role management

- ISO17799 10.1.3
  - Segregation of duties is a method for reducing the risk of accidental or deliberate **system misuse**.
  - Care should be taken that no single person can access, modify or use assets without **authorization** or **detection**.
  - The initiation of an event should be **separated** from its authorization.
  - The possibility of **collision** should be considered in designing the controls.
- COBIT 4.0 PO4.11
  - Implement a **division of roles and responsibilities** that reduces the possibility for a single individual to subvert a critical process.
  - Management also makes sure that personnel are performing **only authorised** duties relevant to their respective jobs and positions.

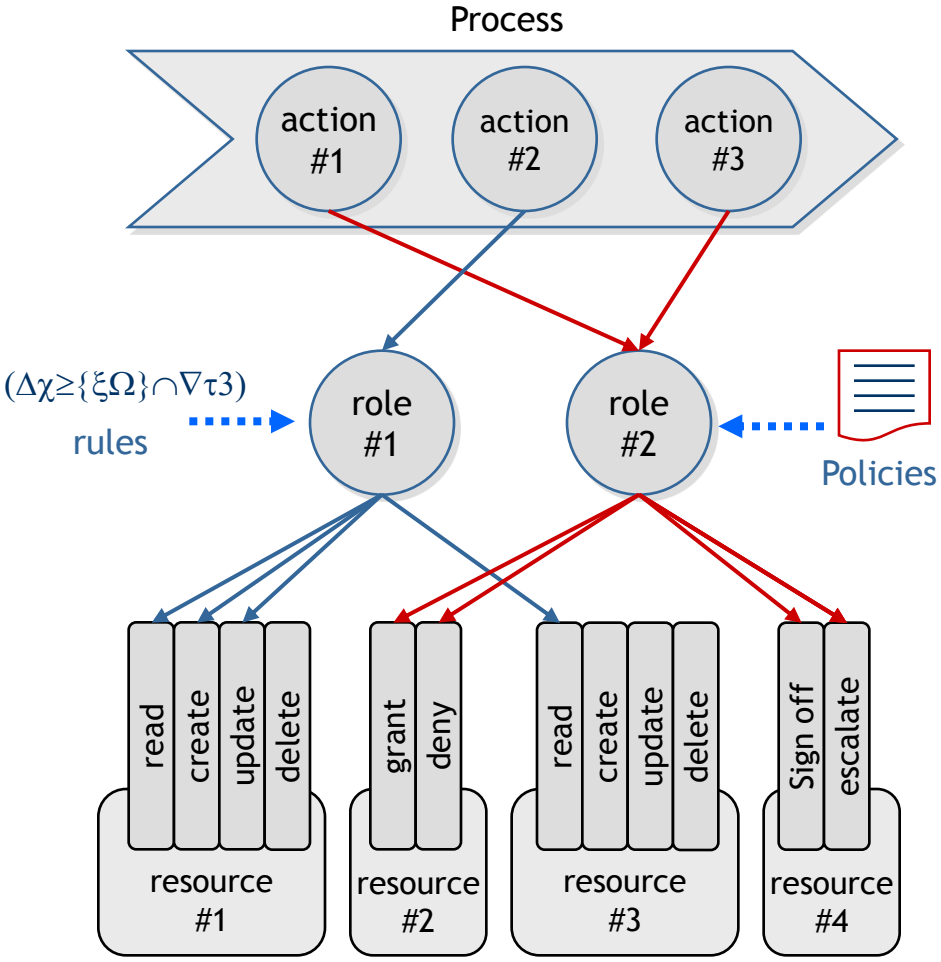
Access control

Compliance requirements to role management

- ISO17799 11.5
  - Access to information, information processing facilities, and business processes **should be controlled** on the basis of business and security requirements [...]
  - The use of utility programs that might be capable of overriding system and application controls **should be restricted** and tightly controlled.
- COBIT 4.0 AI2.3
  - Ensure that business controls are **properly translated** into application controls such that processing is accurate, complete, timely, authorised and auditable.
  - **Issues to consider** especially are authorisation mechanisms, information integrity, access control, backup and design of audit trails.

Processes – roles – rules

they define the organisation



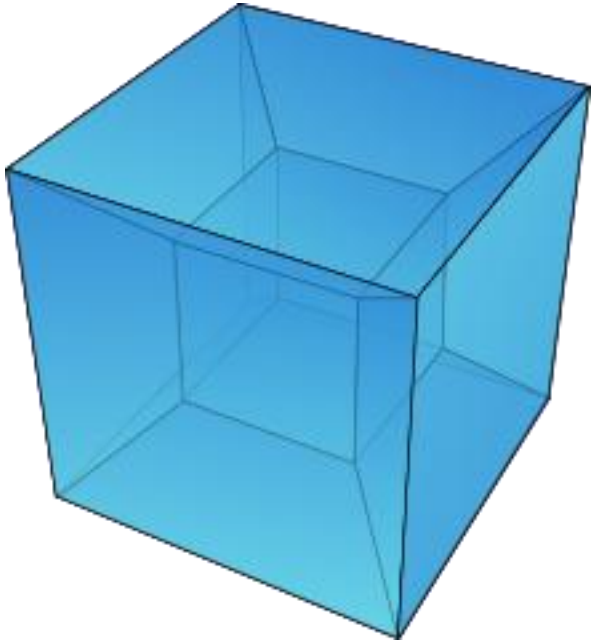
Top-down Modelling

- The operations of organisations can be best described by its business processes.
- Processes consist of elementary actions: one person at a time and a location.
- Actions are performed by roles.
- To be able to do this they need access to resources.
- Processes and roles can't be modelled independently.

The dimensions of privilege assignment

access privileges are not only determined by roles

Dimensions, that determine the privilege …



Tessaract or hypercube: 4-dimensional cube

hierarchy	typically the superior has higher privileges than the subordinate.
function	the business function in a corporation – the sum of its Roles.
location	access rights often depend from the location.
structure	organisational units (OU) differentiate the access rights too,
Cost centre	cost centres often don't match organisational units.
Contract type	Due to common practice employees, contractual staff, consultants, temporary workers are assigned different privileges.

