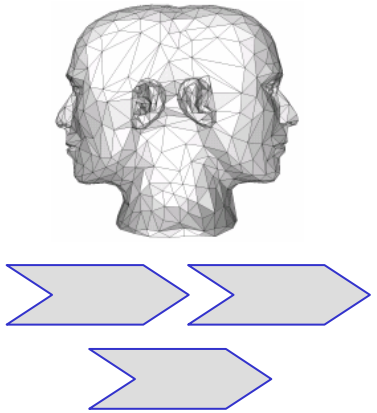


Modelling Generic Processes for the Identity- & Access Management

Work in progress

Version 0.43

2008-01-25, Dr. Horst Walther

Questions we answer here …

- ***Why*** we started the initiative GenericIAM – our Motivation**,**
- ***Where*** it will lead us ***to*** – The objectives of the initiative,
- ***Who*** are the Members of GenericIAM and their experiences,
- ***How*** we work,
- ***What*** the input we receives and the results will deliver and
- ***When*** will we come up with substantial results

agenda

- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

Our motivation

Wanted: a construction kit for standard processes within IAM

The idea behind GenericIAM

- The definition of IAM-processes cause major effort.
  - According to experience they account for up to 2/3 of the overall effort.
  - Nevertheless a core set of standard processes remains remarkable stable.
- Aren't there considerable similarities?
- Why start with a blank sheet of paper?
- Why reinvent the wheel again and again?
- Shouldn't we concentrate our efforts on the differences?
  - … and use the common set of standard processes "of the shelf"?
  - … from "GenericIAM"?

agenda

- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

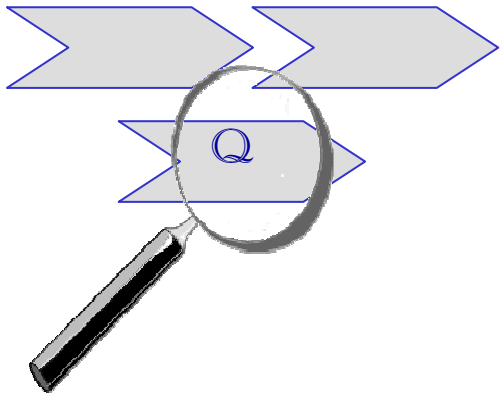
elements

- mission
  which goals are we aiming at?
- target group
  who should be interested in GenericIAM?
- benefits …
  generic IAM-Processes are of use for all market partners
- context
  the industrialisation of the service sector

mission

which goals are we aiming at?

- It is our **objective** to define a multi-purpose generic **process model** for the Identity- & Access Management (IAM)
- The process model may **serve as a template** for enterprise specific processes.
- Occasionally, it will be implemented unmodified.
- The processes shall be of an appropriate **high level of quality**.
- They shall be to in line with regulatory **compliance requirements**.



target group

who should be interested in GenericIAM?

- GenericIAM may be useful for every enterprise and every individual dealing with Identity- & Access Management.
- Our core target group comprises of enterprises with IAM processes and systems in place and / or under construction.
- Together with **vendors**, **consultants**, **analysts** and **system integrators** the represent the entire market.
- This desirable combination promises to deliver high quality and widely accepted results.
- Representatives of this target group are invited to become members of our initiative GenericIAM.
- The are expected to make a contribution in **content-**, **infrastructure-**, **PR-** and/or **financial** terms to support our objectives.

benefits …

stakeholders will gain benefits from generic IAM processes

- **Implementing enterprises** …
  - will benefit most by receiving a stable set of validated standard IAM processes.
  - They may complement and unify their implemented processes.
- **System integrators and vendors** …
  - Are enabled to deliver pre-built proven and realistic sample process.
  - In turn their clients may reduce modeling costs and project schedules.
- **Project Managers and Consultants** …
  - May start from a foundation of generic standard processes.
  - They cab focus on the true enterprise specifics.
- **The entire discipline** …
  - We contribute to the professionalism of the **Identity- & Access Management** in total through an approved and widely used process reference model.
  - We hence **ease the implementation** of policies, processes and IAM systems.
- **GenericIAM members** …
  - Demonstrate their professional IAM process expertise and experience to a broader audience by participating in leading edge standardization actions.

… benefits

implementing enterprises will benefit most

- **Anwenderunternehmen** haben überwiegend nur Teile der notwendigen Prozesse definiert und eingeführt.
  - Hier können sie die Frage beantworten **wie vollständig** bisher die eigenen Prozesse abgedeckt sind und wo es offensichtlich **Lücken** gibt.
  - Sie haben darüber hinaus **kostengünstig** die Möglichkeit, ihr Prozessmodell zu optimieren und zu vervollständigen.
  - Sie erhalten einen **Einblick**, wie weit andere Marktteilnehmer sind
  - Sie können feststellen, wie "**standardisiert**" und "**harmonisiert**" die bisherigen Abläufe sind.
  - Mit diesem Wissen können sie leichter die Frage beantworten: „*Wie (zukunfts-) sicher sind wir, wo besteht **Handlungsbedarf**, wo bestehen Optimierungsmöglichkeiten?*“
  - Mit diesem Wissen können sie die Frage beantworten: „Was müssen wir tun um vollständig **compliant** zu sein?"

Context
the industrialisation of the service sector

- We believe – we are part of a larger movement
- ITIL, SOA, compliance frameworks are details of a broader picture.
  - Regulatory compliance enforces the use of infrastructure standards
  - ITIL is just the beginning – CoBIT, ValIT and others will follow.
  - SOA provides a technical framework for its implementation.
- Market forces will drive to concentration on core competencies.
  - non-competitive actions will become standard commodities.
  - The will be low priced and sourced globally
  - … or outsourced / used as a 3rd party provided service.
- Organisational reference models take the development to the next level.
- GenericIAM as “Open org” may gain an open source like influence.

agenda

- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

elements

- We …
  Who are the individuals driving GenericIAM?
- Current members
  Users, Analysts, consultants, vendors und Integrators
- GenericIAM and the NIFIS
  NIFIS Competence centre „Identity Management“

Who we are …

within the GenericIAM Initiative

- We are …
  - a group of volunteers.
  - lead by the vision to develop a comprehensive generic process model for Identity- & Access Management.
- We are from …
  - various enterprises,
  - consulting companies,
  - analyst corporations,
  - system vendors,
  - system integrators and
  - universities and other academic institutions.
- Our objective is …
  - to develop and professionalize the Identity- & Access Management
  - to derive benefit from the participation for our daily work.

Current members
Users, analysts, consultants, vendors and system integrators

impuls IT Beratungsgesellschaft mbH
DEKRA
SIEMENS
WestLB
KUPPINGER COLE + PARTNER
IDS SCHEER Business Process Excellence
doubleSlash NET-BUSINESS
first@ttribute
SBI Ruhr
betasystems
covisint
Novell
ORACLE
VÖLCKER INFORMATIK AG
SIG
CSC
ConSecur security & consulting
Sun microsystems
trivadis makes IT easier.
SECUDE A HIGHER LEVEL OF IT SECURITY
KPMG
Nicole Kleff IS-Consulting
THORANET
syntlogo
DSK
ULD-i
IC COMPAS
Henkel
JOHANN WOLFGANG GOETHE UNIVERSITÄT FRANKFURT AM MAIN

as of 2007-12-01:

GenericIAM and the NIFIS

Competence center „Identity Management“ within NIFIS

- **Identity- & Access Management** is the essential foundation of an corporate-wide **security architecture.**
- Identity- & Access Management links technical to organizational tasks.
- The “National Initiative for Internet Security” (**NIFIS** e.V.) represents a group of enterprises to jointly fight the threats to the internet security.
- NIFIS acts as a point of contact for questions and issues to solve for all internet security related topics.
- **GenericIAM** fits perfectly in NIFIS’ objectives and approach.
- GenericIAM therefore joined NIFIS as **competence center** on December 1, 2006.
- Despite its national orientation the NIFIS will support GenericIAMs international move.

NIFIS Contact:
NIFIS e.V.
Competence Center
Identity Management
Weismüllerstraße 21
60314 Frankfurt
Phone: +49 69 40809370
Fax: +49 69 40147159

agenda

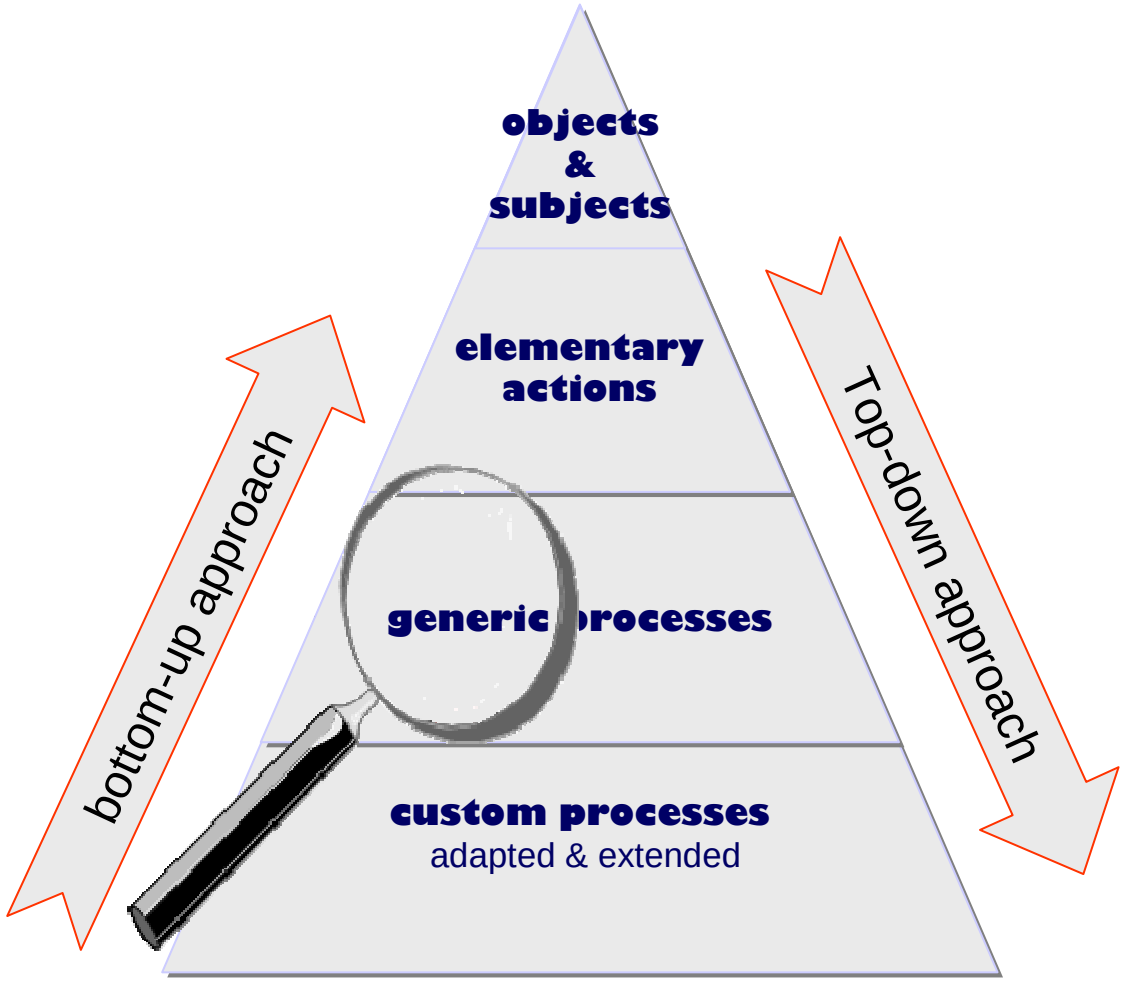
- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

elements

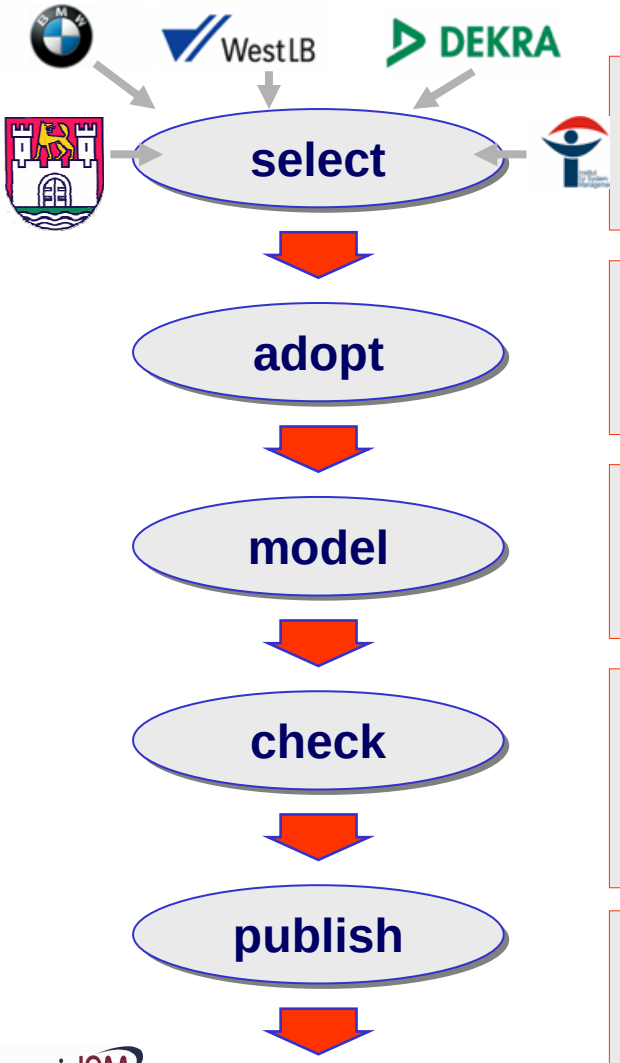
- Layers of processes
  how to include generic processes into a process model.
- Our approach
  From a specific solution to a standardized model
- Quality Assurance …
  is an essential part to achieve our objectives.
- Meetings
  we meet quarterly in person.
- Licence model
  we publish our results under the creative commons licence.

