Identity & Access Management

Get in control: IT Governance, people, permission and technical challenges.

February 2009

Information Risk Control B.V.

Faculty Electrical Engineering, Mathematics and Computer Science

Master:	Computer Science
Specialization:	Information System Design

Thesis Project	
G. Koelewijn	(student, nr. 9452244)

Committee:	
Ir. B.R. Sodoyer	(professor)
Ir. H.J.A.M. Geers	(external professor)
R. Bakker	(irC2)
Prof.dr.ir. J.L.G. Dietz	(chair)

I. Preface

Organizations comprehend the risks of processing information with technology better, because of experience or because they are obligated to assess risk by law or regulation. One of the oldest and most basic measure for protecting the confidentiality and integrity of information is the control of access to data and functionality. Although access control is a very old principle, today it’s still one of the largest challenges of securing information processing.

In this research, it becomes clear why the simple principle of controlling access to information and functionality is very complex to implement and manage in larger organizations. With this research I tried to gain insight in how IT Governance, people, permission and technology are related together in reducing risks to an acceptable level by using access control.

Acknowledgements

This research is made possible by performing consultancy assignments in large organizations where the necessary experiences and deliverables contributed to the end result. I want to thank my employer Remco Bakker of Information Risk Control B.V. (irC^2) for giving me the opportunity to perform these assignments and allowing me to use deliverables for this research. The deliverables are generalized and made anonymous for this purpose.

Thanks go out to my supervisor ir. B.R. Sodoyer, for the pragmatic guidance on writing this thesis.

I want to thank my wife and daughters for the happy and loving distraction from this research and for their enormous patience.

II. Table of Contents

III. Summary

Identity and Access Management (IAM) is about managing "Who has permission to do what on which data and why?" at technical and process level. This is a very complex problem for organizations, because of heterogeneous technology and complex processes. Together with the continuous change in organizations, managing "Who has permission to do what on which data and why?" is a real challenge. (For example: change of working processes, change of people, change of jobs, change of information systems or change of the organization when merging with other organizations.)

Current insights, based on practical experience, reflect that IAM is 20% about technology and 80% about processes and IT Governance. In general IT governance literature and frameworks, IAM is only a small topic. IAM specific literature is often only about technology, of course with a few exceptions. One may conclude a gap exists between IAM technology and IT governance literature/frameworks. In short, this research will try to:

> *"Close the gap between IAM technology and general security or IT governance frameworks."*
>
> *This knowledge will enable organizations to establish IAM more efficiently, without having to go through every known pitfall.*

The research is performed in 7 chronological steps:

1. Using the results of the literature study on COBIT as guidance in practical applications. (Chapter 2.)
2. Setting the research environment and boundary by a general introduction to the term Identity and Access Management as it will be used in this research. (Chapter 3.)
3. Developing insight in why organizations want to implement an IAM process and how IAM will be used to their benefit. (Chapter 4.)
4. Creating a generic IAM process model based on the literature study, former chapters and practical experience. (Chapter 5.)
5. Business Case: an assignment to implement an IAM process in a large organization. The process model is used as a starting point for this assignment. (Chapter 6 to 12.)
6. Compare theory to practical experiences gained in the business case. (Chapter 13.)
7. Ideas for further research (Chapter 14.)

These steps will be discussed in short below.

(1.) In the 'research assignment' an analysis of relationships between the IAM process and other IT processes is performed, based solely on literature (COBIT). The result of this research is used as starting point of this research.

(2.) The term "identity and access management" is very broad and used in various contexts, for technical solutions and for management processes as well. In this paper, identity and access management is defined as the activities and tools that manage identity and access through their lifecycle. For a typical implementation in an organization, this includes processes, procedures, administrations and software.

The scope of identity and access management in this paper is the organization. Identities related to the organization (employees, clients, partners, etc.) with access to resources related to the organization. Within this context, the process of building an identity and access management structure can be viewed from governance to technical perspective.

(3.) Common business drivers for IAM are: Security, Compliancy, Improving service and Cost reduction. The motivations for identity and access management can be conflicting with each other. Security and cost reduction for example, can be conflicting at first sight. Prioritizing and balancing business needs is prerequisite for any identity and access management project, while this can have enormous impact on processes and technology implemented later on.

(4.) The management of access generally consists of the activities appointed below. The actual implementation of these activities in processes and procedures can be very different in various organizations.

1. managing identity information
2. defining and modifying permission
3. assigning or closing permission
4. reviewing and reporting on permission modification, assignment or closure

Correct alignment of these activities on organizational and technical level is crucial for successful management of access.

(5.) The business case is an assignment executed for a large (+40.000 identities to manage) international organization, with the goal to implement an IAM process. The IAM technology was already implemented by another party. The final deliverable of this project is included in this thesis, the chapter names that are part of this deliverable are prefixed with [BC]. The deliverable is a design of the IAM process and must include the following items:

- IAM process requirements (set by stakeholders);
- the procedures and relationships between them (process flow);
- needed input and expected output of procedures;
- responsibilities in the execution of procedures;
- dependancies in procedures;
- decision moments in procedures;
- controls and reporting.

In the final deliverable, the whole IAM process was divided and integrated in other IT processes. The processes that were described are: Change Management, Release Management and Role engineering as part of the Security Management process.

(6.) To summarize the conclusion regarding the IAM process model: it is very useful for dividing the complex structure of tasks into pieces that can be handled separately, but in practice the activities will often be part of other processes. The value and applicability of the term “IAM process” can be subject of discussion. The result of the ‘research assignment’ performed really well. This is remarkable for such a general framework (COBIT) that has such little explicit text in regard to IAM.

1 Introduction

People have permission to perform certain actions on information, very often stored in digital information systems. For example someone who owns a bank account and has subscribed to the online banking service, has the permission to do transactions with the online banking system. Or people have the permission to use certain information systems in organizations like email or accounting software, because of tasks that originate from their job description.

For many organizations, information is the greatest asset and is processed within information systems. Information should always be available when needed, should be exclusively available for authorized persons only and should contain what it's meant to contain. To be able to meet these criteria, an organization has to clearly define and manage which permissions are given to parties that interact with their information. At the level of the information system, the following question should be answered: "Who has permission to do what on which data and why?" An information system should therefore contain a structure to control and monitor the w-w-w-w.

1.1 Problem Analysis

Software developers started building mechanisms like user authentication (the "who") and access control (the "what" and "which data") in information systems already in the 1960s(1). Nowadays, almost every piece of software supports some form of user authentication and access control. But these technical mechanisms haven't solved the initial problem of defining and managing the permission of interacting parities.

The complex and dynamic working processes within organizations make it hard to clearly define what somebody's permissions are (the "why") on a certain moment in time. Subsequent management of the assigned permission in such a dynamic environment can be time consuming. The translation of these permissions to privileges on very heterogeneous components of information systems is very error-prone and time consuming. This is even made harder because of the poor standardization and interoperatibility in user authentication and access control mechanisms of software. And at last one of the most difficult things is dealing with change. For example: change of working processes, change of people, change of jobs, change of information systems or change of the organization when merging with other organizations.

There is a lot of literature on topics like access control, IT Governance, Security good-practices and identity and access management technology. In the last 6 years, the term Identity and Access Management became widely used and was a new name for concepts that already existed. But even though, the focus of organizations shifted from access control to a wider scope, were the management of identities and provisioning of identity information got more attention.