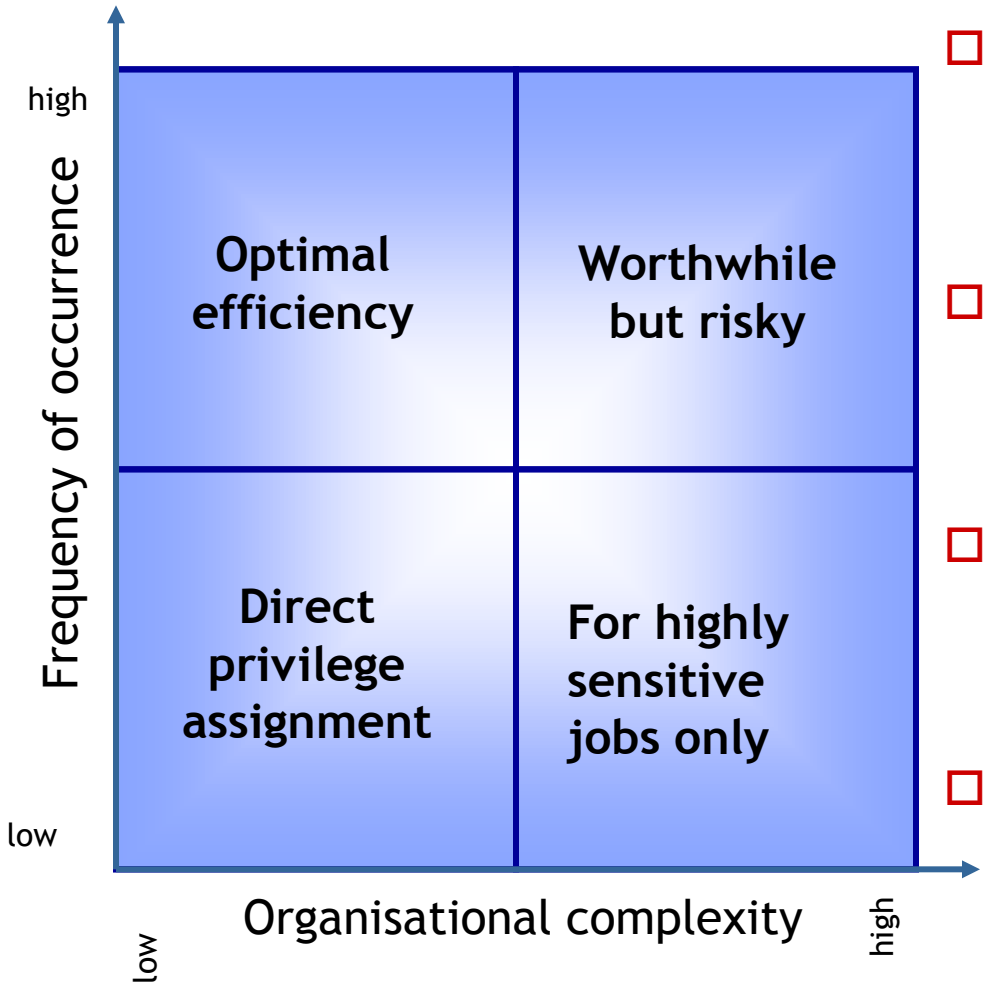
How to find roles

➔ Role finding requires good knowledge of the business domain, some experience in related business modelling areas and a sound portion of intuition.

Watch out for …

- **User categories**
  - User types: employees, partners, suppliers, customers, and investors.
- **Jobs**
  - Employee jobs (Director, Manager, Supervisor, Accountant, Sales Representative, Researcher, Designer, and so on)
- **Job functions**
  - Business operations: Sales Representative submits orders, views orders for the district, manages customer complaints, and accesses the company intranet.
- **Aggregate job functions**
  - All Employees use the company intranet; all sales personnel can view order status.
- **Job tasks**
  - Two tasks for using the company intranet : view intranet and print intranet pages

Where roles promise optimal results?