Modelling approach

bottom-up- and top-down-approach lead to one generic model



Our approach
From a specific solution to a standardized model



- Enterprises contribute their IAM processes
- These processes are processed to the generic process model.
- They usually don't add to their competitive advantage.

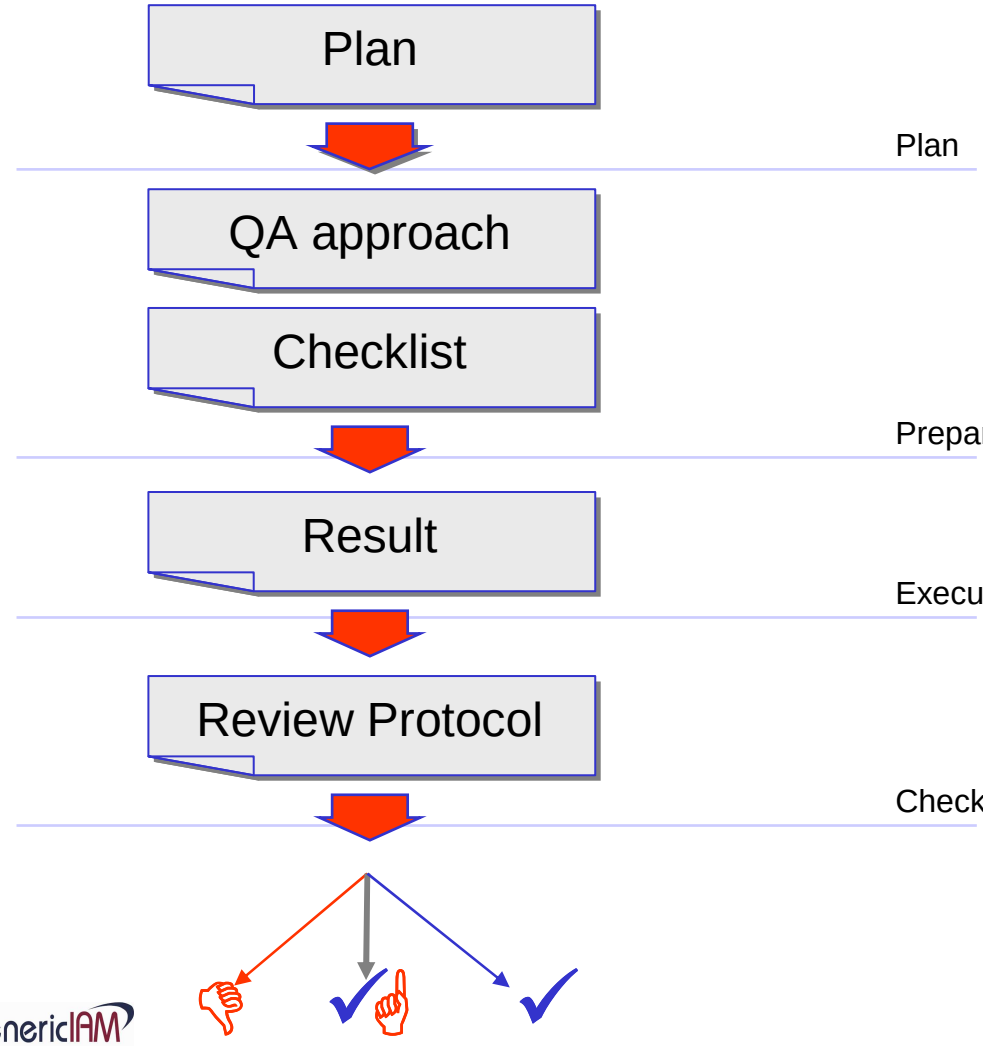
- Enterprises may hand over theirs models in various formats.
- NDAs will be signed on request.
- The modeling team selects the generic process candidates.

- The processes are anonymized to remove enterprise specific terms.
- They are standardized through naming and modeling conventions.
- They are generalized to take advantage of standard roles.

- The results will be checked by our review team.
- The generic processes will be formally signed off for publication
- Reviewers are GenericIAM- and occasionally external experts.
  - They release only defect-free processes.
  - The modeling team will remedy deficiencies

- The process model will be published annually.
- Members of GenericIAM will get them free of charge.
- Interested parties can purchase the process model.

Quality Assurance …
is an essential part to achieve our objectives.



- Plan sufficient time for QA.
- Define approach,
- Deliver quality criteria (checklist),
- Craft the results,
- Review the results,
- Results are …
  - Signed-off or
  - Conditionally signed-off
  - Rejected

Meetings
we physically meet once per quarter.

- We hold quarterly one day meetings at a member's location.
- We discuss and sing-off results during these meeting.
- We defined and assign new tasks and decide next steps.
- Meeting minutes document the meeting decisions.
- Previous meetings were...
  - 2006-04-25, Frankfurt, host: Kuppinger, Cole + Partner
  - 2006-06-20, München, host: Kuppinger, Cole + Partner
  - 2006-09-27, Wiesbaden, host: Digital ID-World
  - 2006-12-01, München, host: ORACLE
  - 2007-03-02, Düsseldorf, host: WestLB AG
  - 2007-05-07, München, host: EIC 2007
  - 2007-06-29, München, host: CSC
  - 2007-10-12, Frankfurt, host: NIFIS
- next Meeting:
  - 2007-02-08, Frankfurt, host: NIFIS

agenda

- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

Modelling fundamentals

How to remove legacy implementation artefacts

- Here we use McMenamin and Palmer's „Essential Systems Modelling Methodology“.
- It is an "event-oriented" approach to process modelling.
- Their purpose is to identify the "essential (elementary or atomic) processes" being performed and their relationships to the events that drive the business.
- According to Steve McMenamin and John Palmer [McMenamin84] essential systems can be detected by the following
  - "If we had perfect implementation technology (e.g., a computer with infinite speed, unlimited memory, transparent interface, no failures, and no cost), which of the requirements would still need to be stated?"
  - Every requirement that is still necessary in spite “perfect technology” is an essential requirement

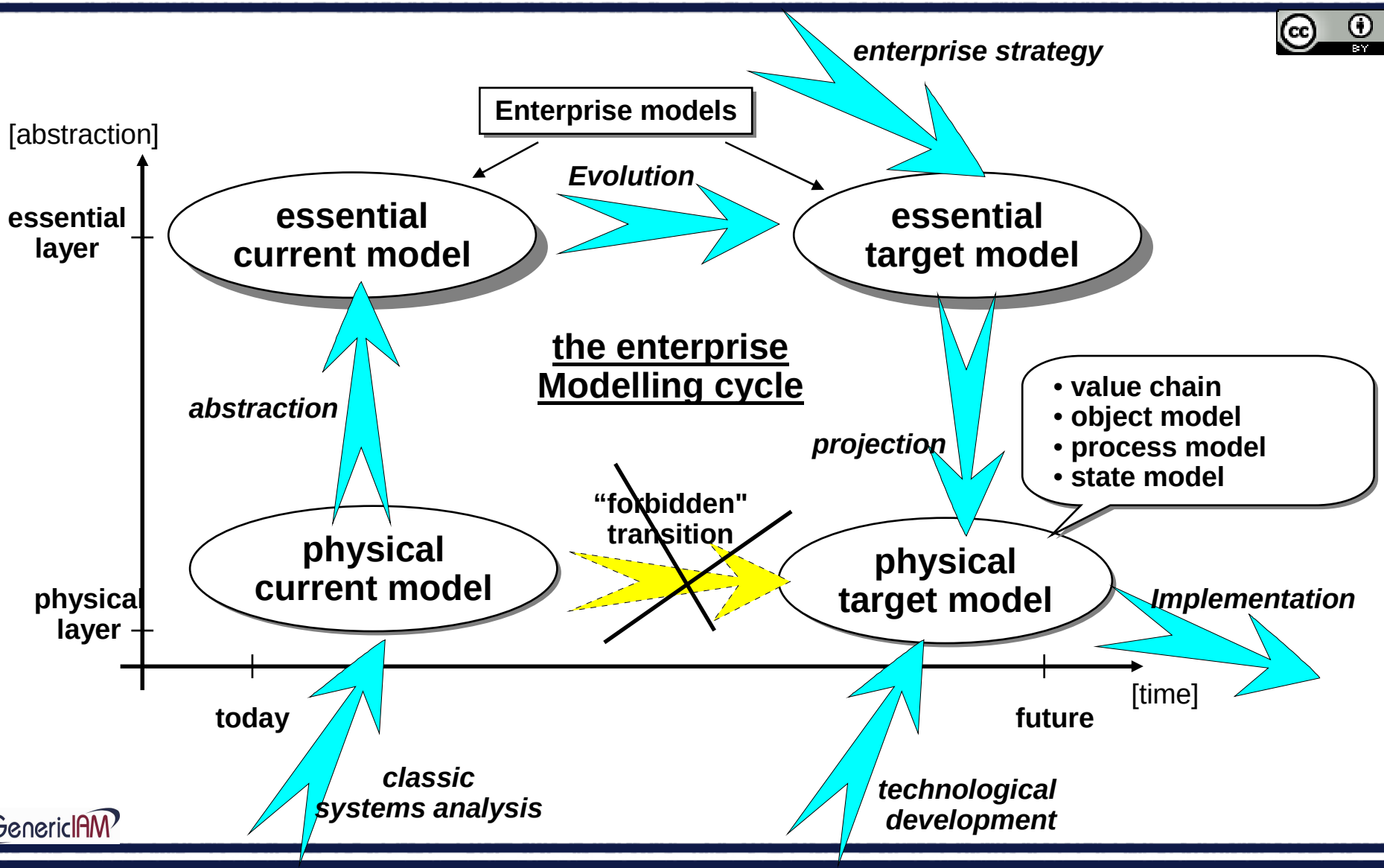
Modelling process
Derive the target implementation model in a 4-step Process

- McMenamin und Palmer recommend to follow a **4-step** specification **process** :
  - Analysis of the **current system**
    - build a model of the actual implementation of the current system.
  - Analysis of the **fundamental concepts** of the current system:
    - Deriving of the essential model of the current system.
    - All implementation specific artefacts are removed in this step.
    - Using “perfect technology” as the guiding principle.
  - Include **new requirements** into the essential model:
    - Build the new essential model by adding new requirements.
    - This model represents all functional requirements.
    - Ideally it is free of any design- and implementation consideration..
  - Design the **new physical model**:
    - Build the implementation model of the new system.
- The 3rd step in this approach is represents the core of the **requirements definition**.

Essential Modelling
avoiding technical „folklore“ by assuming “perfect technology”

- The assumption of **perfect technology** results in:
  - Inside the system there are neither errors nor processing or waiting times.
  - No check-, translation- and transport processes are necessary.
  - But the environment of the system is considered as imperfect.
  - Along the systems boundary a ring of check-, translation- and transport processes connects this real world – the physical Ring.
- Essential Processes may be triggered by an **external** or a **time event**.
- **Fundamental** essential processes yield an externally useful result.
- **Administrative** essential Processes store their results in an internal store to be used by a fundamental essential process.
- Essential Processes communicate asynchronously via essential stores – they are **time decoupled**.

The modelling cycle
finding the essence removes implementation artefacts



Grouping to obtain business processes
elementary actions are grouped by their business relationship

- The elementary actions found are grouped by their inherent business relationship to result in business processes.
  - The elementary actions can be found by discovering state transitions of the fundamental (persistent) business objects.
  - The business relationship is expressed in the value chain and can be taken from there.
- Business processes behave like travelling guests
  - they are created by an **event**,
  - they are **transient** objects.
  - they undergo several state **transition**.
  - they change their state by elementary actions.
  - they carry along their local knowledge about triggering events, acting processor, affected business objects.
  - after delivery they terminate their active life.