The market followed closely with new product suites (often constructed by acquiring software companies or rebranding existing synchronization software) that could connect to many heterogeneous systems and could provision identity and access information to these systems. With these products, central IAM and auditing of a heterogeneous environment became possible on a technical level.

Many technical solutions for IAM engaged the market, but at the moment organizations begin to realize that IAM is only 20% about technology and 80% about processes and IT Governance. In the literature, there still exists a gap between technical IAM documentation and general security or IT Governance publications.

Wouldn't it be nice to have a summary of aspects that should be thought of when establishing IAM in an organization? At the moment a lot of IAM projects stall, because of forgotten prerequisites on the organizational level or because the focus is too much on implementing technology. With input from existing literature, like COBIT, ISO27000X and RBAC, combined with the use of business case(s), such a summary can be made.

In short, this research will try to:

"Close the gap between IAM technology and general security or IT governance frameworks."

This knowledge will enable organizations to establish IAM more efficiently, without having to go through every known pitfall.

2 Starting Point

In the ‘research assignment’ an analysis of relationships between the IAM process and other IT processes is performed, based solely on literature (COBIT). The result is a list of 11 IAM core activities, with a total of 28 relevant relations to other processes. These relationships can be regarded as prerequisites for an organization wanting to implement an IAM process. They give an overview of what should be implemented on the process and governance level, to enable effective IAM. The following text is quoted from COBIT 4.1 and gives a very short introduction to COBIT.

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT’s good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The COBIT control framework contributes to these needs by:

- *Making a link to the business requirements*
- *Organising IT activities into a generally accepted process model*
- *Identifying the major IT resources to be leveraged*
- *Defining the management control objectives to be considered*

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

In this research project, this list will be challenged in practice. Intuitive questions like: “Is the list complete?”, “What are the most important items and for which application?”, “Are they a required relationship?” are examined by analyzing a business case. In the end, new findings could result in refinement of the current literature and a useful overview for organizations that are implementing an IAM process.

The research is performed in 7 chronological steps:

1. Using the results of the literature study on COBIT as guidance in practical applications. (Chapter 2.)
2. Setting the research environment and boundary by a general introduction to the term Identity and Access Management as it will be used in this research. (Chapter 3.)
3. Developing insight in why organizations want to implement an IAM process and how IAM will be used to their benefit. (Chapter 4.)
4. Creating a generic IAM process model based on the literature study, former chapters and practical experience. (Chapter 5.)
5. Business Case: an assignment to implement an IAM process in a large organization. The process model is used as a starting point for this assignment. (Chapter 6 to 12.)
6. Compare theory to practical experiences gained in the business case. (Chapter 13.)
7. Ideas for further research (Chapter 14.)

On the next page the relationships between the IAM process and other IT processes are summarized in a table.

This table is a summary of the 28 relevant process relationships that enable identity and access management in an organization, as found in the COBIT model. In the left column the processes, activities and output is stated that is relevant to the IAM process. In the middle column the process is stated that holds the core IAM activities. Note that COBIT doesn't identify IAM as a stand-alone process, but as part of the 'DS5 Ensure Systems Security process'. In the right column the processes, activities and input (from the IAM process) is stated that is relevant to the IAM process.

PO2 Define the Information Architecture PO2.1 Enterprise Information Architecture Model ➔ Information architecture PO2.3 Data Classification Scheme ➔ Assigned data classifications 16.Define the Information Architecture 17.Create data classification scheme 18.Assign data owner	**DS5 Ensure Systems Security** DS5.1 Management of IT Security DS5.2 IT Security Plan 12.Management of IT Security, so that security actions are in line with business requirements 13.Translate business, risk and compliance requirements into an overall IT security plan ***DS5.3 Identity Management*** ***DS5.4 User Account Management*** *1.Uniquely identify all users and their activity on IT systems* *2.Enable user identities via authentication* *3.Make user access rights to systems and data in line with business needs* *4.Attach job requirements to user identities* *5.User access rights requested by user management* *6.User access rights approved by system owner (and/or data owner)* *7.User access rights implemented by security-responsible person* *8.Maintain user identities and access rights in a central repository* *9.Create user account management procedures that apply for all users* *10.Contractually arrange the rights and obligations relative to access to enterprise systems and information for all types of users* *11.Regular management review of all accounts and related privileges* DS5.5 Security Testing, Surveillance and Monitoring DS5.6 Security Incident Definition 14.Test and monitor the IT security implementation in a proactive way 15.Create security incident definitions	➔ Security incident definition **DS8 Manage Service Desk and Incidents** DS8.1 Service Desk 23.Establish a service desk function, which is the user interface with IT
PO3 Determine Technological Direction PO3.4 Technology Standards ➔ Technology standards 19.Create technology standards		➔ Specific training requirements on security awareness **DS7 Educate and Train Users** DS7.1 Identification of Education and Training Needs 24.Educate and Train Users
PO9 Assess and Manage IT Risks PO9.4 Risk Assessment ➔ Risk assessment 20.Assess risk		➔ Process performance reports **ME1 Monitor and Evaluate IT Performance** ME1.4 Performance Assessment 25.Monitor process performance
AI2 Acquire and Maintain Application Software AI2.4 Application Security and Availability ➔ Application security controls specification 21.Address application security and availability requirements		➔ Required security changes **AI6 Manage Changes** AI6.2 Impact Assessment, Prioritization and Authorization 26.Manage Changes
DS1 Define and Manage Service Levels DS1.4 Operating Level Agreements ➔ Operating level agreements 22.Define Operating level agreements		➔ Security threats and vulnerabilities **PO9 Assess and Manage IT Risks** PO9.3 Event Identification 27.Assess risk
		➔ IT security plan and policies **DS11 Manage Data** DS11.6 Security Requirements for Data Management 28.Create security requirements for data management

Table 1. COBIT – IAM process relationships

COBIT Domains

PO = Plan and Organize
AI = Acquire and Implement
DS = Deliver and Support
ME = Monitor and Evaluate

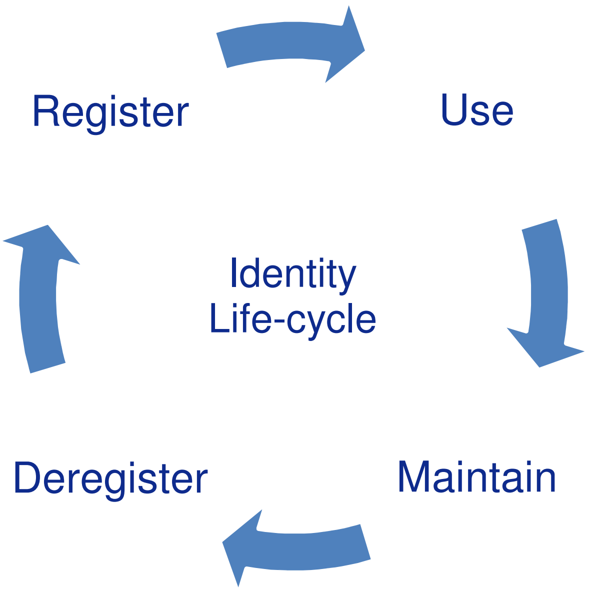


Figure 1

3 Introduction to IAM

3.1 Concept of the Identity

"A digital identity[1] contains data that uniquely describes a person or thing (called the subject or entity in the language of digital identity) but also contains information about the subject's relationships to other entities." (2)

In a typical organization, an identity goes through various stages. The identity comes into existence when a subject is registered in an information system and should be discarded on determined criteria. These stages can intuitively be modeled in a lifecycle, the identity lifecycle. In Figure 1 an identity lifecycle is given with 4 stages of processes that are involved.