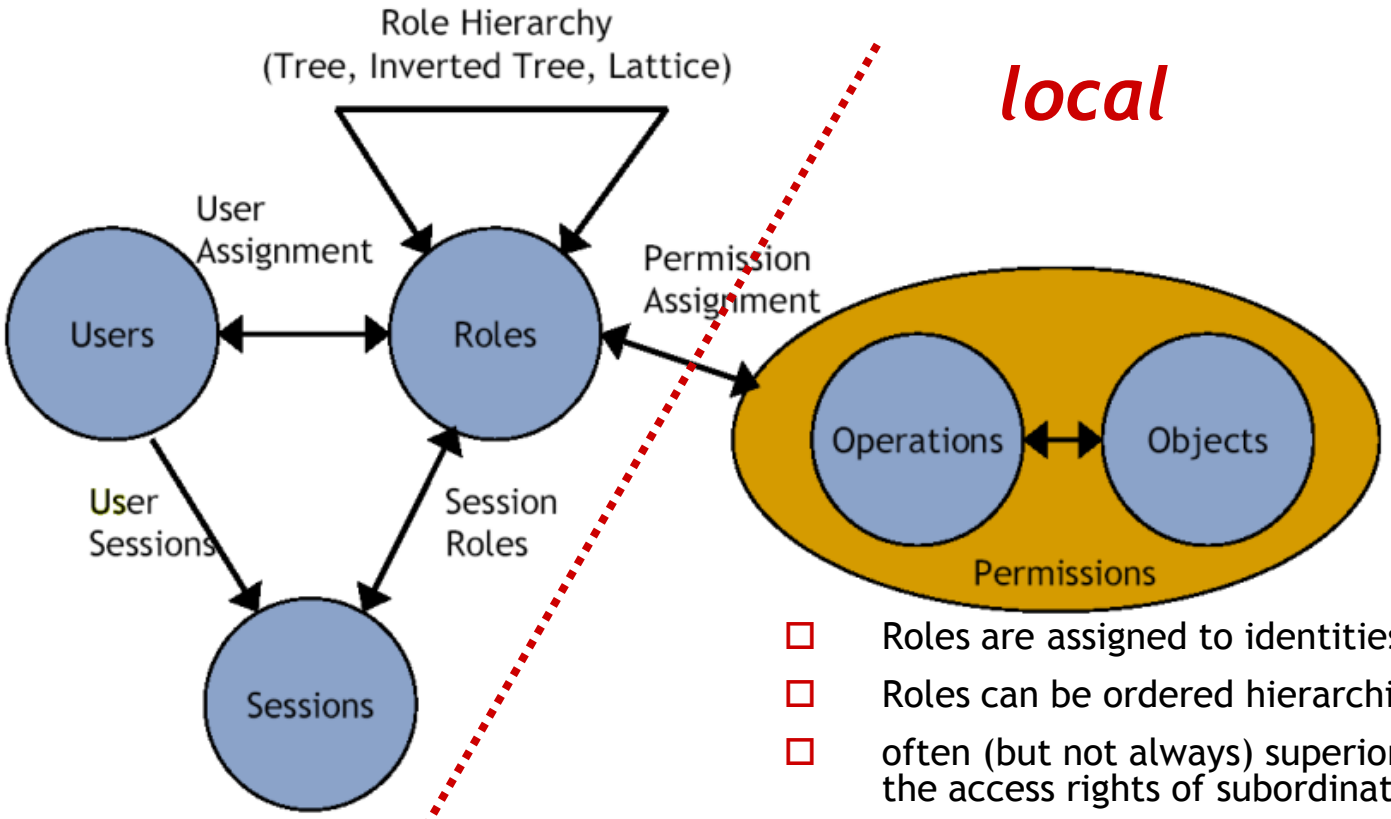


- High frequency – low complexity
  - Optimal efficiency
  - Roles were invented for this.
  - Start here
- Low frequency – low complexity
  - Direct privilege assignment
  - Role engineering is not worth the effort.
- High frequency – high complexity
  - Worthwhile but risky
  - Continue here if the conditions are promising.
- Low frequency – high complexity
  - For highly sensitive jobs only
  - You must have good reasons to do role engineering here.

➔ expect optimal results at high number of jobs with low complexity.

central or local

IDs & Roles have central, access rights local focus.



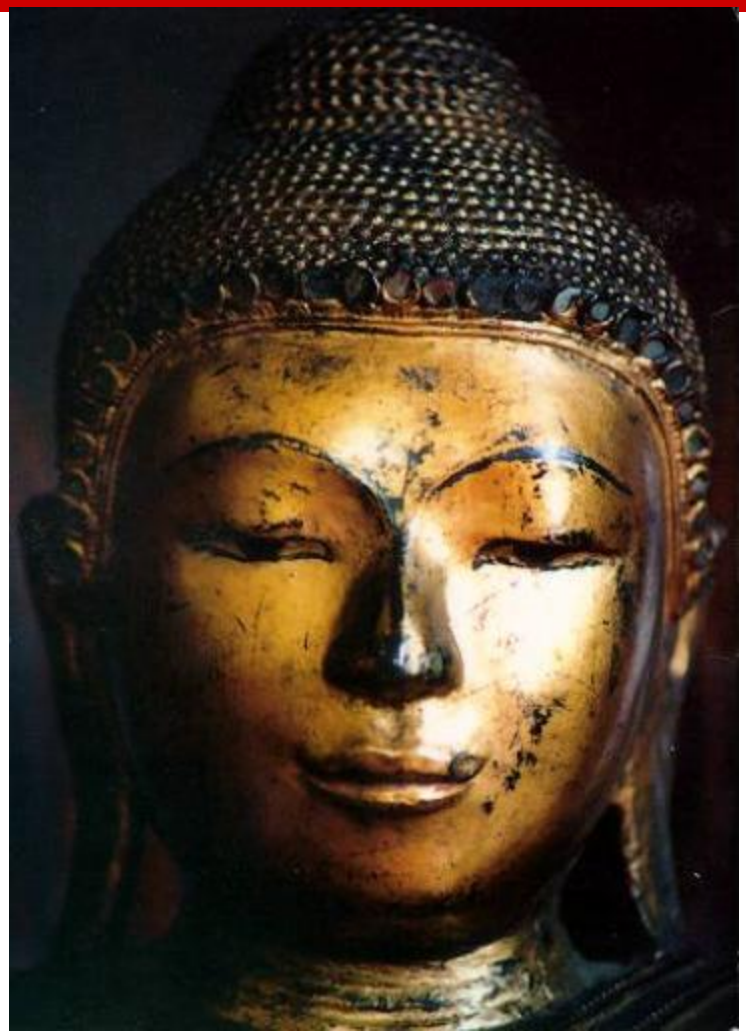
local

central

- Roles are assigned to identities
- Roles can be ordered hierarchically.
- often (but not always) superior roles have all the access rights of subordinate roles
- permissions are operations on objects.
- permissions can be assigned or denied additionally.
- Roles may be valid for a session (temporarily).

Source: Ferraiolo, Sundhu, Gavrila: A Proposed Stundard für Role-Based Access Control, 2000.

Best practise advice



- A combination of **Roles** and **Rules** balances best the desired goals with the capabilities of the systems.
- Not all business areas are **equally well** suited for role engineering.
- **Frequently** occurring functions with low or medium complexity give best result to effort ratios.
- They are found **at the lower end** of the traditional enterprise pyramid.
- **Operational functions** are a good starting point for role engineering.
- The nearer the role engineer comes to the **headquarters** and the more he **moves up** the corporate hierarchy the more difficult his task becomes.
- Role engineering processes are **no real time processes**.
- Role engineering can lead to **fatal bottlenecks**.