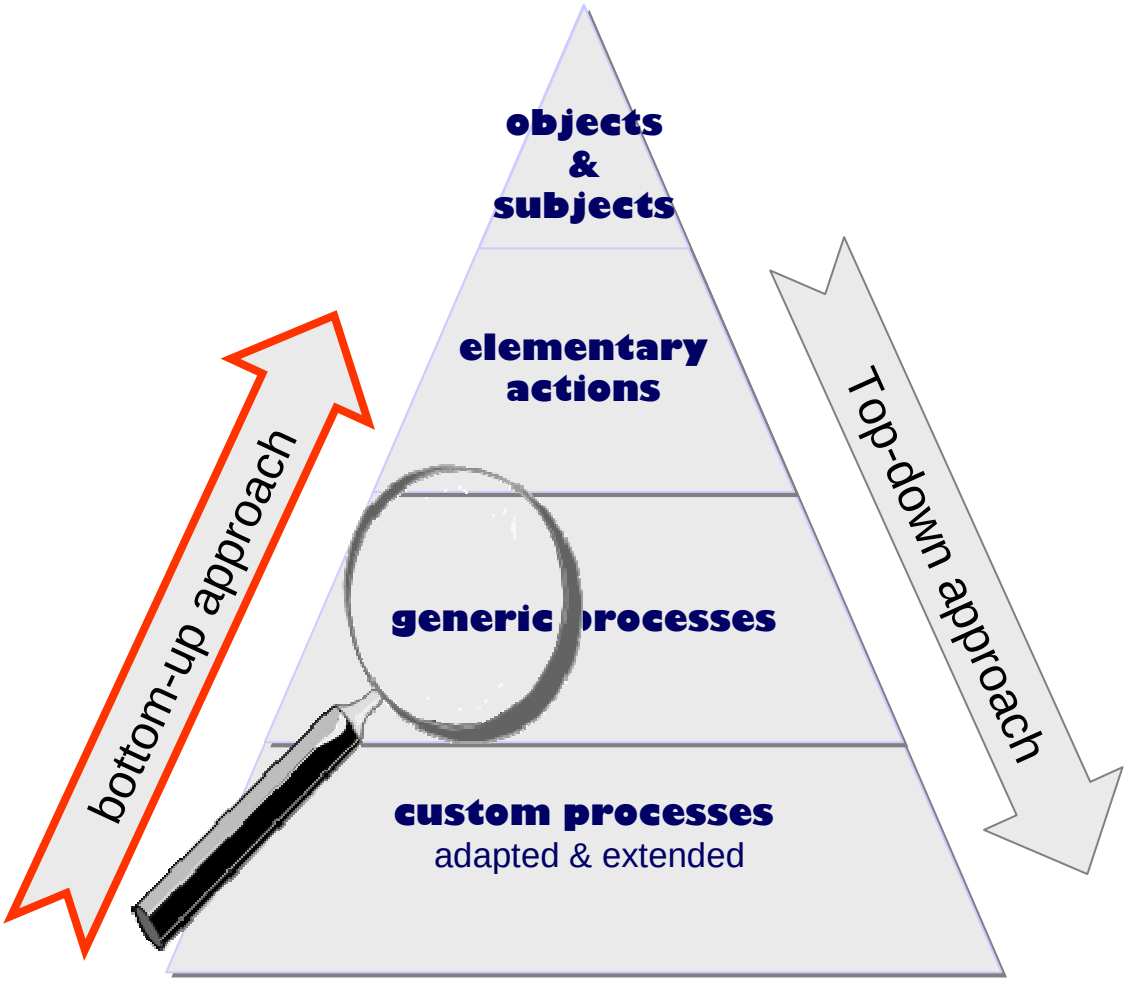
Modelling Guidelines
domain related modelling criteria

IAM-processes need to be modelled according to few overall guiding principles:

- Linked to embedding business processes
  - IAM-processes are triggered **by business needs** in a defined context.
  - Embedding business processes should be **in place** before hand.
- Business adjusted
  - It is the business **process responsible** to decide on the protection level.
  - Business process responsible need **adequate advice** for their decision.
- Risk based
  - The strength of the security measures should be determined by the corresponding **business risks**.
  - "**Too much security**" may cause losses in business terms as well.
- Feasible
  - Feasibility and fit to **practical needs** is a major requirement.
  - Processes which are **hard to follow**, will be ignored or circumvented.
  - Automation, self service and ease of use are **key factors** for success.
  - In multi-step processes the actual status must be **transparent** and traceable for all involved.

Modelling bottom-up

deriving genericity from implemented real world processes

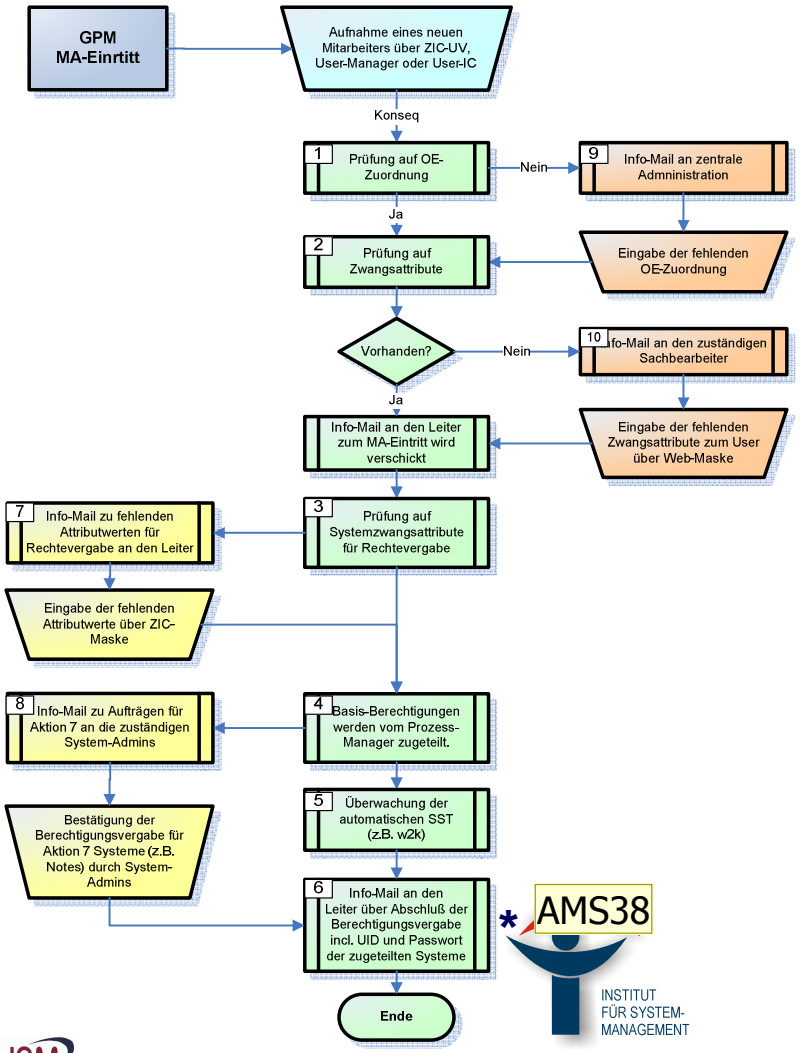


Process list

bottom-up processes - anonymised, standardized but not generic

- **hire employee**
  an employee enters an organisation.
- **release employee**
  an employee leaves an organisation.
- **logout globally**
  immediately terminate all current applications sessions.
- **sack globally**
  immediately lock an employee's privileges on all enterprise resources (as an exception).
- **re-certify**
  confirm an identities current privileges on a resource.
- **certify**
  confirm the compliance of products and services to standards.
- **clean data**
  find and clean inconsistent, fragmentary and redundant IAM data.
- **request account**
  request and approve a single access to an IT system.
- **request role**
  request and approve a role assignment.
- **request group**
  request and approve a group assignment.

Input-Example
non-generic process “Hire employee”



- If an employee is not assigned to a business unit:
  - Inform the central administration.
- If the necessary user attributes are not known:
  - Identify and inform the corresponding official.
  - Insert missing user attributes.
- If necessary system attributes are not known:
  - Inform recipient, e.g. manager
  - Insert missing system attributes.
- Assign basic access right automatically via basic roles.
- Assign logon name for systems automatically according to name generating rule.
- Create privileges within systems automatically (user provisioning) or via mail to system administrator.
- Technical monitoring of the connectors
- Inform manager about employee’s privileges.

*** Modeled by ism – Institute for System Management**

Folie 32

AMS38 Hier gibt es sicherlich von iSM schon eine einglische version, die man einfügen kann. Wenn nicht, kann ich die Texte noch verallgemeinern (da produktbezogen und nicht "generisch") und übersetzen.
Dr. Angelika Steinacker; 05.05.2007

Process List

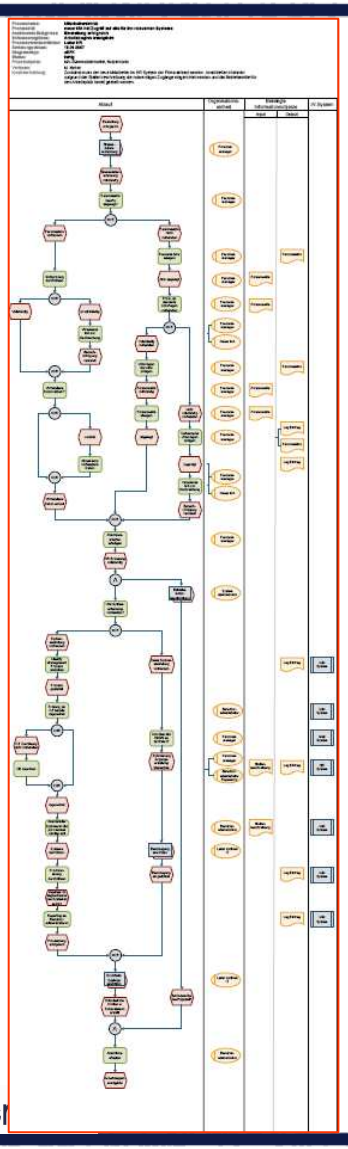
bottom-up Processes - anonymised, standardised but not generic

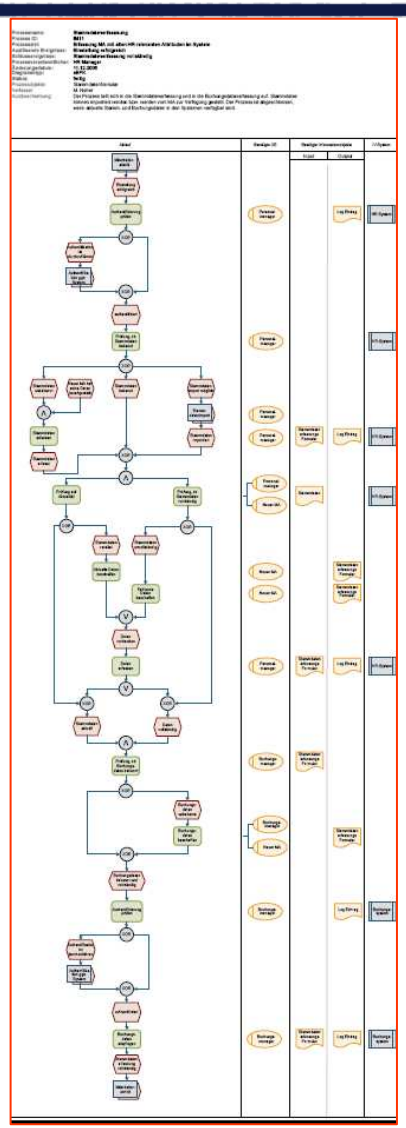
- IM10 Mitarbeitereintritt
- IM11 Stammdatenerfassung
- IM12 Basiszugang einrichten
- IM13 Erweiterte Zugänge einrichten
- WM10 Antragsverfahren Nutzerkonto
- WM20 Antragsverfahren Rollen
- WM30 Antragsverfahren Gruppen