3.1.1 Register

The registration stage mainly contains administrative processes, in which an information system is populated with identity and attributes of the identity. The identity is the established relation between the entity and the registration. Within the scope of the registration, it is uniquely described by its attributes.

An important aspect in this process is the level of trust that can be given towards the attributes of the identity. The attributes are assertions about the entity. Decisions in business processes could be based on these assertions. For example decisions about system access, based on job title or project membership. Trust levels can be determined in the registration procedure and the degree in which identification of the entity and verification of the attributes should be performed can be related to these levels.

The security requirements for the administrative processes and related information systems should reflect the risk involved with managing identity information on these systems. A risk assessment will give insight in the risks that are specific for the process environment.

[1] In this paper, the term 'identity' is referring to the term 'digital identity' as defined here.

On a technical level, the identity data is propagated to systems in which the data is needed. For example, the creation of accounts on systems for which the identity should be able to logon. With the use of Identity Management software, the propagation of identity data (e.g. the creation of an account) can be automated.

When accounts are created, they are secured with credentials that enable the identity to authenticate itself and should prevent the account from being used by entities other than the entity related to the identity. Examples of credentials are: a signature, a password, a digital certificate, a biometric template. In this stage, procedures for creating and issuing credentials are executed.

3.1.2 Use

Obvious use of identity information is when the entity logs on to a system to gain access to functionality and data, with an account that is related to the identity. Within information systems, the identity data can be used to relate other data objects to, for example bills or payrolls.

3.1.3 Maintain

Identity information is subject to change. For example when characteristics of the entity change and the attributes of the identity are updated accordingly. Some common characteristics are: telephone number, job title or service subscription. The administrative processes deal with changes in identity information or the users can change certain attributes themselves by using self-service applications. One of the most well-known examples of self-service is a password reset application, which enables the user to reset its own password.

On a technical level, the relevant changes are propagated to the systems that contain the identity information. When attributes of the identity are used to decide about system access, changes in attributes could for example result in accounts being added or deleted on certain systems. But, the systems itself change too: new, updated or discarded systems. This could have an effect on the identity information and administration, when attributes are recorded that have a system dependant meaning.

Maintenance of identity information can be seen as a change process that contains procedures for processing changes that result from: changing characteristics of the entity, changes in processes or the organization and changing systems. When identity information is regarded in respect to access management, the change process will need to deal with changes related to permission and system privileges too.

3.1.4 Deregister

Deregistration is the last stage, in which the identity is discarded. There are various reasons why an identity should be discarded, but the withdrawal of access related to the identity is the most important one. In an organization where an employee has access to information systems, the accounts should be discarded when the employee changes job or leaves the organization. Other reasons are preventing clutter of unused identity information and efficient use of system resources.

The procedures that handle deregistration can be rather complex. The procedures for deregistration should start on predefined criteria. It should be clear why and when identities should be discarded. All administrations where this identity is registered should deregister. The identity information should be removed or marked ‘inactive’ in all related information systems. All related accounts should be removed or deactivated. All credentials should be withdrawn. All data that is related to the identity should be dealt with. For example, what to do with files in personal directories, after an employee leaves the organization? Identity management software could automate certain procedures, but often a lot of manual work is needed.

3.2 Concept of Access

Access, in the context of information technology, is the ability to use resources or services within information systems. More specifically, the fact that an identity has permission to perform certain actions results in privileges on systems that give the ability to perform those actions. The permission associated with an identity is access defined in functional terms. Privileges are technical statements in system dependant terminology that create the ability to access resources and services. Privileges are usually associated with an account, related to the identity.

Access is related to the identity on two levels. On the first level permission is recorded in the identity administration. On the second level, accounts with privileges are created on the systems. Between those levels, various access control models can be used to perform access control. The most well known model is Role Based Access Control (RBAC), in which permission is modeled with roles and roles are assigned to identities. This paper will discuss access control independent of the model, but specifics for RBAC will be given too.

The association of permission with an identity goes through various stages. Access is requested for an identity, the request is validated and assessed, when granted access is assigned to the identity and access should be closed on determined criteria. These stages can intuitively be modeled in a lifecycle, the access lifecycle. In Figure 2 an access lifecycle is given with 4 stages of processes that are involved.

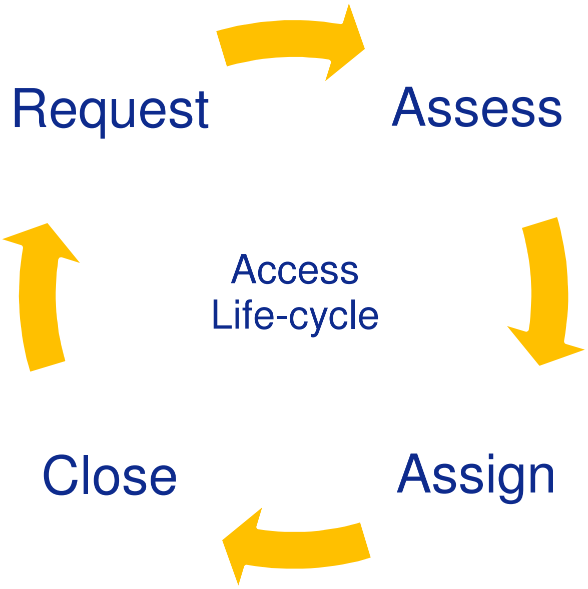


Figure 2

3.2.1 Request

In the request procedure information is gathered to support the assessment, assignment and closure of access. For organizations where permission of many employees needs to be managed, the following information items are commonly processed in the request procedure:

- the identifier of the requested permission,
- the identity for which the permission is requested,
- the identity of the requester,
- the reason or need for assigning permission,
- a risk assessment,
- the approvals needed (information or system owners),
- the criteria for closure.

In the next phases, the use of these common items will be discussed.

3.2.2 Assess

The consequence of assigning permission to an identity needs to be assessed, before the request can be granted. In obvious cases, like access to a web forum, the only assessment that takes places is validating the email address of the identity. In more complex organizations, the risk associated with "Who has permission to do what on which data and why?" needs to be assessed and compared to the reason or need for the requested permission. If the risk is acceptable compared to the business need, then access can be granted. To be able to perform this assessment the requested permission, the identities and the business need have to be recorded in the request procedure. The risk has to be assessed by competent people. The responsibility of the actual decision about granting access has to be set down. In practice the responsible parties are often the information and system owners.

This whole procedure is in practice optimized by performing it once for a type of user or role in combination with certain permission, and then reapplied to similar requests. For example, when an organization using RBAC has the role 'Teller' with associated permission to access the point-of-sale software, this role is assessed once and automatically assigned to all tellers in the organization. But, most organizations are not structured enough to be able to use fixed roles for each job description. Therefore the procedure still applies for assessing requests for permission that is not part of the role model. For example, permissions or tasks that are not repetitive and not applicable to multiple employees. Very complex permissions, such as needed by system administrators or engineers, often are left out of the role model too.

3.2.3 Assign

Assigning permission to an identity is an administrative action. The actual creation of privileges and accounts on the system level is done by system administrators or automatically by identity and access management software. The most important aspect is the relation between permissions and privileges. How do system administrators know which privileges to create?