- ➔ We have to face the brutal truth, that business modelling is not an easy task and may offer various pitfalls on its envisioned pathway to success.

Questions - comments – suggestions?

Questions to the audience

please answer the following questions

- Does your company have compliance work to do?
  - Which regulations do you have to be compliant with?
  - Which of them are liked to role management
- Has your company implemented a role management?
  - Full coverage or restricted to some business areas?
  - Do you feel that role management helps getting compliant?
- Do you feel, that we have the right methods & tools at hand?
  - For doing an effective role management
  - For becoming compliant – but efficiently?

Attention
Appendix

From here the notorious back-up slides follow ...

What are Roles – Origin

- The idea of cross-platform user administration goes back to the **late eighties**.
- Software companies saw the need to maintain users and privileges **on corporate level** across all of their systems in one step.
- At about the same time US-researchers worked on **RBAC**.
- **Roles** are an ordering scheme, which originates from the organisation theory.
- In the middle of the nineties 1st **tools** appeared.
- At the same time, **NIST** research provided the first formal role models.

➔ Adoption of RABC was surprisingly slow and suffered set-backs.

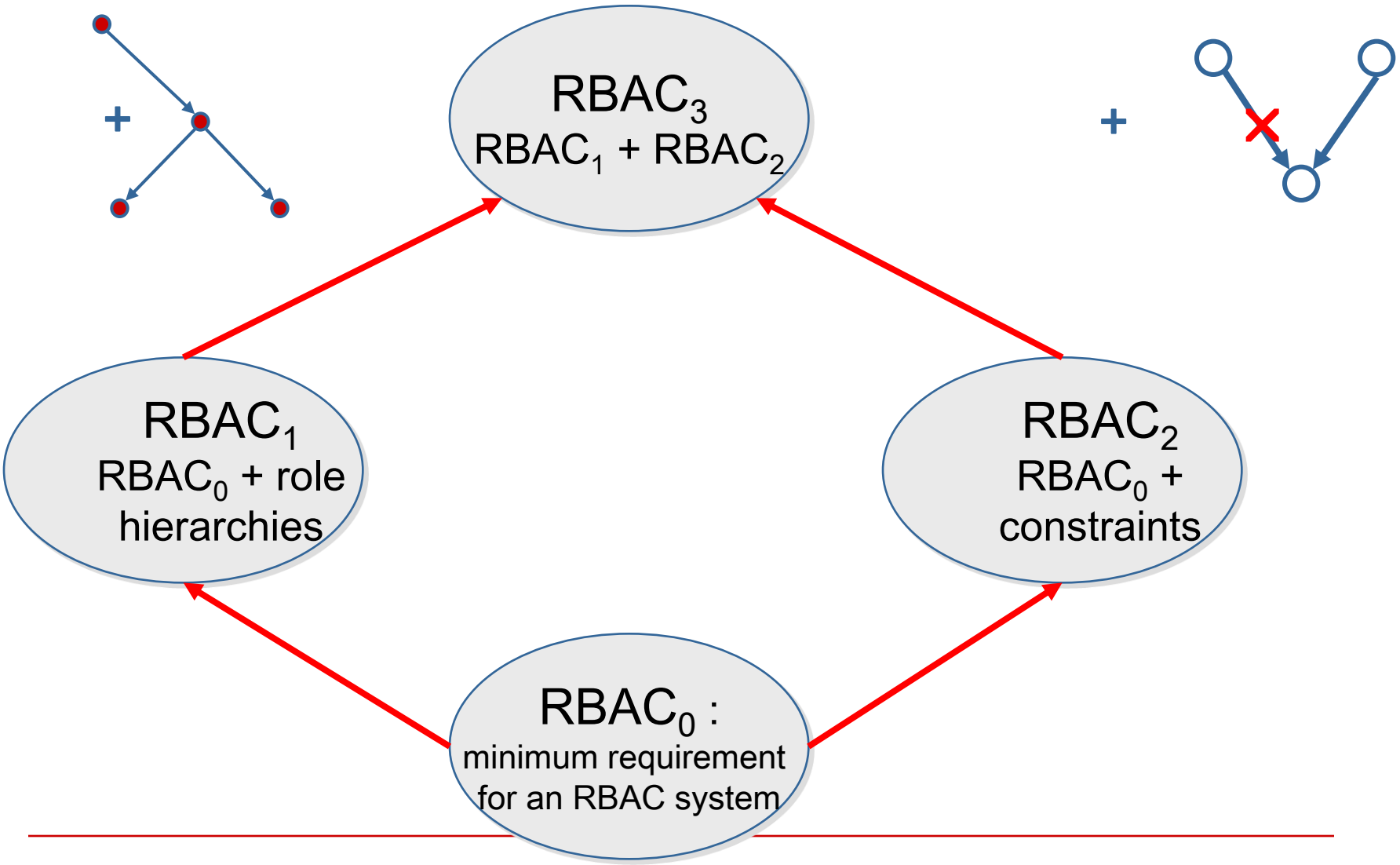
Roles & related Concepts

Often confused:

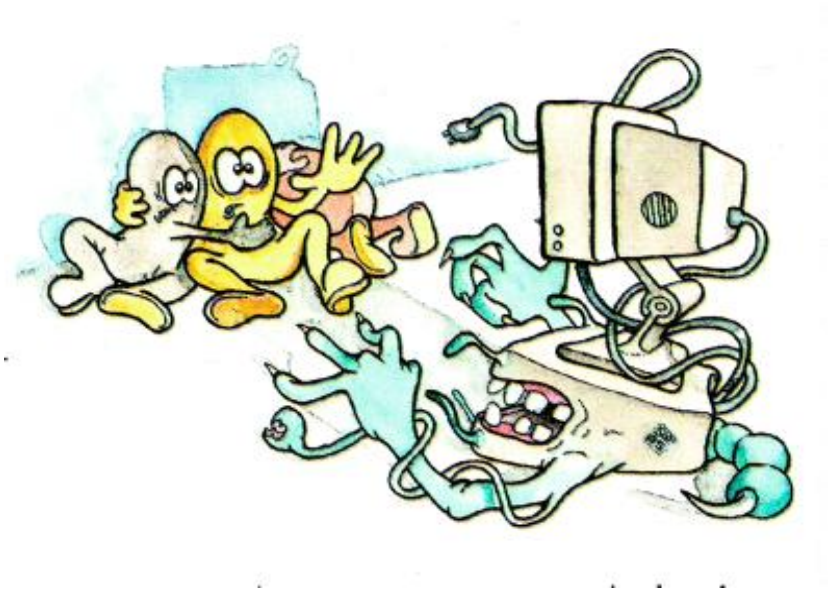
- **roles**, **rules** and **groups**.
- NIST: roles can be understood as **groupings of cross system privileges** on enterprise level.
- "groups" are "groupings of users".
- More **confusion**:
  - Some vendors implement roles through dynamic groups.
  - Plus they maintain user groups.
- Both are **statically** usable constructs.
- Rules unfold their power when interpreted **at runtime** only.
- Rules are **general expressions** using symbolic variables and Boolean or even arithmetic operators.
- The may be **nested**.

➔ All three concepts may be used independently but to achieve optimal modelling results it is recommended to combine them in balanced way.

RBAC – The NIST Standard



Security Policies



- RBAC is policy free.
- It can be used to express policies.
- Four of the most commonly known policies.
  - Least Privilege Principle
  - Separation of Duties
  - Discretionary Access Control
  - Mandatory Access Control

➔ Some basic policies can be expressed in RBAC directly – others through the use of rules.

Least Privilege Principle

limitation

- The principle of least privilege is important for meeting **integrity objectives**.
- It requires that a user be given only the **privilege necessary** to perform a job.
- It requires …
  - **identifying** the user's function,
  - **determining** the minimum set of privileges necessary, and
  - **restricting** the user to a set of roles with only those privileges.
- By excluding users from transactions that are unnecessary for the performance of their duties, those transactions cannot be used to circumvent organizational security policy.
- With RBAC, enforced minimum privilege is easily achieved.

➔ The principle of least privilege is the leading principle in RBAC.

Separation of Duties

- ➔ **Static** separation of duty enforces the mutual exclusion rule at the time of role definition.
- ➔ **Dynamic** separation of duty enforces the rule at the time roles are selected for execution by a user.

- Separation of duties (SoD) is an **organizational policy**.
- In a particular sets of transactions, **no single role be** allowed to execute all transactions within the set.
- Used to **avoid fraud**.
- For example:
  - **separate transactions** are needed to initiate a payment and to authorize a payment.
  - **No single role** should be capable of executing both transactions.
  - A branch manager's permission is qualified by an affiliation to a particular branch. Thereby conferring branch manager permission within that branch.
- Two forms of SoD exist:
  - **static** (SSD) and **dynamic** (DSD).

Barings Bank – an Example

- 1995 the Barings-Bank was acquired by the Dutch ING-Group for **one pound.**
- The **Bank of the British kings** has been one of the noblest in London since 1762 .
- Until 1992 Nick Leeson in Singapore started **exploiting price differences** between Japanese Derivates.
- The resulting loss mounted up to **1,4 Billion** Dollar.
- Leeson was convicted of fraud and sentenced to **6 ½ years** in Singapore's Changi prison.
- Leeson was responsible for trading derivates in Singapore **and** for the Back-Office where the Trades were settled.

  - A **catastrophic mix!**

➔ A role based separation of duties would have cost less.

MAC - mandatory access control

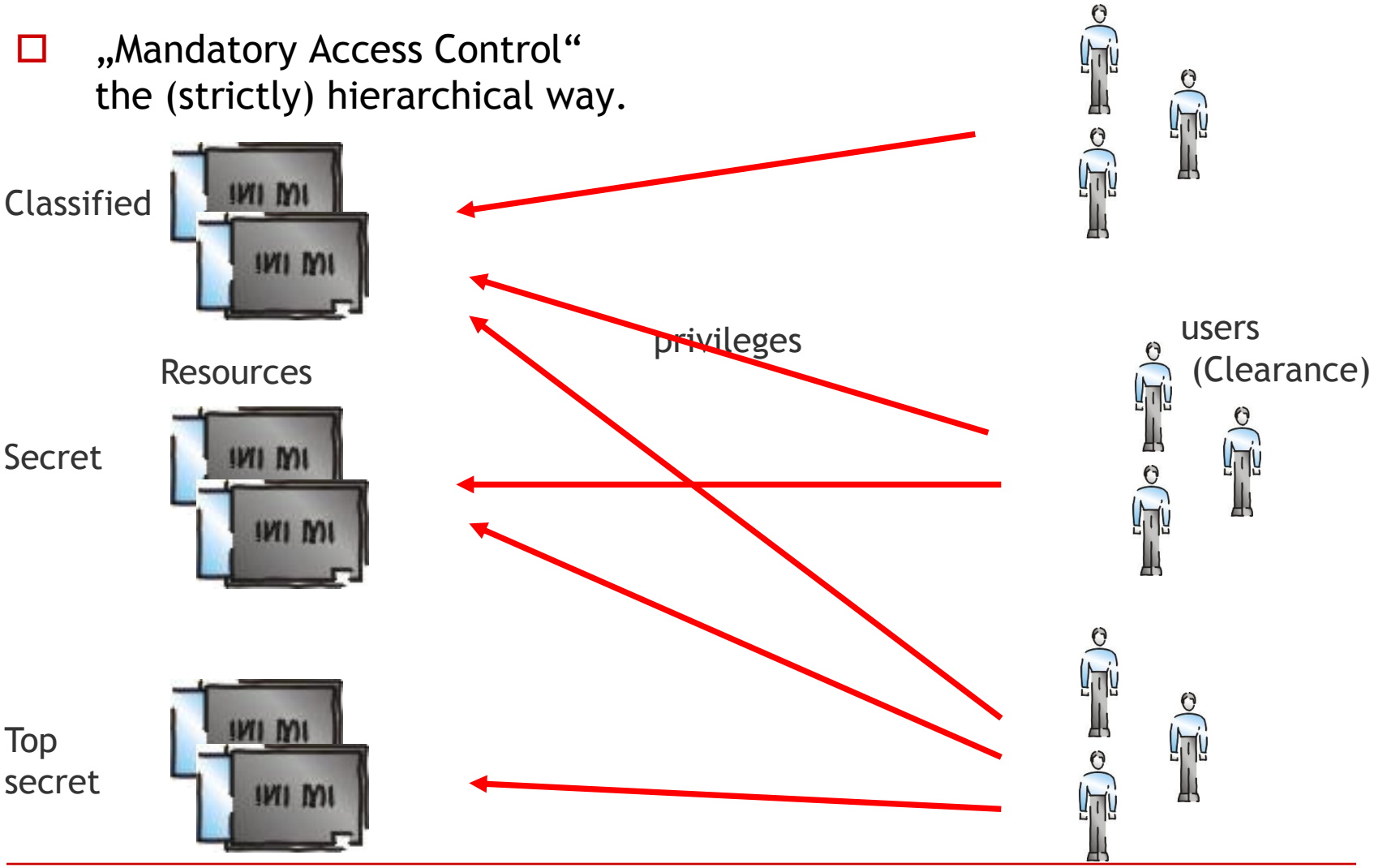
- An access policy
  - Supported for systems processing especially sensitive data
- All access decisions are made by the system
- Each subject and object has a sensitivity label
  - Example: confidential, secret, top secret
  - A user's sensitivity label specifies the sensitivity level, or the level of trust, associated with that user
  - A file's sensitivity label specifies the level of trust that a user must have to be able to access that file
- Read down and write up
  - To read, the subject's sensitivity level must dominate the object's sensitivity level
  - To write, the object's sensitivity level must dominate the subject's sensitivity level