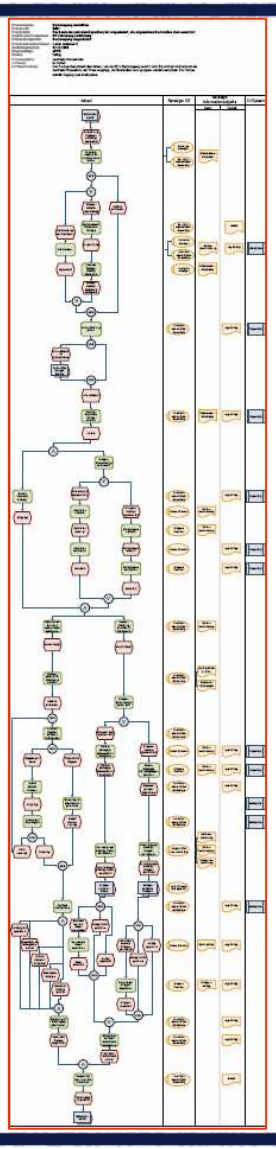
Still modelled in German language

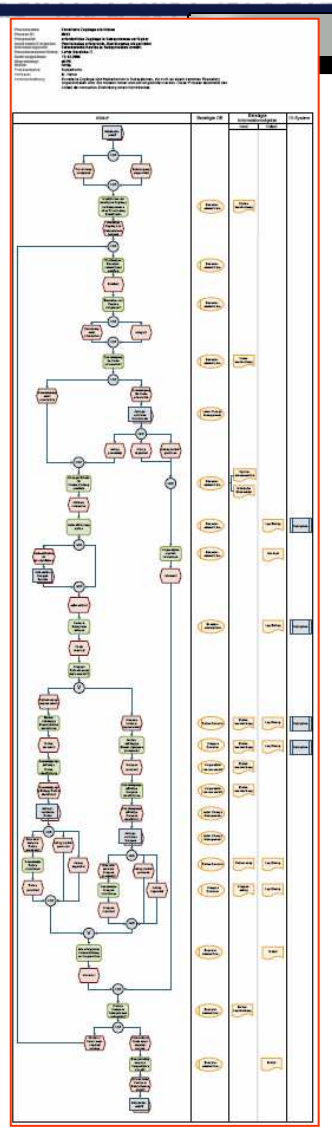
Process List I

bottom-up Processes - anonymised, standardised but not generic



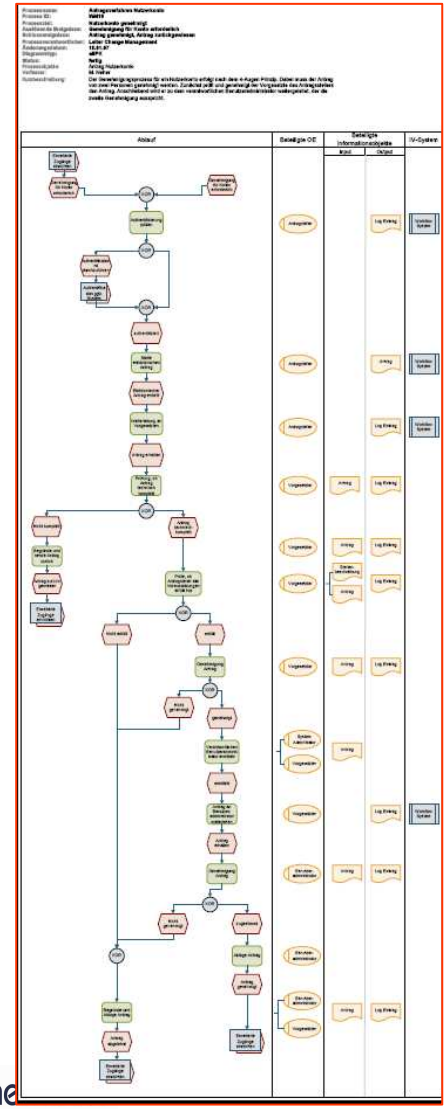


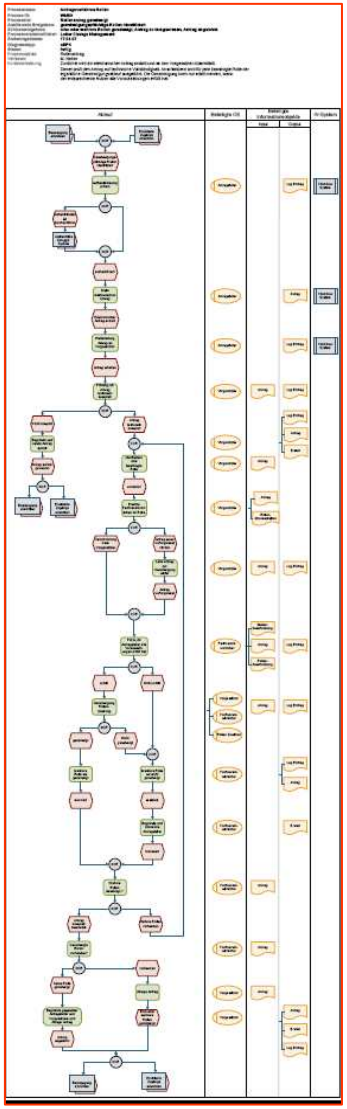


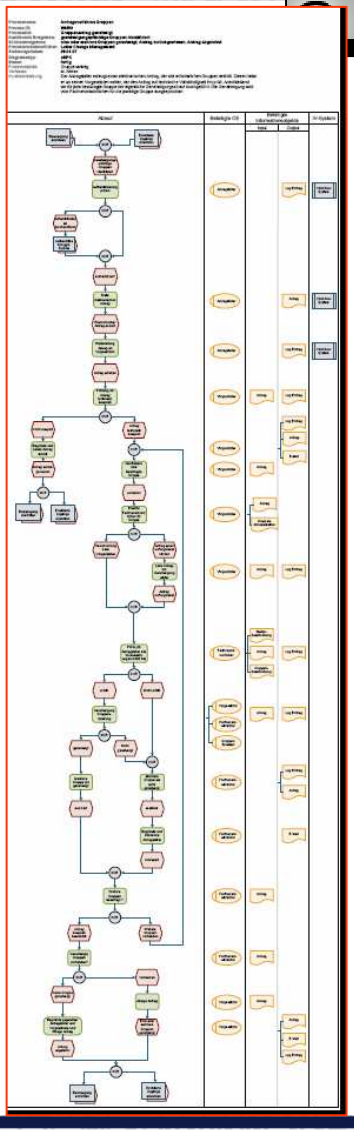


Process List II

bottom-up Processes - anonymised, standardised but not generic

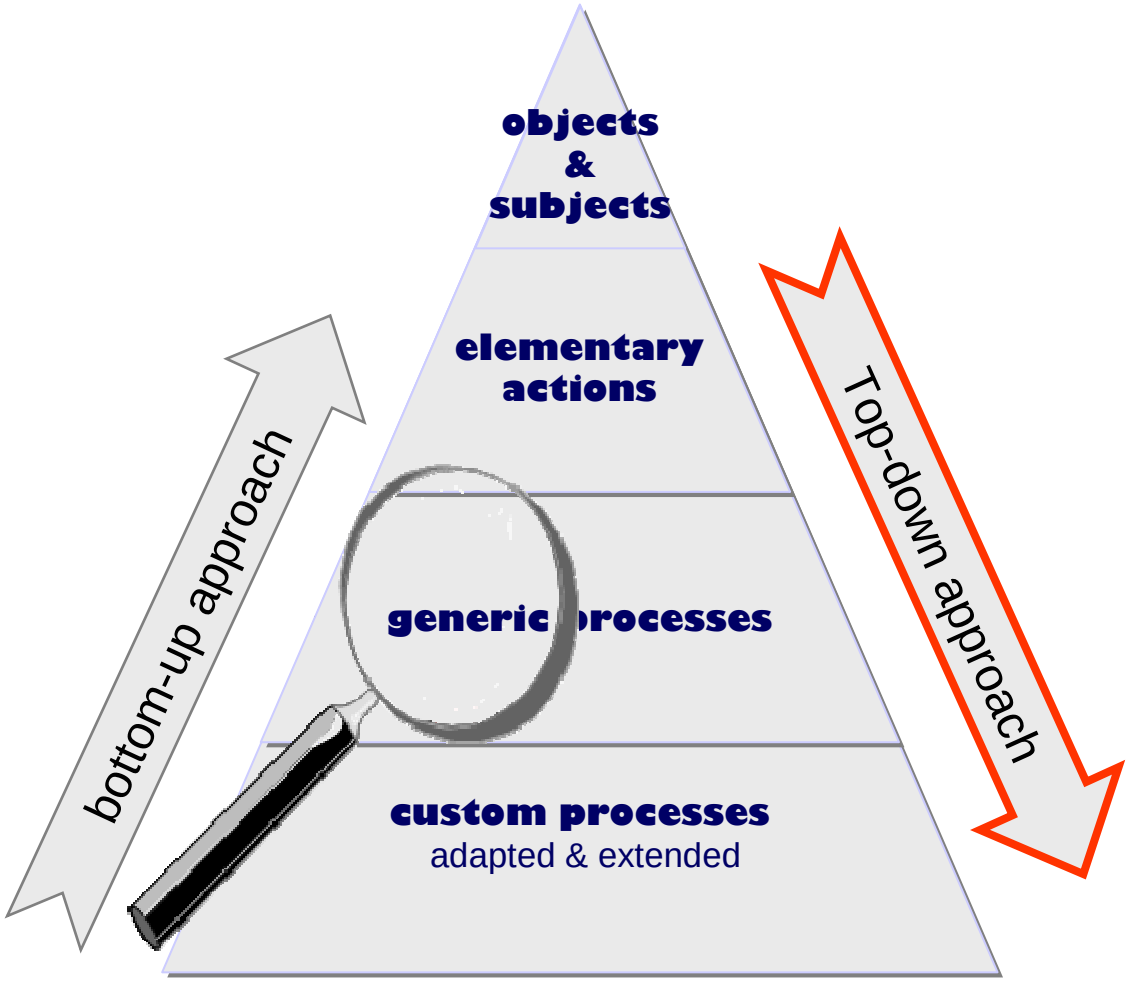




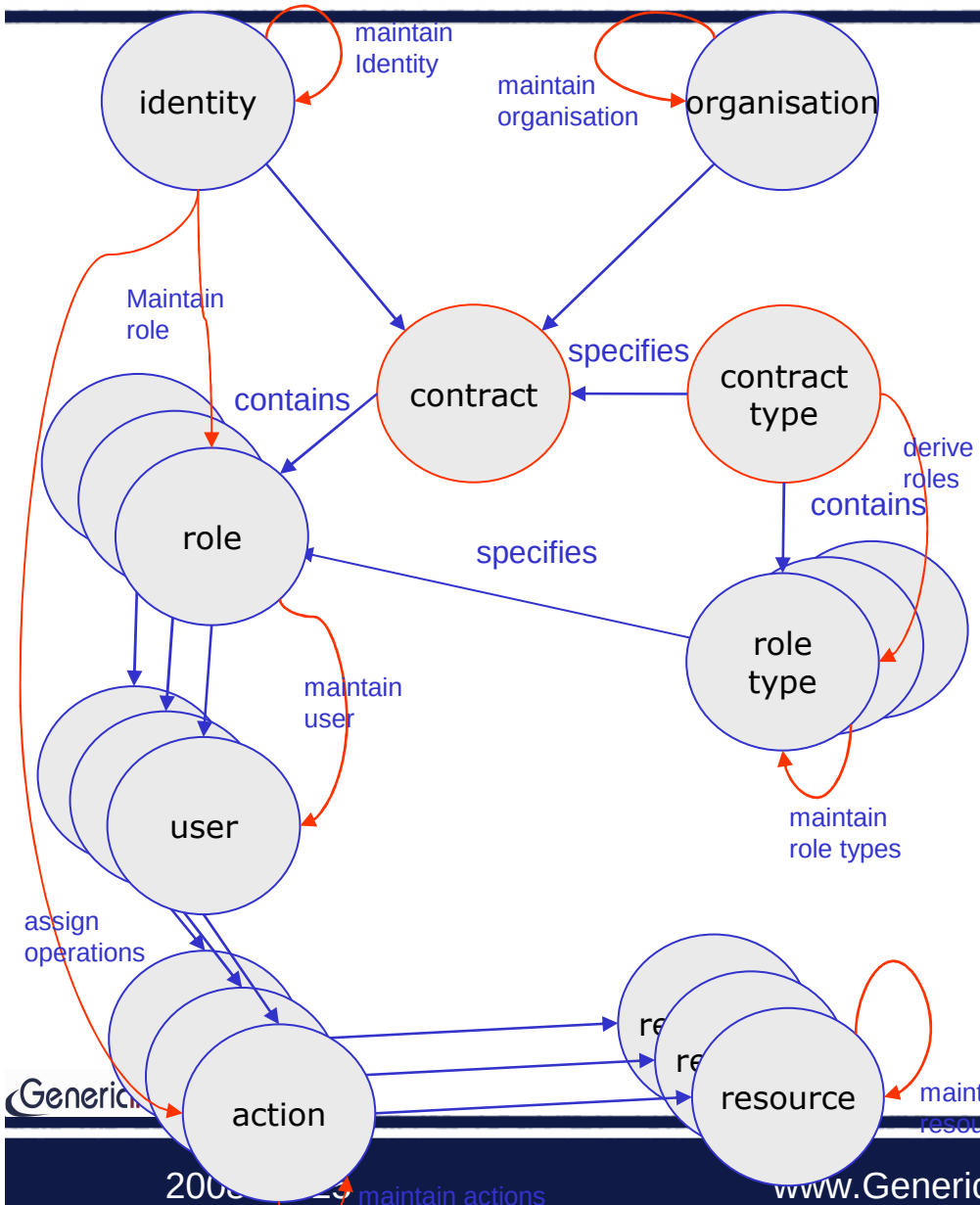


Modelling top-down

deriving genericity from interactions of generic objects



elementary actions – changes on objects



- The Identities role in an organisation performs actions on resources
- The Processes consist of >= 1actions.
- They are triggered by an event.
- They lead to a meaningful result to a subject.
- Process types (the class or definition) and process instantiations (incarnation, actual).
- Operational processes and managerial processes.
- Operational processes: *identification*, *authentication* and *authorisation*.
- The managerial:
  - *administrative processes*,
  - *audit processes* and
  - *change processes*.
- The administrative processes represent the “lions share” of all IAM processes.
- Its most prominent representative is the “*request & approval process*”.
- defines the relationship
  - a role defines incarnation details
  - “the contract is expressed by several roles”