Permissions are requested, assessed and granted, but privileges define actual access to the resources and services. The privileges should carefully reflect the permission that is granted. For a web forum, the technical statement could just be a bit in a database column that permits the user to create topics. The relation between the permission 'create topics' and the privilege 'bit in a column' is straightforward. In organizations with complex information systems, there could be thousands of such relations. For access control to be effective, these relations must be carefully managed supporting the communication between business (functional terms) and IT (technical terms).

3.2.4 Close

An important but often forgotten procedure in the access life-cycle is the closure of access. A common security problem in organizations is the fact that employees only gain more access and access is never closed when there is no need for it anymore. For example, an employee who has had various jobs within the organization and still can use the accounts and privileges that belonged to previous jobs[2]. Another common security problem in organizations is the fact that access is not closed when an employee or temporary employee leaves the organization. This uncontrolled access enables misuse of resources or fraud, which could be a great risk for an organization. If uncontrolled accounts are shared with others or reassigned to other identities, control over access to systems is lost, resulting in even more risk. For the web forum example, these accounts just consume extra resources and a criterion for removal is the period of inactivity.

The closure of access can be handled by procedures that are carried out on predefined events, such as employees quitting or switching jobs, or by periodic checks on the permission administration and accounts with privileges on systems. These procedures can be made much more effective if criteria for closure are included in the request for permission. The applicability of these criteria can be monitored and access can be closed when they apply. These criteria make it possible to automate the monitoring and closure procedures with identity and access management software.

3.3 Identity and Access Management

The term “identity and access management” is very broad and used in various contexts, for technical solutions and for management processes as well. In this paper, identity and access management is defined as the activities and tools that manage identity and access through their lifecycle. For a typical implementation in an organization, this includes processes, procedures, administrations and software.

The scope of identity and access management in this paper is the organization. Identities related to the organization (employees, clients, partners, etc.) with access to resources related to the organization. Within this context, the process of building an identity and access management structure can be viewed from governance to technical perspective.

[2] This phenomenon is called ‘authorization creep’.

4 Business Drivers

Why should an organization invest in identity and access management? Are current activities, such as creating accounts and assigning privileges not sufficient? This is of course dependent of the current state, specific environment and needs of the organization. But, there are common motivations for investing in identity and access management, which can be more or less applied to every situation. These motivations are called business drivers and will be discussed in the following paragraphs.

4.1 Security

The most intuitive motivation for having a formalized identity and access management process is security. The impact of unauthorized use of information systems, compromising the confidentiality, integrity or availability of information can be really damaging to an organization.

Organizations want to control and manage this risk, by implementing security measures. One of the oldest and most widely adapted security measure is controlling access to information systems. But, ad hoc and poorly-managed access control will not reduce risk and possibly hinder the primary activities of the organization. Common examples are the existence of active accounts and privileges on systems, which belong to an employee that has quit or changed to another job, or confidential information which is well protected in a financial application, but widely accessible in a reporting application.

Prerequisite of being able to manage risk is being able to manage and monitor "who has permission to do what on which data and why", in which balance is found between the risk of access (who, what and which data) and business need (why). Well implemented identity and access management puts the business in control of the level of risk that is accepted.

Some concrete actions that enable risk reduction by identity and access management are:

- establishing the needed level of trust by: identification of the entity in identity administration procedures and securing the identity with authentication,
- ensuring the integrity of identity data,
- granting access only on business need,
- evaluating risk,
- ensuring the actual system privileges reflect the intended permission,
- ensuring access to information and services is consistent between all systems,
- ensuring access is closed when the business need does not apply anymore,
- monitor and review permissions and privileges.

4.2 Compliancy

The term compliancy is shorthand for organizations complying with regulations or standards. Regulations are dictated by governments for certain organizations and have an impact on the requirements for information security. In the following list, some examples of regulations are given.

- In The Netherlands, government institutions have to comply with the 'Besluit voorschrift informatiebeveiliging rijksdienst 2007' (3). These regulations require the application of information security management and risk analysis, to ensure the confidentiality, integrity

and availability of information. A method to comply with this regulation is certification for the ISO27001 standard (Information Security Management System).
Access to information and services can only be aligned to security management, if access is managed in a structured and controllable way: Identity and access management.

- In the US public companies[3] have to comply with the Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX. Section 404 which addresses internal control over financial reporting, relates implicitly to IT control, because the reliability of financial reporting is heavily dependent on a well-controlled IT environment.
  Identity and access management is an important aspect of a controlled IT environment. The IT Governance Institute has published a research paper called: "IT Control Objectives for Sarbanes-Oxley" (4). In this paper IT control is linked to SOX, where system security and access control are important aspects for reliable financial reporting.
- Also in the US, thousands of organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The Security Rule is a key part of HIPAA -- federal legislation that was passed into law in August 1996. The overall purpose of the act is to enable better access to health insurance, reduce fraud and abuse, and lower the overall cost of health care in the United States.(5)
  HIPAA dictates security requirements for electronic protected health information (EPHI), such as a security management process, facility access controls, access control, audit controls, person or entity authentication, transmission security.

These regulations all dictate some form of controlled information security. While SOX is very broad and implicit in respect to information security, HIPAA is literally stating security measures. Identity and access management is often related to compliancy as an implicit requirement from these regulations. Current technical solutions focus on supporting compliancy by implementing functionality, such as: logging and auditing, separation of duty (reliable financial reporting) and predefined compliancy checks. A more in depth discussion of this implicit requirement can be found in numerous articles about the topic[4].

4.3 Improving service

Fast and effective service is most important for organizations where identity and access management is supporting their primary business process. For example, application service providers that are offering different services to many customers, or large banks that have numerous employees working with confidential data. An effective identity and access management process will enable the organization to serve more customers and improve scalability, by structuring and automating assignment and closure of permission. In case of the bank, employees don't have to wait a long time for their accounts to be created and permissions to be granted, which in practice could take weeks.

Technical solutions that can improve service are:

[3] A public company usually refers to a company which is permitted to offer its securities (stock, bonds, etc.) for sale to the general public, typically through a stock exchange. [Wikipedia]

[4] Article about identity and access management, SOX and the Dutch 'Code Tabaksblat': Bart de Best. "SOX en Code Tabaksblat: tijd voor identity management?" (8)

- Automated propagation of identity and access data to systems, applications and services, allowing very fast creation, modification and removal of accounts and privileges.
- Single sign on, the ability for the user to authenticate once and use various systems and applications, without having to authenticate again.
- Password reset, the ability for the user to reset forgotten passwords efficiently, without having to consult various system administrators or a service desk. Renewal of other credentials, such as certificates on smart cards, falls into the same category.
- Self service, the ability for the user to administer his/her own identity information, allowing for fast adoption of changes if the user whishes to do so. (E.g. location, address, etc.)
- Workflow, the ability to automate identity and access management procedures, while putting the responsible users in control of decisions. This enables fast execution of identity and access management procedures, which can improve performance of the whole process.

The fully automated process is often referred to by vendors of identity and access management products as the great benefit of implementing their product. (6)

4.4 Cost reduction

The management of identity and access takes a lot of time and resources on various levels of the organization. When the identity and access management processes are formalized and more mature, large parts can be automated by software available on the market. Given that most organizations already managing identities and access on heterogeneous systems, efficiency can be gained by formalizing and automating the process.