➔ **MAC's** focus is to keep information secret. It relies on a strict hierarchy. It is not appropriate for commercial organisations.

MAC

Types of access control schemes

- „Mandatory Access Control“
  the (strictly) hierarchical way.



DAC - discretionary access control

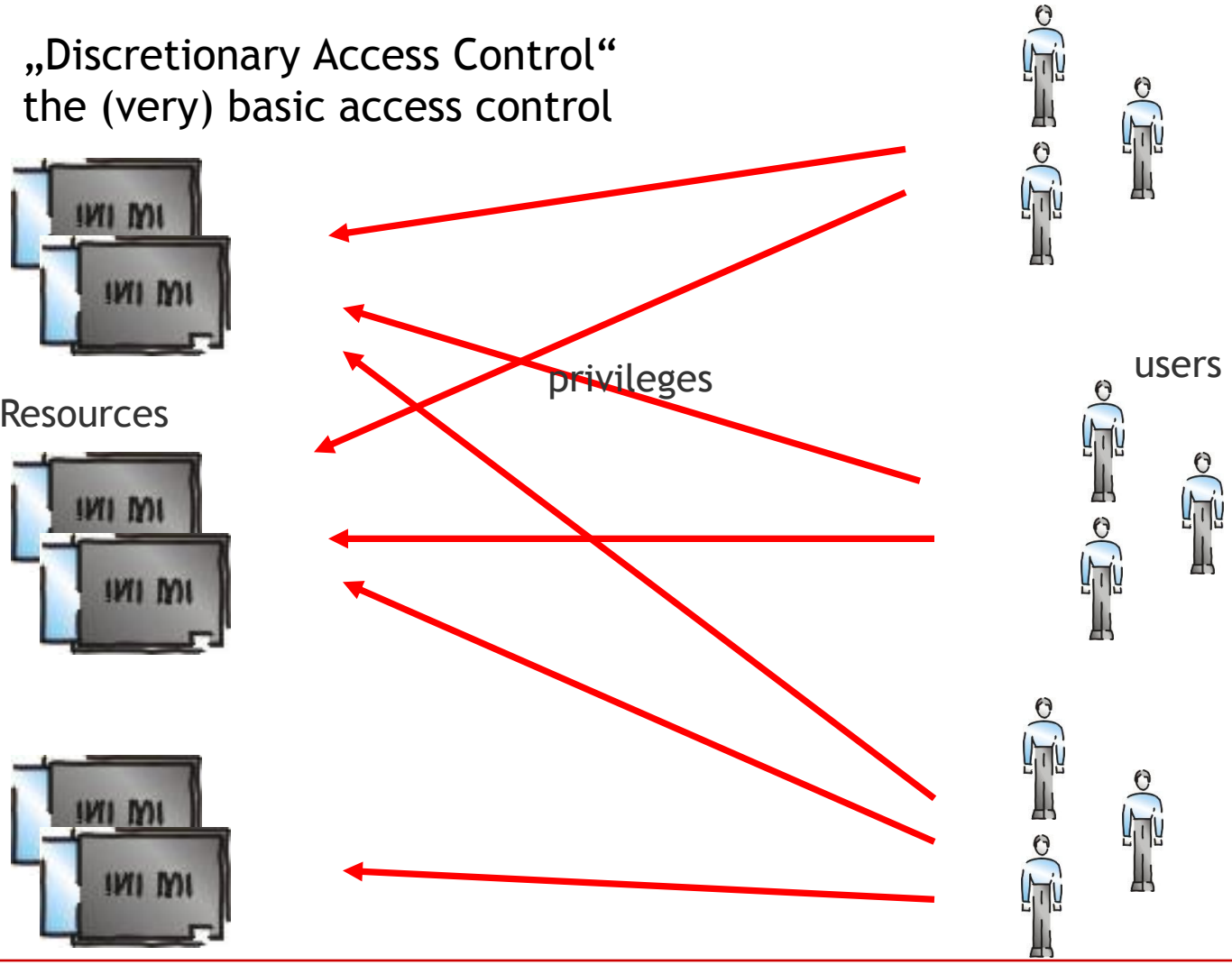
- An access policy
  - Restricts access to files and other system objects based on the identity of users and /or the group to which they belong
- At your own discretion
  - Not only does DAC let you tell the system who can access your data, it lets you specify the type of access allowed
- Types of DAC
  - A simple method: ownership
  - Access Control Lists (ACLs): a flexible way of providing discretionary access control

➔ **DAC** may be considered as a very basic policy, only suitable for isolated non-critical systems with few users only.