Deriving elementary actions is an obvious process

- Each object in the big picture needs a maintenance process
- Maintenance covers CRUD (create, read update, delete) and assignment

object	process	class	level	event	result
owner	maintain owner	administrative	essential	new owner, oor change	mantained owner
rule	maintain rule	administrative	essential	new or chaned policy	maintained rule
user	activate / deactivate user	administrative	essential	role change	(de-) activated user
operation	report operations on object for owned identities	audit	essential	request	report
policy	maintain authentication policy	change	essential	new or changed authentica	maintained authentica
policy	maintain federation policy	change	essential	new or changed federation	maintained federation
role	maintain role	change	essential	request	maintaned role
role type	maintain role type	change	essential	request, new system, new	maintained role type
system	maintain system assigments	change	essential	system change, policy char	maintained system as
system	maintain system	change	essential	new or changed system	maintained system
identity	autenticate identity	operational	essential	request	autenticated, rejected
identity	maintain role to identity assignment	operational	essential	request, contract change	maintained role type
identity	notify identity on request status	operational	essential	request fulfilled / rejected	subject notified
identity	maintain identity	operational	essential	new or changed identity	maintained identity
operation	maintain operation on object	operational	essential	new or changed object, ope	maintained operation
operation	reconciliate operations on objects	audit	physical	request, time	exception report
identity	federate identities	operational	essential	new or changed identity	federated identitties
system	login to system	operational	physical	login request	user logged in
system	(de-) provision operation on objects	operational	physical	request fulfilled / rejected	(de-) provisioned oper

Applying the generic essential model

The model enables deriving a complete set of elementary actions.

- In order not to underestimate the number of ‘trivial’ maintenance processes.
- The majority of processes consists of only one elementary action.
- A minority of processes is more complex.
- Customising the model to a specific situation covers …
  - Naming all resources
  - listing all actions
  - Fleshing out the organisation
  - Naming the specific owners
  - Stating policies
    - e.g. for pre-approved role assignments
- Adding physical actions
- Linking to embedding business processes

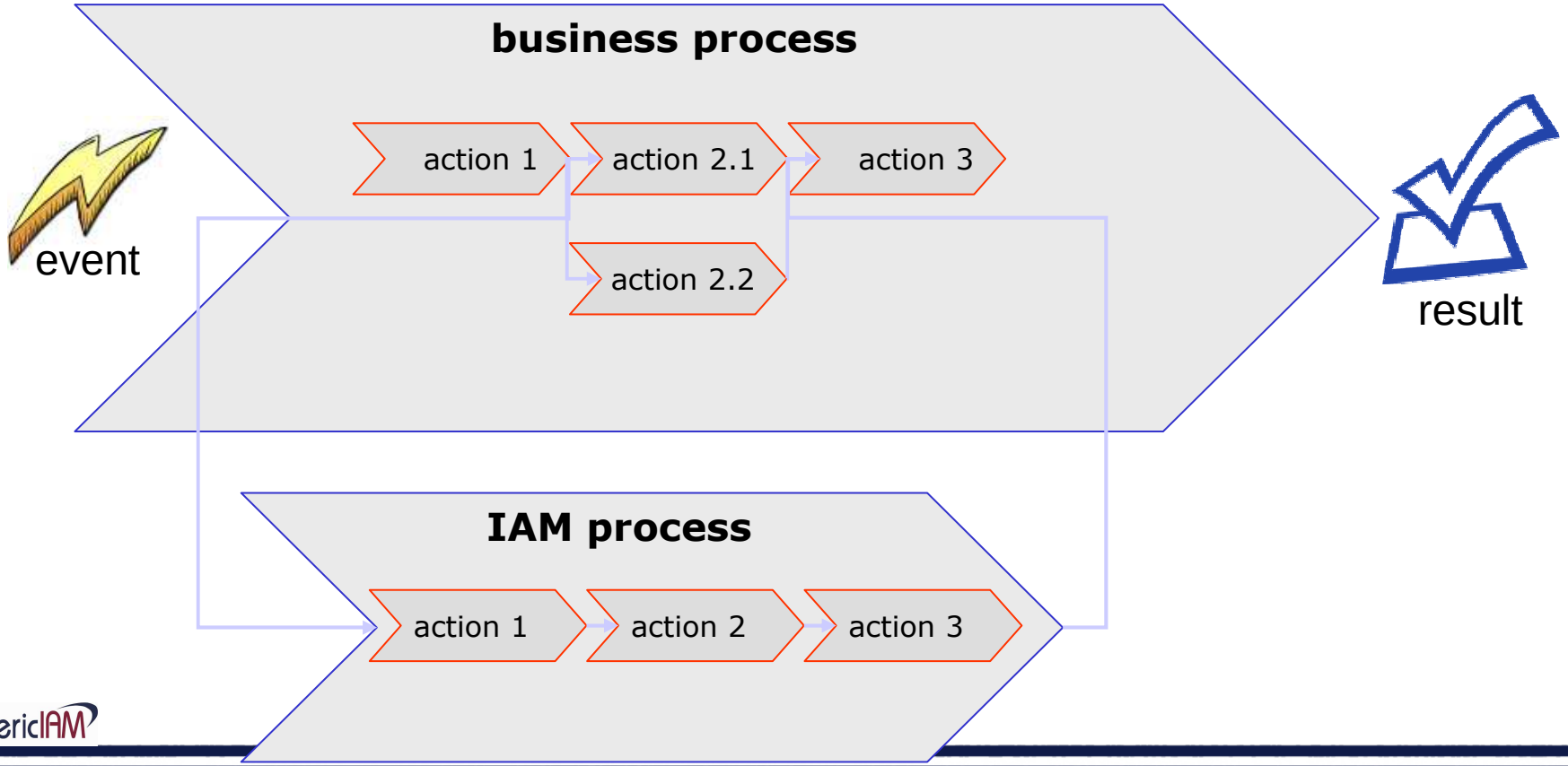
Applying the generic essential model
Adding physical actions

- Transport
- Translation
- Check controls (for GRC)
  - Preventive
    - avoiding an unwanted situation.
    - Policies and procedures
      - example.: change Management.
      - "all changes will go through a formal change management process“
    - Because 80% of computer errors are related to human error
    - Formally reviewed, tested and a rollback plan been developed if the change failed.
    - Monitoring can be used preventively.
    - preventive controls are not sufficient.
  - Detective
    - alert us when an unwanted event transpires.
    - as soon as possible, but it is after-the-fact.
  - Corrective
    - restoring the system to its expected state.
    - Having backup configuration files or hard drive images that can be reloaded to restore the state are both good examples.
    - predicated on an organization having effective change control and configuration management.

Linking to embedding business processes

IAM-processes are triggered by business needs in a defined context.

- IAM-processes often are not stand-alone
- They are mostly part of embedding business processes
- This relationship has to be maintained seamlessly



Business processes
embedding business processes should be in place before hand.

typical business driven processes
which require the invocation specific IAM-sub-processes are:

- On boarding processes
  - hire employee
  - acquire customer
  - contract partner
  - contract temporary staff
- Off boarding processes
  - terminate employee
  - terminate customer
  - terminate partner
  - terminate temporary staff
- Change processes
  - change employees job description
  - de-activate contract (employee, customer, partner, temp. Staff)
  - re-activate contract (employee, customer, partner, temp. Staff)
  - changes identity attributes (marriage, name-, sex-change, …)

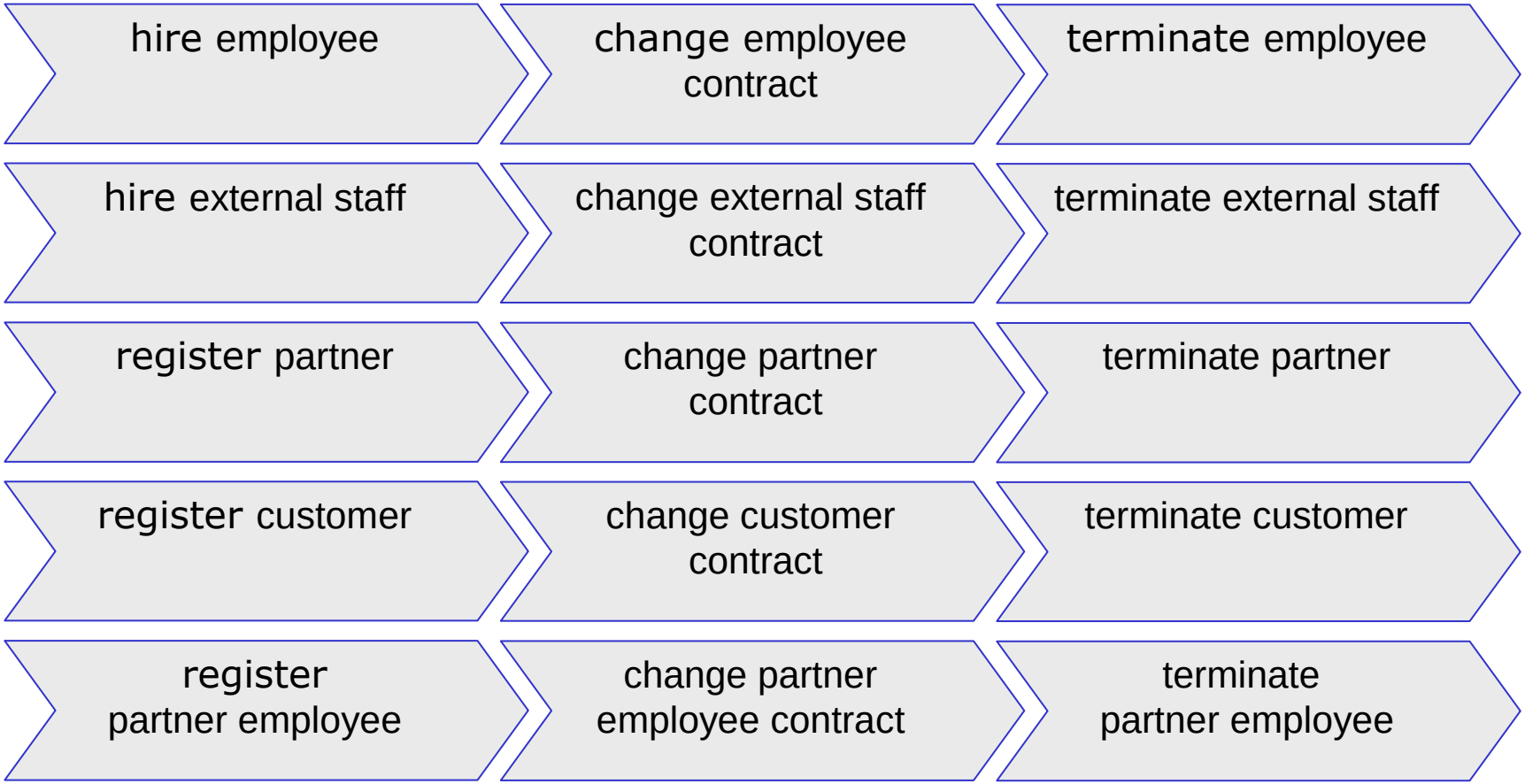
For these processes in an early stage it has to be determined, whether this individual is known to the corporation already (a digital identity exists).

Terminating means flagging as arched. Records are deleted when they are no longer of value or when data protection rules require deletion.

Change process tend to be complicated. Rarely there is a clear cut. Often an overlap of responsibilities requires phasing-in & phasing-out periods. Temporary responsibilities like project roles may be assigned additionally for a limited period.

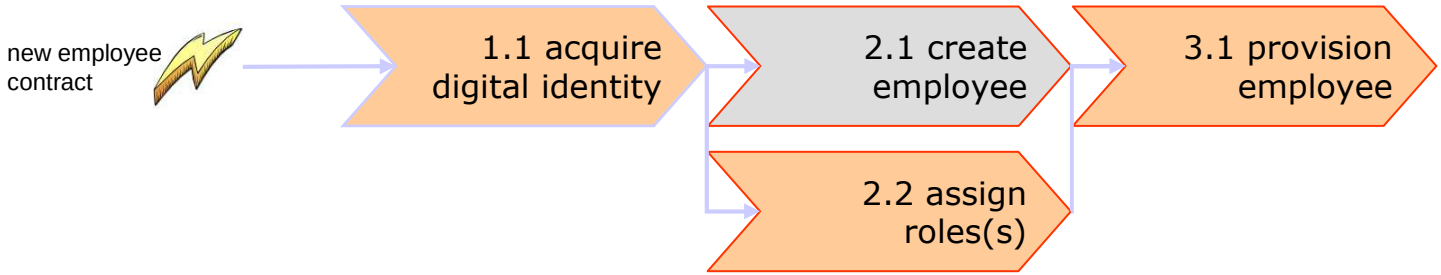
fundamental business process groups
and their variation by type of digital identity

- The 3 fundamental business process groups on-boarding, off-boarding & change processes split of by type of digital identity.