But, this does not work the other way around: software will not formalize and mature the identity and access management processes by itself. Cost reduction by gaining efficiency with automated procedures is not guaranteed. The investment needed to improve or implement identity and access management processes and technology is very dependant of the current state of processes and technology. It is difficult to oversee the total implementation costs, the current state of processes and technology has to be assessed from identity and access management point of view.

4.5 Conclusion

Each motivation can be more or less important depending on the specific organizational environment. A bank will focus on compliancy and security, taking efficiency and cost reduction as secondary conditions. An application service provider will focus on efficiency and cost reduction, taking security and compliancy as secondary conditions.

The motivations for identity and access management can be conflicting with each other. Security and cost reduction for example, can be conflicting at first sight. Prioritizing and balancing business needs is prerequisite for any identity and access management project, while this can have enormous impact on processes and technology implemented later on.

5 Identity and Access Management Process Model

The management of access generally consists of the activities appointed below. The actual implementation of these activities in processes and procedures can be very different in various organizations.

1. managing identity information
2. defining and modifying permission
3. assigning or closing permission
4. reviewing and reporting on permission modification, assignment or closure

Correct alignment of these activities on organizational and technical level is crucial for successful management of access. For this reason, the organizational and technical aspects of the whole identity and access management process will be described in the following paragraphs.

5.1 Needs and requirements of the organization

Access should only exist, because the organization has a clearly defined need for it. This principle must be pursued when defining, assigning and closing permissions. On execution of these activities the following question will rise repeatedly: “Who has permission to do what on which data and why?” The answer to this question must be given by the organization, based on need and risk as stated earlier in paragraph 4.1.

One of the most important aspects is following a standardized method, in which the relation between need of the organization and technique is continuously tuned. In this relation, the translation is made from the permissions defined by the organization, to technical system dependant privileges. In the end, these privileges determine the actual actions a user can perform.

The total process must comply with the requirements, which are defined by the organization for the process and related information systems. The commonly acknowledged requirements are:

- effectiveness, the degree in which the process must realize the objectives of the organization;
- efficiency, the degree in which time and resources may be used for the execution of the process;
- verifiability, the degree in which information has to be delivered that enables verification of the requirements;
- confidentiality, the degree in which the processed information must be protected from unauthorized disclosure;
- integrity, the degree in which the processed information must be accurate and complete;
- availability, the degree in which the processed information must be available when required.

5.2 Managing identity information

The management of identity information is an activity in which the basis is formed for access: the identity with accompanying attributes. The identity is translated to accounts on the system level and the permissions to be assigned can be deducted from attributes of the identity, such as job description, department, projects and tasks or can be assigned directly to the identity.

In practice, one or multiple administrative processes managing identity information already exist. For example: Human Resource Management, Customer Relationship Management or Supplier Relationship Management. These processes can be tailored for connecting to the overall identity and access management process, provided that information is consistent and well managed within these processes. In this case, existing administrative processes will register and administer the access needs of the organization in terms of identity and permission. It's important to realize that these administrations will have direct impact on access to information and services. An assessment of the security requirements (CIA[5]), which are postulated by the organization for the administrative processes, will make clear if the requirements should be tightened.

5.3 Defining and modifying permissions

This activity will define and modify access in terms of the organization and processes. These definitions reflect the need for access of the organization, for example the permission to 'do salary payments' or 'access sales reports'. These definitions must determine what someone can do on which data.

The permissions are often related to task and job descriptions. If Role Based Access Control is used for modeling access, permissions are aggregated into roles. These roles do not only define what someone can do on which data, but often define who this role should be assigned to by naming the role to a job, project group or department. The role will be assigned to every identity that has attributes that match the department or job name.

5.3.1 Management of standard criteria

Permission is often related to task or job descriptions. Based on a standard criterion permission can be assigned to an identity, if the attributes of the identity correspond to the requirement of the criterion. If the standard criterion is linked to the definition of permission, for example permission that is always granted to a certain job, department or project member, permission can be granted very efficiently. Once permission is evaluated and granted, granting permission to others who match the criterion can be done without thorough evaluation. Granting permission based on standard criteria is easier to automate and maintain. It does introduce an extra dimension to defining and modifying permission: job descriptions, departments and projects do change a lot and definitions of permission and standard criteria have to be maintained.

If Role Based Access Control is used for modeling access, permissions are aggregated into roles. These roles do not only define what someone can do on which data, but often define who this role should be assigned to by naming the role to a job, project group or department. The role will be assigned to every identity that has attributes that match the department or job name.

An ideal automated implementation of Role Based Access Control does barely include manual interaction for granting or closing permission. In practice this is only realistic in organizations with very well structured job/permissions structures, such as large shop chains or production lines. In an office environment the need for access of the organization is less consistent and a more flexible procedure should be followed. Flexible in the sense that permission will be more often assigned on request and manually evaluated. The permission assignment in this procedure can deviate from the standard criteria. For these request and evaluation procedures more human interaction is needed.

[5] Confidentiality, Integrity, Availability

5.3.2 Technology

Within the management of permission the link with technology is contained. From technical point of view, applications and functions within applications are made available together with access control functionality. Take for example the permission to ‘do salary payments’, on the technical level accounts have to be created on systems with privileges that enable salary payments.

Technology, such as applications, functions within applications and access control functionality is likely to change. New applications are introduced, current application are changed or get replaced. Continuous tuning of the dynamic relation between the need of the organization and technology is one of de most critical aspects in the activity ‘Defining and modifying permissions’.

The permission-privilege matrices should be considered as part of the functional requirements of a system and documented accordingly. Changes to these matrices have to be managed by change management procedures, including functional testing and formal approval.

5.3.3 Constraints and Segregation of Duty

For critical activities in an organization a higher form of regulation can be required, to prevent fraud or to split the responsibility of a high risk transaction over multiple persons. To do this, the organization can define rules that constrain the assignment or activation of permission. Some common constraints are:

- An identity can not be assigned both permission A and B.
- An identity can have permission A and B, but can’t use both within one transaction.
- An assigned permission is only active in a defined period or for a defined duration.
- An assigned permission will be closed after a defined period.

When modifying permission, regardless if the change request originated from the organization or technology side, constraints should not be violated. Even with fully automated systems, it is often not possible to automatically check the complete chain from permission to system privilege for violation of constraints. A specific check on modifications of permission for violation of constraints on organizational and technical level should be part of the change procedure.

5.3.4 Granularity and risk

While defining permission, a certain granularity is taken into account. The granularity in which permission is defined has consequences for the access that someone has, intentional or unintentional. A ‘wide’ definition of access is easier to maintain, but gives the user access to information or functionality which isn’t directly needed. Segregation in many ‘narrow’ definitions is harder to maintain, but is closer to the ‘principle of least privilege’ and enables fine-grained segregation of duty. Dependant of the risk that is acceptable considering the concerned functionality and information, a definition of permission can be taken wide or narrow. A risk analysis will provide the organization with the necessary information to be able to decide about granularity of the definition and possible access constraints.

5.3.5 Delegated or decentralized administration of permission

The permission to ‘manage permission’ can be defined too. Dependant of the complexity of the organization and the need for delegated or decentralized administration of permission, these permissions need to be defined. When Role Based Access Control is used, administrative roles can be defined. A commonly used implementation model of such an administrative role structure is called the Role Control Center (RCC).

5.4 Assigning or closing permissions

In this activity the requesting, evaluating, assigning and closing of permission is performed. Of which the closure of permission is the most neglected part. As a result, on the technical level accounts and privileges are created, modified or removed.