DAC

Types of access control schemes

- „Discretionary Access Control“
  the (very) basic access control

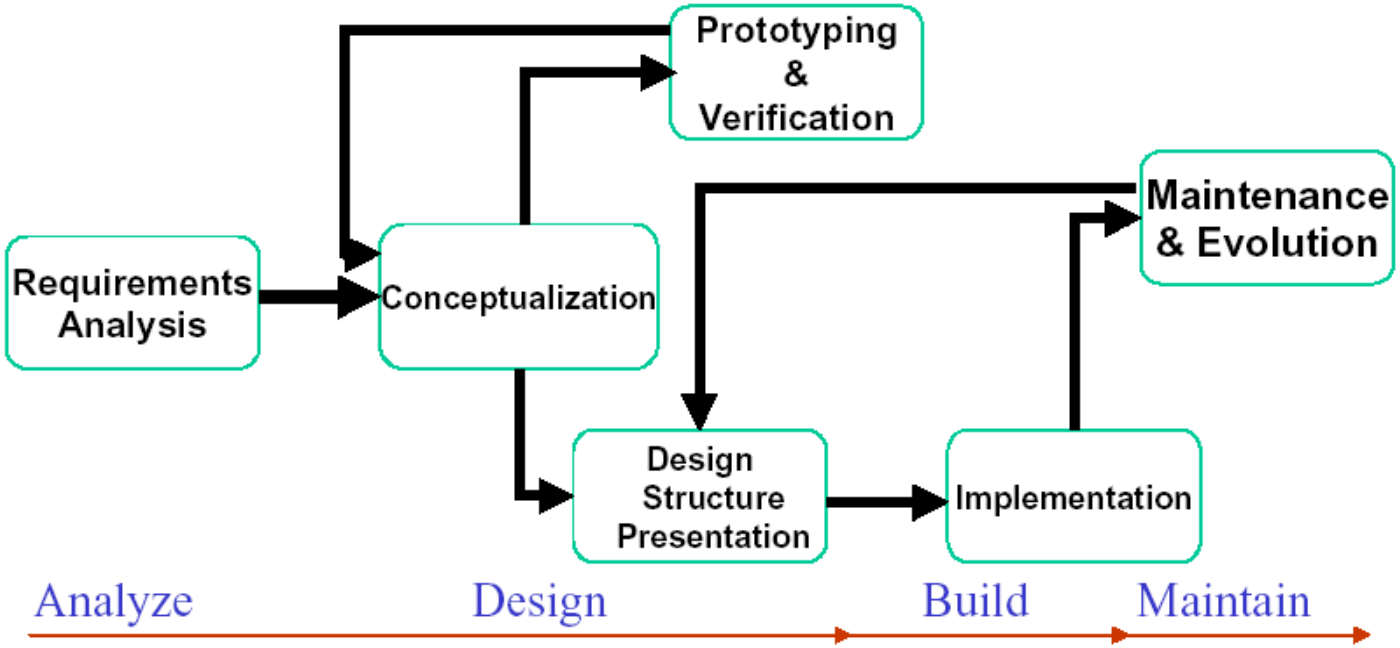


Example - RBAC for banking

- **Roles**
  - Examples: *teller*, *customer service representative*, *accountant*, *accounting manager*, *loan officer*
- **Hierarchical**
  - Examples: *customer service representative* is senior to *teller*
- **SSD**
  - Examples: (*teller*, *accountant*), (*teller*, *loan officer*), (*loan officer*, *accountant*), (*loan officer*, *accounting manager*), (*customer service representative*, *accounting manager*)
- **DSD**
  - Examples: (*customer service representative*, *loan officer*)
- **Prerequisite-Role**
  - Examples: *accountant* is a prerequisite for *accounting manager*.

➔ Banking institutes are a perfect environment for successfully implement RBAC – but beware of ‘politics’.

Role Life Cycle Management



Six activities**, performed within **four phases

Analysis	Find baseline, analyse security policy, decide tool support
Design	Define Model, Check IT-Systems capabilities, Set up the role-finding process, Build a corporate role catalogue .
Build	Deploy the role catalogue Build repository, operate cross-platform administration
Maintain	Cope with changes, watch triggers, maintain model constancy.

Role Life Cycle Management II

Analysis

- Find baseline and applicability of RBAC within the framework of resource ownership and approval rights within the corporation.
- Analyse the company security policy to identify factors impacting the RBAC concept, such as user attributes or approval rights.
- If necessary the policy has to be adjusted to reflect the new world of RBAC.
- Tool Support: Depending on the approach to role finding (top-down vs. bottom-up) appropriate tools for the corporate IT-environment need to be evaluated and decisions to be taken.

Design

- Define the RBAC Model.
- Match organisational, functional and administrative patterns within the entire corporation.
- Verify the Role Model by using prototypes.
- Check capabilities of IT-Systems to represent roles on each platform.
- Set up the role-finding process.
- Find decision criteria and/or attributes leading to roles.
- Build the RBAC data model.
- Define the interfaces with impact to the role-engineering process.
- Set up appropriate documentation standards.
- Build a corporate role catalogue.