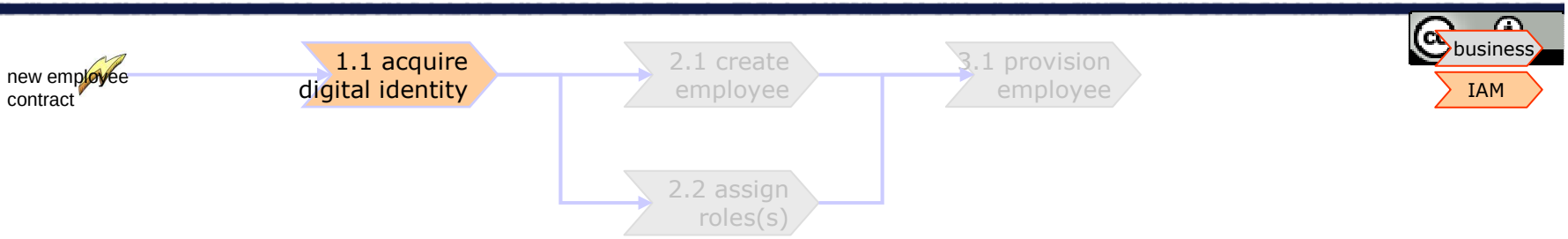
Business process “hire employee”
IAM- and business actions are interlinked

- The existing process “hire employee” …
  - needs to be split up into business- and IAM-actions
  - has to position the assignment of a digital identity up-front
  - must deliver 3 more attributes (+ contract type, + region, + location)
  - Identifies employees (like external staff) by …
    - 1st assigned full name (birth name)
    - date of birth
    - location of birth



business
IAM

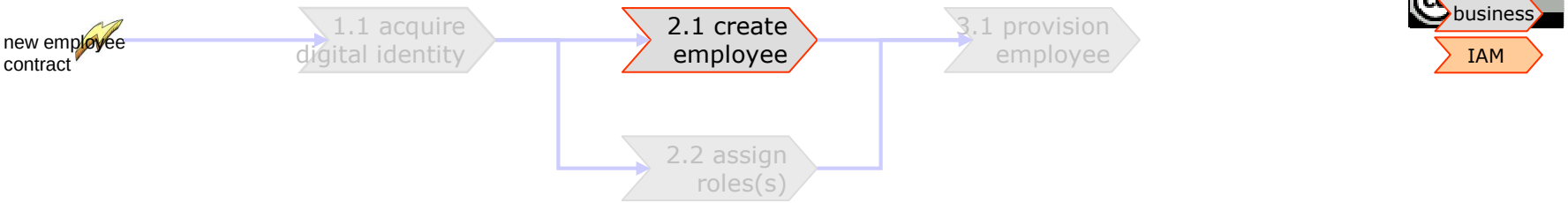
Business process “hire employee”
1.1 acquire digital identity



- The action “acquire digital identity” …
  - 1st looks up a central corporate directory for the employee
    - If it does not exist it will be created
    - If exits it will be reactivated
    - Search must include employee-, partner- & customer-identities
    - Duplicate entries must be detected during search
    - Non-obvious cases must be offered for manual selection
  - requires all identifying attributes to be provided at this point in time.
  - returns a unique ID, which ..
    - is non-disclosing
    - doesn’t carry any additional information
  - returns address data
  - returns it’s result in “real-time” (< 3 sec.)
- The “corporate identity manager” is responsible for this action.

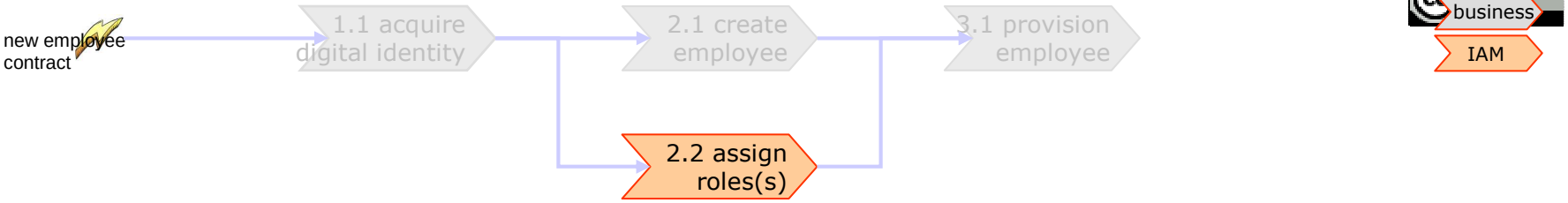
Business process “hire employee”

2.1 create employee



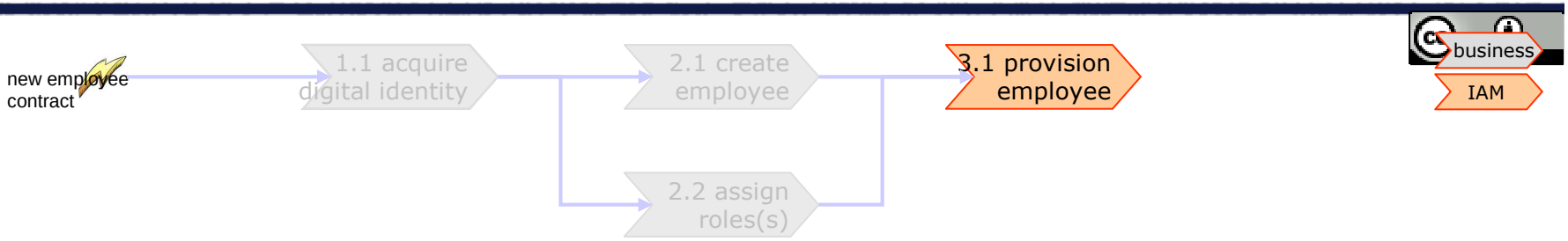
- The action “create employee” …
  - creates the personnel number
  - creates the personnel record in the HR-System
  - stores the ID delivered by action 1.1
  - in contrast to the current implementation stores the additional attributes …
    - contract type (e.g. “full time employee)
    - region (e.g. ASPAC)
    - location (e.g. Singapore)
  - may stay untouched besides these changes.
  - is a manual action and returns it’s result within one working day.
- The “human resource manager” is responsible for this action.

Business process “hire employee”
2.2 assign role



- The action “assign role” …
  - assigns a predefined “business role” to the employee
    - business roles are defined in terms of business entitlements
    - Role assignment doesn’t require detailed system knowledge
  - alerts the “corporate identity manager” in case of missing / ill-defined roles.
  - does not assign individual privileges
  - assigns roles for 85 % of all employees
  - may be skipped in 1st implementation increment due to project design.
  - is a manual action and returns it’s result within one working day.
- The “corporate identity manager” is responsible for this action.

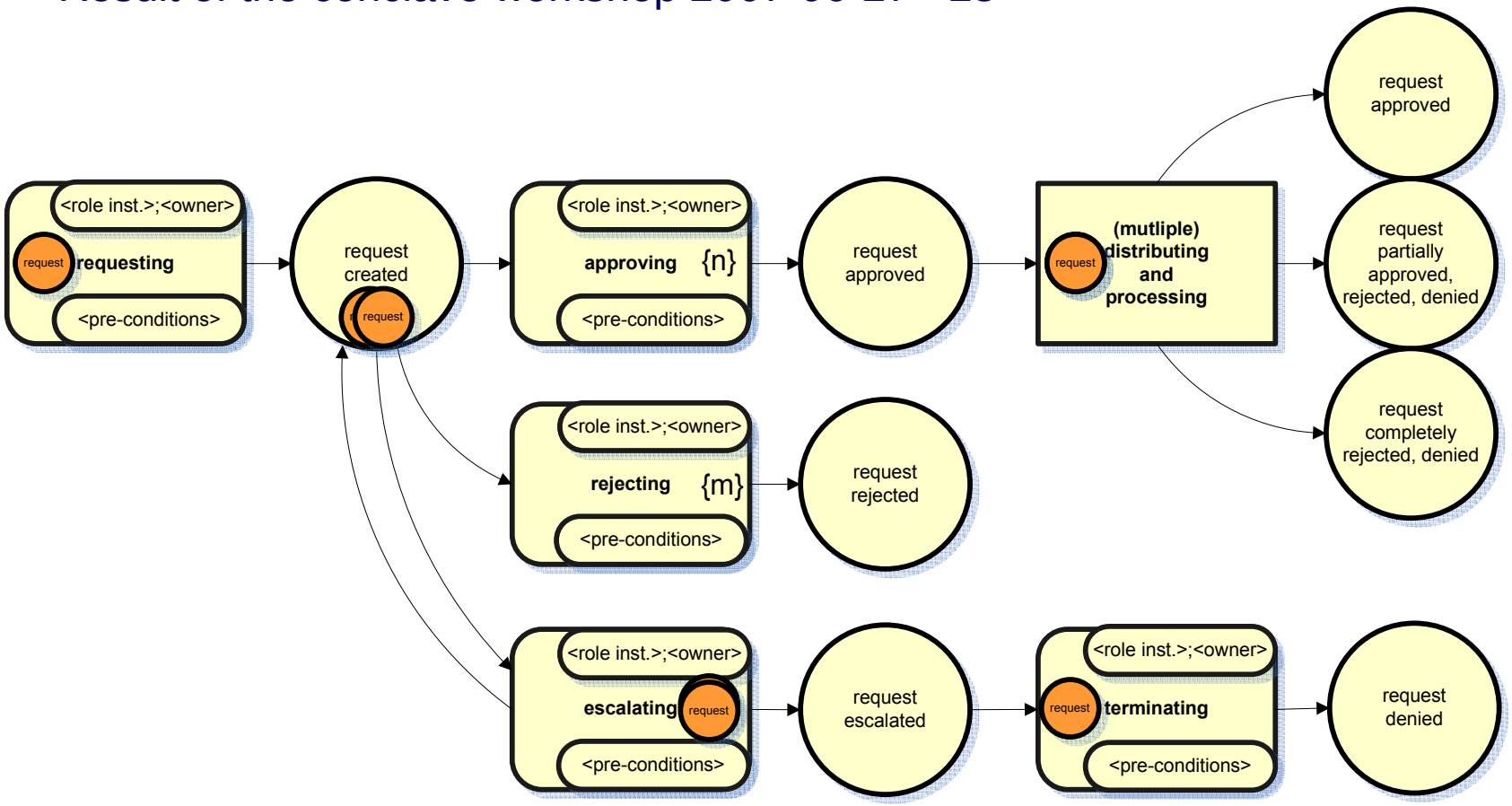
Business process “hire employee”
3.1 provision employee



- The action “provision employee” …
  - provisions all the ID + all current attributes +
    - address data
    - contract type (e.g. “full time employee”)
    - region (e.g. “ASPAC”)
    - location (e.g. “Singapore”)
  - will later be complemented by
    - Translates roles to elementary privileges according to corporate policies.
    - provisioning {1..n} privileges
  - provisions the ISP in “real-time” (< 5 min.)
    - ISP needs adaptations to accept these data
    - This action is subject to change in later project phases
- The “corporate identity manager” is responsible for this action.

Approve request
generic process example using petri nets

- Result of the conclave workshop 2007-06-27 - 28



agenda

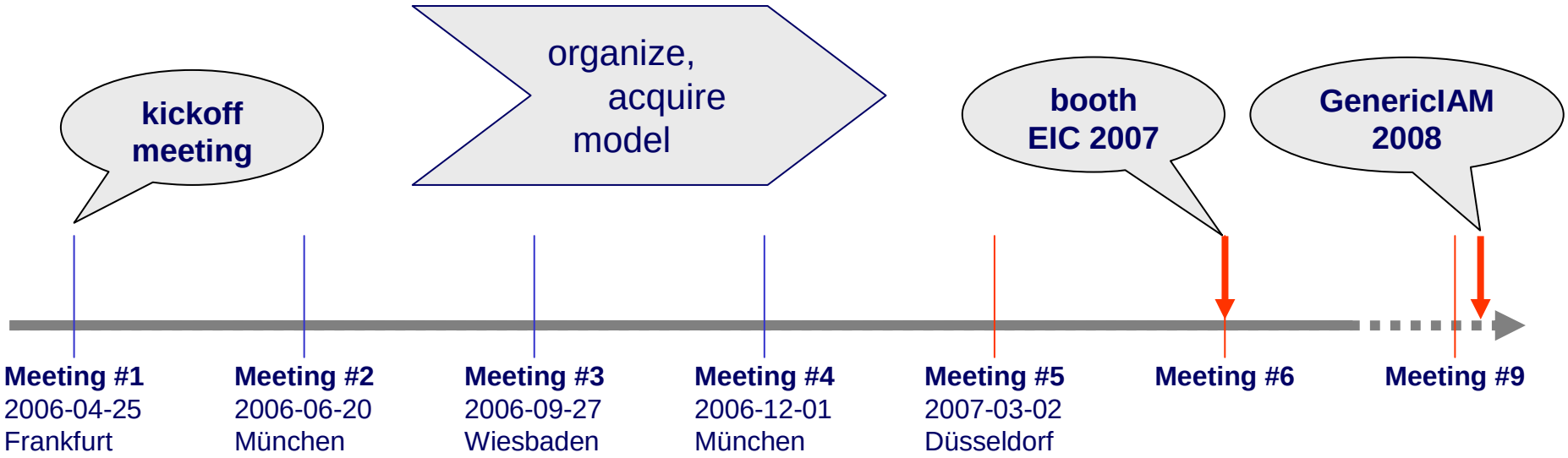
- ***Why?*** – Motivation for GenericIAM
- ***Where to?*** – The objective of the initiative
- ***Who?*** – Members of GenericIAM and their experiences
- ***How?*** – How we work
- ***What?*** – input & results
- ***When?*** – Yesterday, today and tomorrow

History & Orientation
Starting small & national, acting globally.