The whole life-cycle of access can be automated in organizations with very well structured job/permissions structures, when using standard criteria.

5.4.1 Request procedure and evaluation

In the request procedure information is registered to enable evaluation, assignment and closure of permission. The information that needs to be registered consists of:

- the concerning permission;
- the identity for which permission is requested;
- the identity of the requester;
- the reason for the request (need);
- risk assessment;
- needed approvals;
- criteria for closure of the requested permission.

Based on the identities, need and risk a responsible information or system owner can approve for the requested permission. Before approving, the risk and need have to be considered. It is important to have permission defined in terminology of organizational level and not in technical terminology. Permission defined in technical terminology make evaluation difficult, because the persons involved in evaluating need to have enough technical knowledge of the systems.

Based on the criteria for closure of the requested permission, a periodic review on the validity of permission can be done. When the criteria for closure are not registered, this check is very difficult and time consuming.

Very efficient processing is possible, if all the steps of the request procedure are done once and after that standard criteria are defined for assigning the requested permission. When the request, evaluation and approval for permission assigned to a certain job description is done, the permission can be assigned to any person with the same job description without evaluation or approval.

5.4.2 Assigning and closing permissions

With the actual assigning and closing of permission, communication with the technology side takes place to create or remove accounts or privileges. This can be automated if Identity and Access Management software is used. In this software the link of permission and privileges needs to be fully defined. The predefined link between permission and privileges is very important, because otherwise it results in a system administrator deciding about this link, which should actually be a decision of both organization and technology stakeholders.

5.5 Reviewing and reporting on permission modification, assignment or closure

In this activity the validity of assigned permission is reviewed and a check is performed on accounts and privileges on the system level. More specifically, this includes verification of the information registered in the request procedure, verification on the correct execution of the procedures and if all accounts and privileges do actually correspond to identities and assigned permission. The last part is called an ‘actual state – desired state’ comparison.

Next to this, the permission structure will be reviewed to check if the risk resulting from the definitions of permission is acceptable (think of granularity, constraints and segregation of duty). The link to system privileges is significant too, because the actual access is defined with privileges.

The reports need to contain enough information to evaluate the total Identity and Access Management process against the requirements of the organization. The validations mentioned above are only measuring the effectiveness and integrity of the process.

6 Business Case

The business case is an assignment executed for a large (+40.000 identities to manage) international organization, with the goal to implement an IAM process. The IAM technology was already implemented by another party. The final deliverable of this project is included in this thesis, the chapter names that are part of this deliverable are prefixed with [BC].

6.1 Scope

The scope of this assignment comprises processes and procedures acting on the whole identity and access life-cycle, from identities and permission to accounts and system privileges.

The scope in detail is outlined below, with references to the IAM process model as described in chapter 5.

Requirements (par. 5.1)

The requirements the IAM process should meet:

- Dependencies between the process and stakeholders.
- Requirements of stakeholders.
- Impact of dependencies and requirements for the process.

Identities (par. 5.2)

Connecting the IAM process to the identity administration (HRM) includes:

- Procedure for maintaining the administration of permission assignments. This procedure will handle changes to the administration, caused by changes in the definition of permission, HR structure or the organization. For example: new roles, shops, franchise organizations or changes in the HR software.
- Document access criteria: the relationship between identity attributes and permission assignments. These access criteria can be used for defining roles.
- Procedure for maintaining access criteria. This procedure will handle changes to the administration and access criteria. For example: new identity attributes or changing definitions of attributes that will cause role changes.

Permissions (par. 5.3)

The core activities of the IAM process include:

- Procedure for maintaining the definition of permission and the relation between roles and permission. This procedure will handle requests for new or changing roles and permission, which will be defined in functional terms. The procedure will support the communication with the business.
- Procedure for maintaining the system privileges in authorization structures of applications and systems. This procedure will handle the impact of new or changing applications and systems on system privileges and permission. The procedure will support the communication with the IT department.
- Procedure for maintaining the mapping of system privileges on permission. This procedure will handle the new or changing requirements for applications and systems to provide system privileges matching the defined permission. The procedure will support the communication between the business and the IT department.
- Within all change procedures the business rules and constrains on permission assignment must be validated, to avoid violation of these rules by the changes. This validation should be executed on business level (roles, permission) and on technical level (system privileges).
- Within all change procedures the risk of access to applications and information, as intended by the change requests, must be assessed and accepted before changes are applied. Based on risk,

the granularity of the defined roles and permission or the business rules and constrains can be adapted.

- All procedures and activities mentioned above are part of an IAM process, for which roles and permission can be assigned too. In RBAC terminology, these are the administrative roles. A separate procedure for the maintenance of these administrative roles will be drawn up.

Assign/revoke permission (par. 5.4)

Assigning/revoking permission to/from identities is a separate activity in the whole IAM process. These activities include:

- Procedure for requesting, evaluating and assigning permission. (Or evaluation of existing procedure.)
- Procedure for revoking permission. (Or evaluation of existing procedure.)
- When requests deviate from the role model, criteria should be in place for deciding between acceptable deviations from the role model, or trends in deviations that indicate the need to adapt the role model.
- Clear separation in procedures between requesting permission and maintaining the definition of permission, which are different aspects of the IAM process.

Controls and reporting (par. 5.5)

Setting controls, reporting on controls, process performance and the degree of conformance to process requirements. Some basic procedures that focus on process integrity are drawn up, more advanced controls and performance indicators must be developed.

- Procedure for verifying the contents and execution of permission requests. This procedure will verify if the requests procedure is followed correctly.
- Procedure for 'actual state – desired state' comparison. This procedure will verify if all system privileges are complete and are all related to valid assigned permission.
- Procedure for verifying the changes to defined permissions and/or the role model. This procedure will verify if the change procedure is followed correctly, e.g. if the risk is assessed and accepted according to the procedure.
- Develop 'performance indicators'. These are measurable quantities, which express process performance and the degree of conformance to process requirements.
- Reporting standard, based on the process requirements and performance indicators.

General IAM process description

The description of the IAM process will include the following items:

- IAM process requirements (set by stakeholders);
- the procedures and relationships between them (process flow);
- needed input and expected output of procedures;
- responsibilities in the execution of procedures;
- dependancies in procedures;
- decision moments in procedures;
- controls and reporting.

6.2 Action plan

The information needed to draw up the IAM process will be gathered by interviews and workshops with stakeholders. In the following is stated: the project phases in order of execution, the involved stakeholder and the estimated time required (of the stakeholder and the project itself).