Role Life Cycle Management III

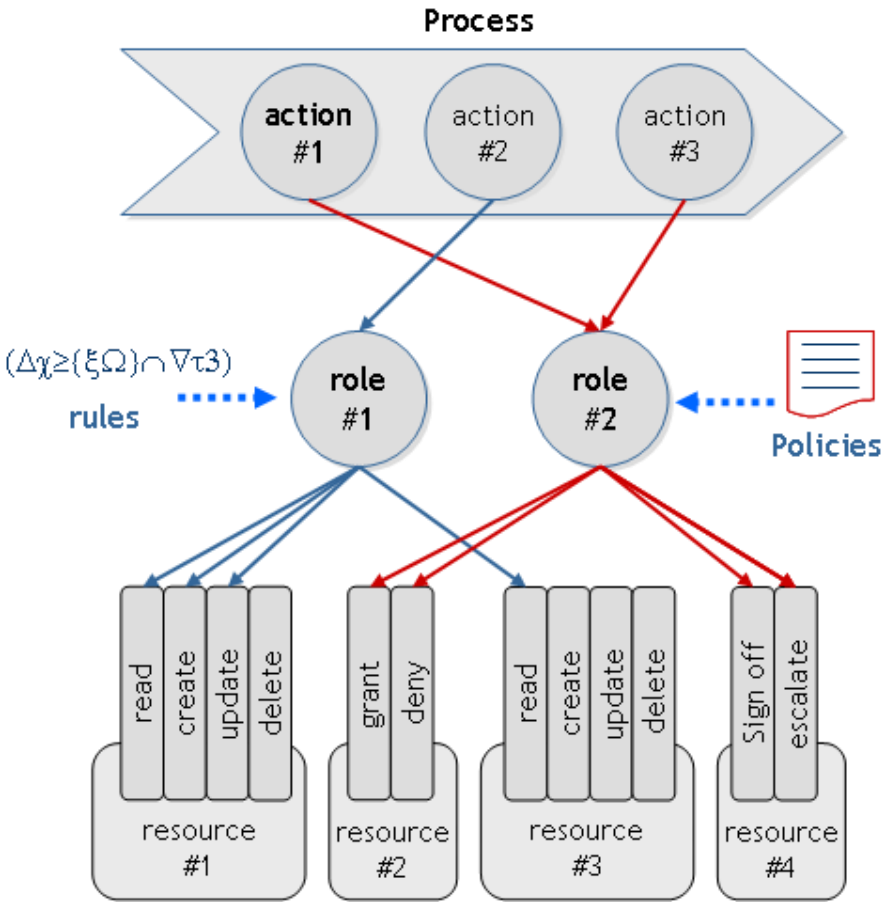
Build

- During the build phase, the following activities are performed
  - Deploy the role catalogue in the production environment.
  - Build repository using a cross-platform administration tool
  - Begin operating with cross-platform administration.
- Maintain consistency of role catalogue, the repository and request management procedures.

Maintain

- An enterprise wide processes to cope with changes and their impact to roles …
  - Adding roles,
  - Deleting roles and
  - Modifying roles.
- Triggers for role maintenance …
  - New or modified job descriptions within the HR organization,
  - Hiring and allocation of people to jobs,
  - Assignment to jobs of a temporary nature, like projects or task forces,
  - Business reorganisations, mergers & acquisitions, strategic alliances, partnerships like the appointment or termination of dealerships,
  - RBAC consistency checks, such as detection of unused roles,
  - IT configuration changes like new hardware or new applications.

From Processes to Roles



- A companies **planned activities** are documented as business processes.
- **Fundamental** business processes are triggered by an outside event and deliver their results there again.
- **Administrative** business processes deliver their results to a store.
- Business processes consist of a chain of **elementary activities**.
- An activity is defined as **„one person (Role) at a time in one location“**.
- A Role is the combination of von **Qualification**, **Responsibility** and **competence** for decision.
- **Permissions** to access a system result from the necessity for this role to act on it.

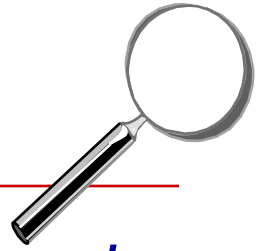
➔ Existing defined and documented business processes are an excellent starting point for successful role engineering.

Advantages of RBAC

- RBAC allows a **holistic view** at a corporation (unlike e.g. ACL‘s).
- RBAC supports entitlement **hierarchies**.
- RBAC support dynamic entitlement **inheritance**.
- RBAC enables to answer questions on **corporate level**, e.g. to which resources user B has (had) access to?
- RBAC represents a **compact notation**.
- RBAC can be implemented **across different platforms**.
- Policies implemented by an RBAC model are **easy to verify**.
- RBAC-models are easier and hence faster **changeable** .

➔ **RBAC** tends to be modelled after organisation’s **natural structure**.

RBAC – words of warning.



"An Enterprise could end up with as many or more roles than identities which only complicates matters.

Defining Roles can be a politically charged effort that requires enormous amounts of cross organizational cooperation.

Consequently, no enterprise has fully deployed a 'pure' RBAC model for Identity Management."

Burton Group Directory and Security Strategies Research Report, "Enterprise Identity Management: It's About the Business," v1, July 2, 2003

Pitfalls of RBAC

- Roles are **too static** for some dynamic business environments.
- Role based privilege assignment can be **misunderstood** and simply done wrong.
- Don't try to represent **all user entitlement** requirements in Roles.
- **Role proliferation** is a serious management problem.
- Sometimes **more roles than users** exist.
- Inappropriate design may let the situation **deteriorate**.
- Best practise is a balanced combination of **Roles and Rules**.
- Not all **business areas** are equally well suited for role engineering.
- Centralised business function can easily lead to a fatal **bottleneck**.
- business modelling is **not an easy task** anyway

➔ **RBAC** is not easy, but But leaving essential administrative processes on the currently lower level of maturity is no solution.

RBAC

Types of access control schemes

- „Role Based Access Control“ the business way.