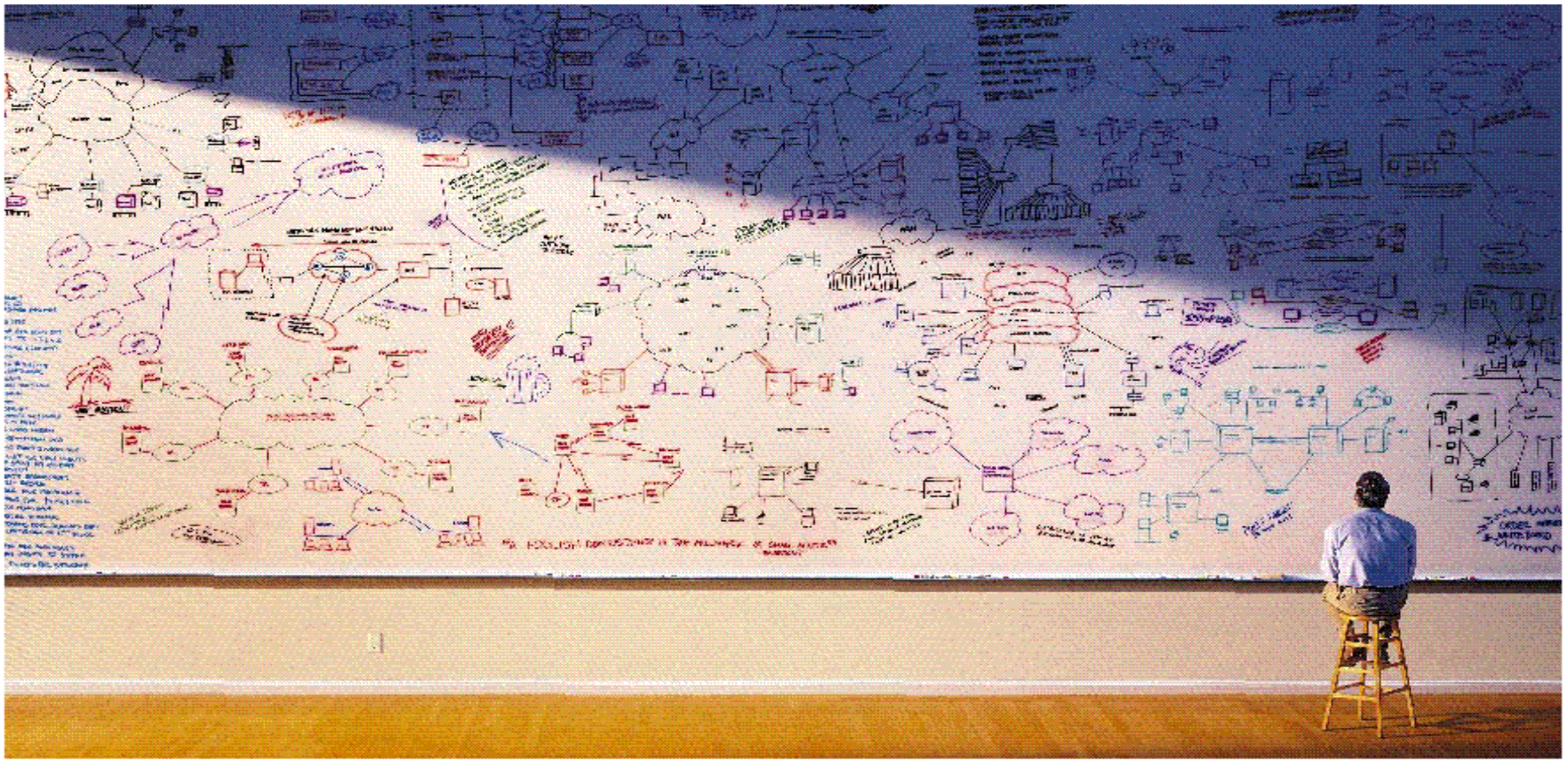
- GenericIAM started in Germany in May 2006.
- GenericIAM is set up as a competence center within **NIFIS** e.V..
- After one year (~ May 2007) we decided to internationalize our work.
- We synchronized our actions with **The OpenGroup** so far.
- We are in talks with several other standardization bodies and focus groups: ITU-T, enisa, more …
- Our first results will be delivered in 2008.
- From then on we will publish them yearly.
- An appropriate success provided, we will feed our results to an established international standardization body.

When?
Yesterday, today and tomorrow

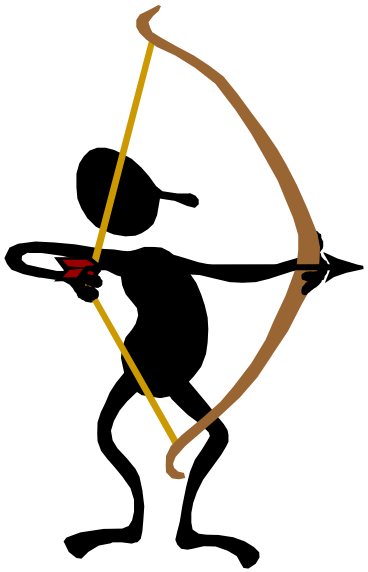
- We met for the first time in Q1/2006 triggered by a call for meeting published in a Kuppinger, Cole + Partner newsletter.
- Since then we meet quarterly.
- We will deliver the first results in Q1/2008.

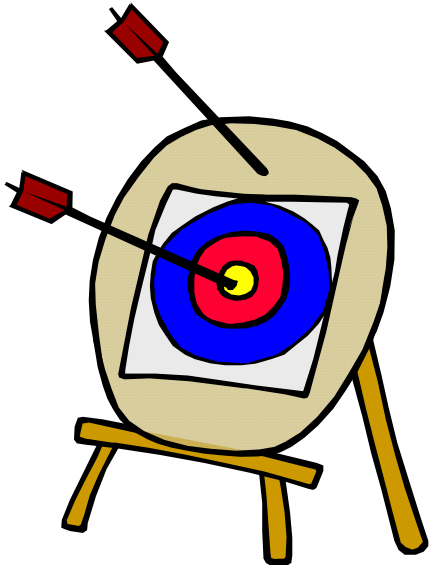


Questions – Comments – Suggestions?



The end ...





Thank you very much for your attention!

In case of any questions:
horst.walther@nifis.org,
skype: HoWa01

VoIP: +40 40 414314453

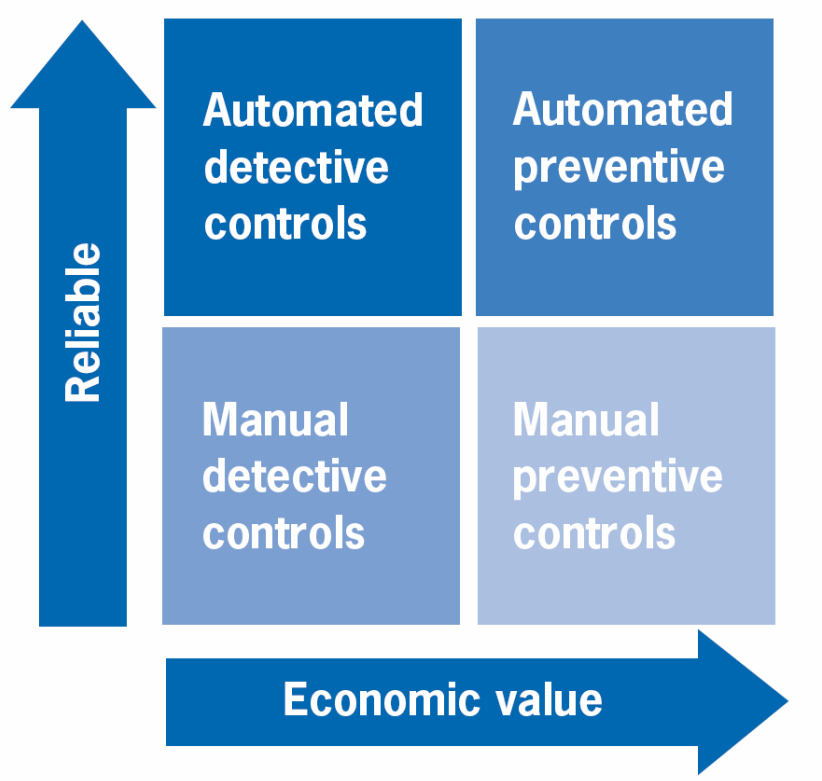
quoted literature

- **[McMenamin84]**
  Stephen M. McMenamin and John F. Palmer, *Essential Systems Analysis*, Yourdon Press,1984, Chapters 1 through 4. See also: Ed Yourdon, *Modern Structured Analysis*, Yourdon Press, 1989, Chapter 17
- **...**

Attention

Backup slides

GRC controls
detective vs. preventive – manual vs. automated



- controls can be classified as preventive or detective.
  - They either prevent errors before they occur or
  - They detect errors after they have occurred but in time to correct them before they do real damage.
- Both types of controls are important.
- preventive controls are preferred to detective ones.
  - detective controls act after an error has occurred, this means that the undetected errors go on to have a negative impact on the business.
  - preventing errors is cheaper than to detecting and fixing them.
- Preventive controls generally have a higher “economic value” to an organization.
- detective controls may enable an acceptable control environment to meet minimal requirements.
- To improve the bottom line a proper balance of detective and preventive controls is necessary.

GRC controls
examples in 4 categories

Examples of **detective** and **preventive** controls

- Detective Controls are designed to identify an error or exception after it has occurred. Examples include:
  - Exception reports
  - Reconciliations
  - Reviews of operating performance
  - Periodic inventories
- Preventive Controls focus on preventing errors or exceptions. Examples include:
  - Use of checklists
  - Training
  - Proper segregation of duties
  - Authorization levels/approvals

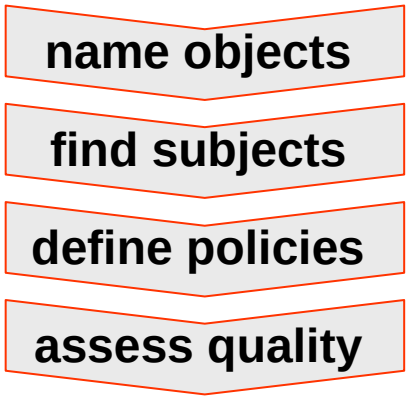
Examples of **manual** and **automated** controls

- Manual Controls operate through human intervention. They are the most flexible but are also subject to human error. Examples include:
  - Comparison of amounts entered to source documents
  - Signatures/initials noted on completed documents
  - Budget-to-actual reviews
  - Re-performance of computations
- Automated Controls operate through and within information technology systems. They function systematically and work with a high degree of consistency. Examples include:
  - System access controls
  - Data entry requirements prior to transaction processing
  - Automated balancing and reconciliations
  - Automated flags that identify possible invalid or duplicate entries/data

Introducing IAM – project or process?

implementing Identity Management is no one-off business

--- initial **project** ---



- Initial project
  - IdM cannot be introduced by a single project
  - But an **initial organisational framework** has to be set-up up-front.
  - Definition of the basic **objects** and the **subjects** operating on them.
  - Definition of access **policies** and
  - Assessing the existing data's **quality**

--- ongoing **process** ---

- Ongoing process
  - The initial set-up has to grow in a **step-wise** approach.
  - IdM must have a common ownership
  - Process quality must be controlled in a PDCA life cycle
  - The process does the Maintenance of policies, objects, subjects, actions & processes.