1. Project phase plan
   Format : -
   Part(y)/(ies) : -
   Deliverable : Project phase plan, containing scope and detailed action plan
   Approval : Project manager
   Stakeh. effort : -
   Proj. effort : 16 hours

2. Read documentation, gain insight to current IAM related processes and procedures
   Format : -
   Part(y)/(ies) : All stakeholders
   Deliverable : Documentation from stakeholders
   Approval : -
   Stakeh. effort : -
   Proj. effort : 40 hours

3. Kick-off meeting + process requirements
   Format : Workshop
   Part(y)/(ies) : All stakeholders
   Deliverable : Proces requirements document
   Approval : Stakeholders
   Stakeh. effort : 4 hours
   Proj. effort : 24 hours

4. Identities (Users)
   Format : Individual interviews and workshop
   Part(y)/(ies) : Business Unit (pilot implementation)
   Human Resources department
   HR Business Consultant
   Deliverable : Procedure steps for IAM procedures related to identities in the involved business unit. (See Scope, paragraph 'Identities')
   Approval : Stakeholders
   Stakeh. effort : 4 hours workshop, max. 1 hour p.p. interview
   Proj. effort : 40 hours

5. Permissions (business side)
   Format : Individual interviews and workshop
   Part(y)/(ies) : Business Unit (pilot implementation)
   Human Resources department
   Risk & Information Security

Administrative Organization
HR Business Consultant
ITIM Architect
Deliverable : Procedure steps for IAM procedures related to permission, regarding the business side.
Approval : Stakeholders
Stakeh. effort : 4 hours workshop, max. 1 hour p.p. interview
Proj. effort : 40 hours

6. System privileges (permissions, technical side)
Format : Individual interviews and workshop
Part(y)/(ies) : Service Delivery Manager (IT department)
Risk & Information Security, Administrative Organization
HR Business Consultant
ITIM Architect
Deliverable : Procedure steps for IAM procedures related to permission, regarding the technical side (system privileges).
Approval : Stakeholders
Stakeh. effort : 4 hours workshop, max. 1 hour p.p. interview
Proj. effort : 24 hours

7. Controls and reporting + review on results of past workshops
Format : Individual interviews and workshop
Part(y)/(ies) : All stakeholders
Deliverable : Procedure steps for IAM procedures related to audit and control. Process performance indicators and basic reporting template.
Approval : Stakeholders
Stakeh. effort : 4 hours workshop, max. 1 hour p.p. interview
Proj. effort : 24 hours

8. Draw up procedures and process steps, client evaluation
Format : Individual interviews
Part(y)/(ies) : All stakeholders
Deliverable : Procedure documents.
Approval : Stakeholders, Project manager
Stakeh. effort : max. 1 hour p.p. interview, evaluation on own insight
Proj. effort : 40 hours

9. Draw up IAM process
Format : Individual interviews
Part(y)/(ies) : All stakeholders
Deliverable : IAM process, according to scope
Approval : Stakeholders, Project manager
Stakeh. effort : max. 1 hour p.p. interview
Proj. effort : 32 hours

6.3 Milestones

The following milestones are agreed on.

Milestones	Planned due date
All workshops have taken place and the summaries and findings are accepted by the stakeholders.	13-06-2008
Procedures are ready for review.	27-06-2008
Role engineering process is ready for review.	18-07-2008
Procedures and processes accepted by stakeholders.	31-07-2008
End of project	31-07-2008

Table 2. Milestones

6.4 Key deliverables

The final deliverable is a role engineering process that will deal with changes in the whole chain of Role Based Access Management, from the administration of users and permission to technical system privileges.

This deliverable will include the following topics:

- IAM process requirements (set by stakeholders);
- the procedures and relationships between them (process flow);
- needed input and expected output of procedures;
- responsibilities in the execution of procedures;
- dependancies in procedures;
- decision moments in procedures;
- controls and reporting.

Key deliverable	Target group	Review group	Planned due date
Workshop summary and findings	Stakeholders	Stakeholders	13-06-2008
Procedures	Stakeholders	Stakeholders	27-06-2008
Role engineering process	Stakeholders	Stakeholders	18-07-2008

Table 3. Key Deliverables

Reviewers key deliverables

Review group	Reviewer	Reviews on
Stakeholders	[anonymous]	
Advisors	[anonymous]	

Table 4. Reviewers

6.5 Acceptance of Key deliverables

To finish the phase concerned, the representatives of the adjoining target group, as mentioned in the table Key Deliverables, need to accept the key deliverables.

The requirements and acceptance criteria will be determined in the first workshop, which all stakeholders will attend.

6.6 Project Risks

6.6.1 Risk identification

Risk Id	Risk	Chance	Impact	Responsible
1.	Absence of stakeholders	Medium	Medium	Concerning stakeholders
2.	Absence of irC2 consultants	Medium	Medium	Information Risk Control
3.	Incompatible requirements or expectations of stakeholders	High	Medium	Concerning stakeholders
4.	Documentation of existing environment is lacking	High	Low	Stakeholders, Project manager
5.	Adjustments to existing procedures and processes	High	Medium	Stakeholders

Table 5. Risk identification

6.6.2 Risk description

Risk Id	Risk description	Counter measure
1.	Project delay because of absence of stakeholders	Long term planning and delegation of tasks.
2.	Project delay because of absence of irC2 consultants	Well informed consultant standby.
3.	Project delay because of incompatible requirements or expectation of stakeholders	Escalate decisions to steering committee of information security.
4.	Project delay because of documentation of existing environment (processes, procedures, technology) is lacking	Interviews with stakeholders before workshops, delegation to subject experts.
5.	Adjustments to existing procedures and processes	Use most recent documentation. Clear consent about versions used. Later adjustments are out of scope of this phase.

Table 6. Risk description

6.7 Human resources

The following human resources are available to the project.

Role/Function	Name	Department
Stakeholder	[anonymous]	Business Unit
Stakeholder	[anonymous]	SDM
Stakeholder	[anonymous]	HR
Stakeholder	[anonymous]	Risk & Information Security
Stakeholder	[anonymous]	Administrative Organization
Advisor	[anonymous]	HR Business Consultant
Advisor	[anonymous]	ITIM Architect
Project support	[anonymous]	Project Office
Project owner	[anonymous]	Project Management
Advisor and author of deliverables	Bert Koelewijn	irC^2 (external)
Quality assurance	Arjan Bot	irC^2 (external)

Table 7. Human resources

7 [BC] Role Engineering Process Model

The process diagrams in this chapter are based on the ITGOV2008 process template v1.0. At the time of writing, no detailed process flow diagrams exist for ITGOV2008. The goal is to provide structure for the role engineering activities in process diagrams that are easily integrated into future ITGOV2008 processes.