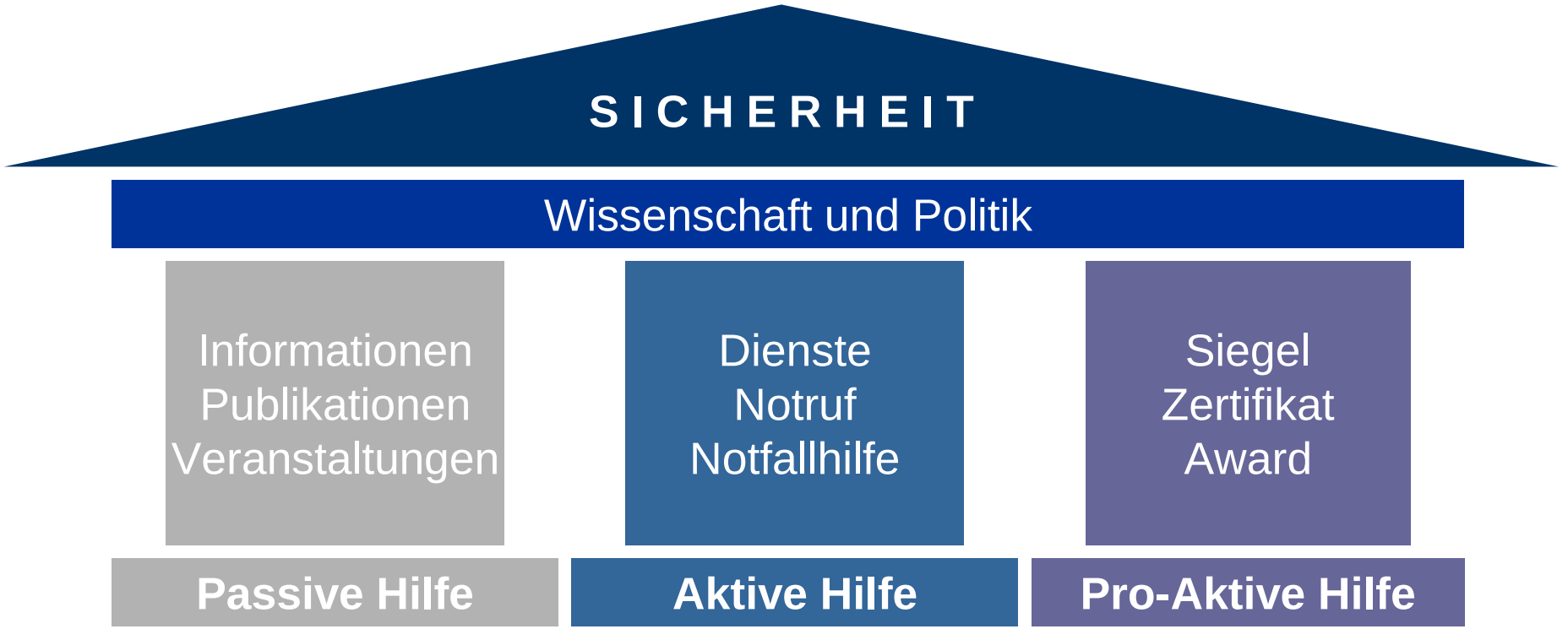
Die NIFIS im Überblick

- Nicht gewinnorientierter, eingetragener Verein
  - Motto - „aus der Wirtschaft für die Wirtschaft“
  - Position - „neutrale, herstellerunabhängige Institution“
- Gegründet im Juni 2005 mit Sitz in Frankfurt am Main
- Mitglieder (Auszug):

Fraport, SIEMENS, DEKRA, OKI PRINTING SOLUTIONS, KPMG, interxion, Magirus IT advisorygroup, COMPUWARE, controlware communicationssysteme, EVANGELISCHES KRANKENHAUS HAMM, clara.net, PRESECURE

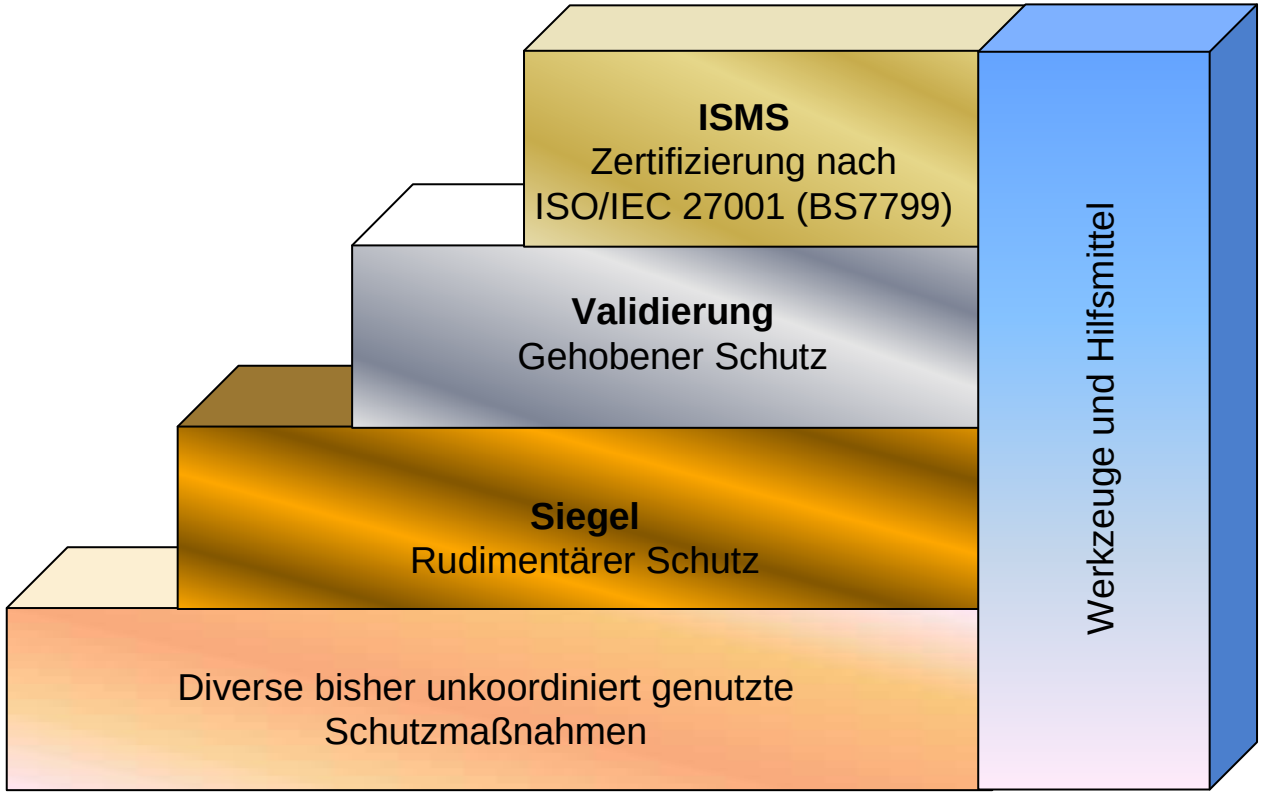
Der Sicherheitsbedarf in Unternehmen

Sicherheit beginnt nicht erst beim Virenscanner und hört auch nicht an der Firewall auf:



Die Sicherheitsstufen

Zwischen „keinem Schutz“ und einem „optimalen Schutz“ muss kein Vakuum sein:



Aufbau der NIFIS

Exekutivbeirat

- Fr. Dr. Krogmann MdB, CDU
- Hr. Otto MdB, FDP
- Fr. Stokar von Neuforn MdB, BÜNDNIS 90 DIE GRÜNEN
- Hr. Tauss MdB, SPD

Vorstand

Peter Knapp (Vors.)
Dr. Thomas Lapp (stellv. Vors.)
Brad Chapman
Mathias Gärtner

Wissenschaftlicher Beirat

- Hr. Prof. Dr. Heckmann
- Hr. Prof. Dr. Herberger
- Hr. Prof. Dr. Merle

Mitgliederversammlung

NIFIS ist primär Kompetenzzentrum für

- Informations-Sicherheits-Management-Systeme
- Identity Management
- Business Continuity Management
- Datenschutz
- Flächendeckende CERT-Infrastruktur
- Förderung sicherer IP-Kommunikation in Unternehmensnetzwerken
- Sicherheit von Rechenzentren und Informationstechnologie
- Sicherheit von Software-Anwendungen
- Sicherheit von VoIP

Identity and Access Management Terminology

- **Access management.** Processes and technologies for controlling and monitoring access to resources consistent with governing policies. Includes authentication, authorization, trust, and security auditing.
- **Authentication**. A process that checks the credentials of a security principal against values in an identity store. Authentication protocols such as Kerberos version 5, Secure Sockets Layer (SSL), NTLM, and digest authentication protect the authentication process and prevent the interception of credentials.
- **Authorization**. The process of resolving a user's entitlements with the permissions configured on a resource in order to control access. Authorization in the Windows operating system involves access control lists (ACLs) on files, folders, shares, and directory objects. Applications such as SQL Server, SharePoint® Portal Server, and Exchange Server implement access control mechanisms on resources they manage. Application developers can implement role-based access control using Windows Authorization Manager or ASP.NET roles.
- **Credential**. Typically a piece of information related to or derived from a secret that a digital identity possesses, although secrets are not involved in all cases. Examples of credentials include passwords, X.509 certificates, and biometric information.
- **Digital identity**. The unique identifier and descriptive attributes of a person, group, device, or service. Examples include user or computer accounts in Active Directory, e-mail accounts in Microsoft Exchange Server 2003, user entries in a database table, and logon credentials for a custom application.
- **Entitlement**. A set of attributes that specify the access rights and privileges of an authenticated security principal. For example, Windows security groups and access rights are entitlements.
- **Federation**. A special kind of trust relationship between distinct organizations established beyond internal network boundaries.
- **Identity integration services**. Services that aggregate, synchronize, and enable central provisioning and deprovisioning of identity information across multiple connected identity stores. MIIS 2003 SP1 and the Identity Integration Feature Pack 1a (IIFP) for Active Directory provide identity integration services.
- **Identity life-cycle management**. The processes and technologies that keep digital identities current and consistent with governing policies. Identity life-cycle management includes identity synchronization, provisioning, deprovisioning, and the ongoing management of user attributes, credentials, and entitlements.
- **Identity store**. A repository that contains digital identities. Identity stores are usually some form of directory or database managed and accessed through a provider such as Active Directory or Microsoft SQL Server. Identity stores can be centralized, for example on a mainframe computer, or distributed; Active Directory is an example of a distributed identity store. They generally have well-defined schemas for what information can be stored and in what form it can be recorded. They usually incorporate some form of encryption or hashing algorithm to protect both the store and components of the digital identity, such as credentials. Older and custom identity stores may not have such strict security mechanisms and may store passwords in plaintext (with no encryption).
- **Identity synchronization**. The process of ensuring that multiple identity stores contain consistent data for a given digital identity. This process can be achieved using programmatic methods such as scripts or through a dedicated product such as MIIS 2003 SP1.
- **Provisioning**. The process of adding identities to an identity store and establishing initial credentials and entitlements for them. Deprovisioning works in the opposite manner, resulting in the deletion or deactivation of an identity. Provisioning and deprovisioning typically work with identity integration services to propagate additions, deletions, and deactivations to connected identity stores.
- **Security auditing**. A process that logs and summarizes significant authentication and authorization events and changes to identity objects. Organizations will differ in their definition of significant events. Security audit records can be written to the Windows Security Event Log.
- **Security principal**. A digital identity with one or more credentials that can be authenticated and authorized to interact with the network.
- **Trust**. A state that describes the agreements between different parties and systems for sharing identity information. A trust is typically used to extend access to resources in a controlled manner while eliminating the administration that would otherwise be incurred to manage the security principals of the other party. Trust mechanisms include cross-forest trusts in Windows Server 2003 and trusts between realms using the Kerberos version 5 authentication protocol.

Roles, tasks, and operations
according to Microsoft

- A **role** …
  is a set of permissions that a user must have to do a job.
  - Well-designed roles should correspond to a job category or responsibility (for example, receptionist, hiring manager, or archivist) and be named accordingly.
- A **task** …
  is a collection of operations, and sometimes other tasks.
  - Well-designed tasks are inclusive enough to represent work items that are recognizable (for example, "change password" or "submit expense").
- An **operation** …
  is a set of permissions that you associate with system-level or API-level security procedures like WriteAttributes or ReadAttributes.
  - You use operations as building blocks for tasks.

- **Role definitions**
  The role definitions that are appropriate depends on the structure and goals of your organization. Roles support inheritance from other roles. To define a role, you specify a non-arbitrary name, a friendly description, and some lower-level tasks, roles, and operations that are part of it. This provides a mechanism for role inheritance. For example, a Helpdesk role might include a Product Support role.
- **Role assignments**
  A role assignment is a virtual container for application groups whose members are authorized for the role. A role assignment is based on a single role definition, and a single role definition can be the basis of many role assignments.
- **Task definitions**
  A task definition is smaller than a role definition and can be used to define roles and other tasks.
  You associate tasks with roles in an intuitive way. For example, the Recruiter role might include the Interview task. Tasks, like roles, are defined in a way that is appropriate to the organization. To define a task, you specify a name, a friendly description, and some lower-level tasks and operations that are part of it.
- **Operation definitions**
  Operations are small computer-level actions that are used to define tasks and are not relevant to an administrator. You define operations only in developer mode.