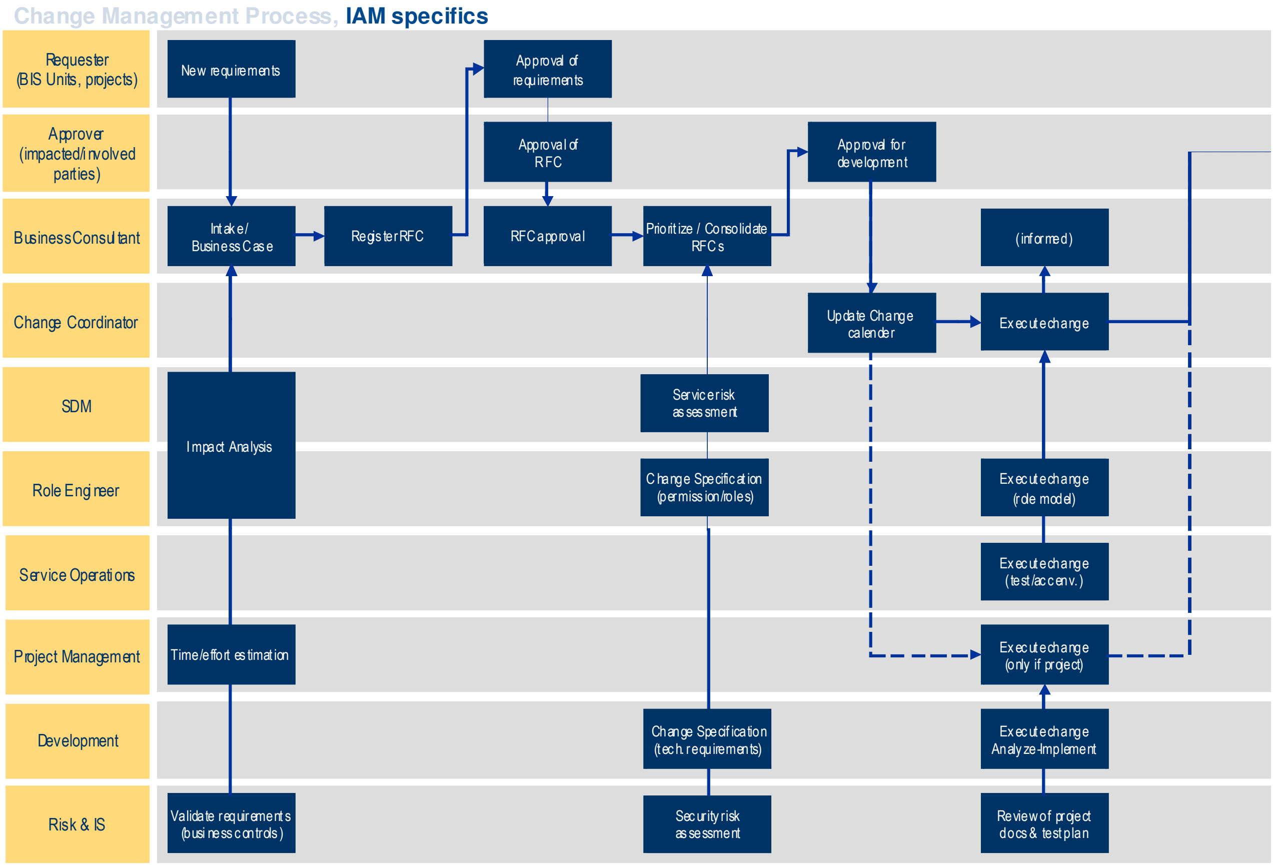
Role engineering can be initiated in 3 different ways:

- By the Change Management process.
- By the Release Management process.
- Within projects, creating an initial role model for a business unit or applications.

Role engineering is performed as part of the Security Management process. Change, Release and Security Management will be discussed in the following paragraphs.

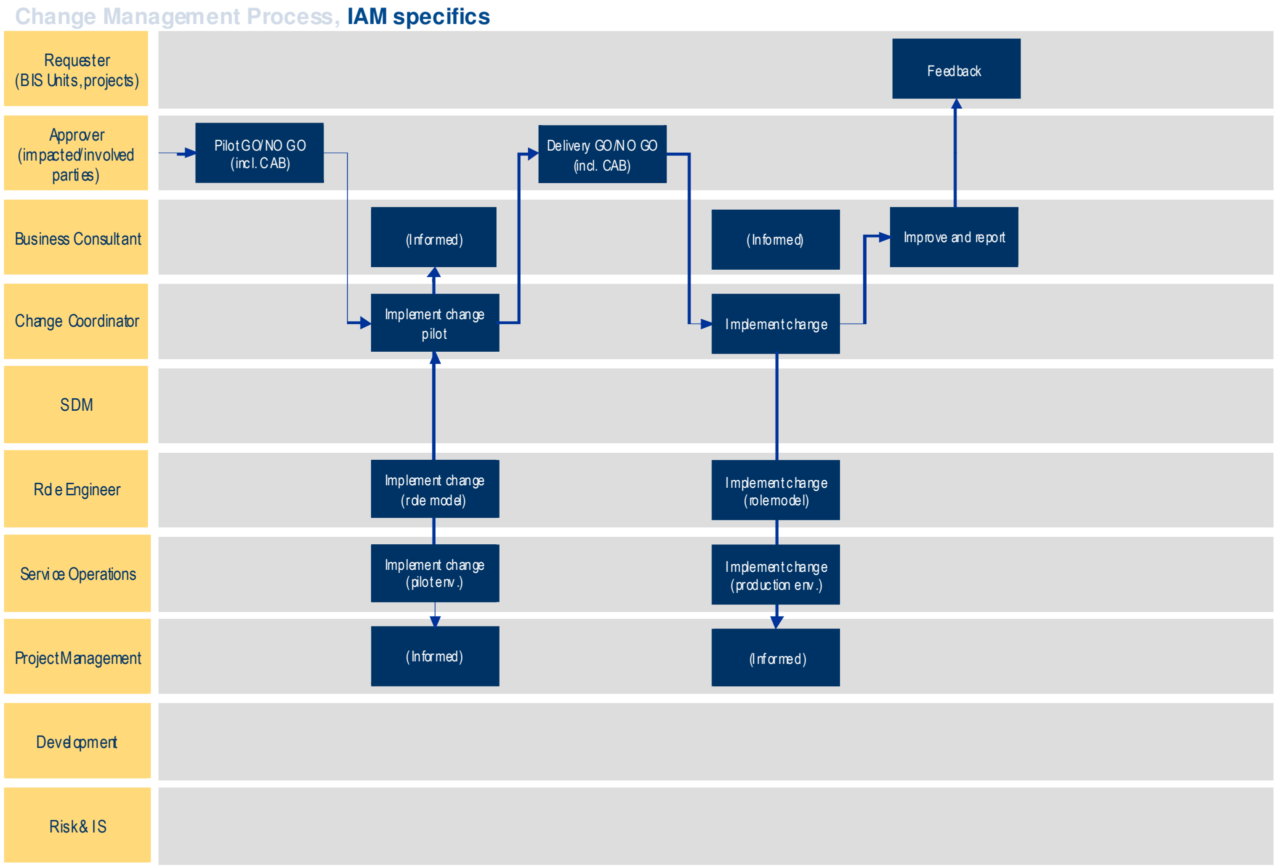
7.1 [BC] Change Management

Once an initial role model is created, role engineering will be driven by changes in the organization or technology that affect the role model. These changes will be handled the same as all other changes: by the Change Management process. In the following diagrams, the Change Management process flow is defined, with specifics for handling changes on IAM technology or the role model.



Change Management Process, IAM specifics
Requester (BIS Units, projects)
Approver (impacted/involved parties)
Business Consultant
Change Coordinator
SDM
Role Engineer
Service Operations
Project Management
Development
Risk & IS
New requirements
Approval of requirements
Approval of RFC
Intake / Business Case
Register RFC
RFC approval
Prioritize / Consolidate RFCs
Approval for development
(informed)
Update Change calender
Execute change
Impact Analysis
Service risk assessment
Change Specification (permission/roles)
Execute change (role model)
Execute change (test/acc env.)
Time/effort estimation
Execute change (only if project)
Change Specification (tech. requirements)
Execute change Analyze-Implement
Validate requirements (business controls)
Security risk assessment
Review of project docs & test plan

The diagram continiues on the next page…


Change Management Process, IAM specifics
Requester (BIS Units, projects)
Approver (impacted/involved parties)
Business Consultant
Change Coordinator
SDM
Role Engineer
Service Operations
Project Management
Development
Risk & IS
Feedback
Pilot GO/NO GO (incl. CAB)
Delivery GO/NO GO (incl. CAB)
(Informed)
(Informed)
Improve and report
Implement change pilot
Implement change
Implement change (role model)
Implement change (role model)
Implement change (pilot env.)
Implement change (production env.)
(Informed)
(Informed)

The Change Management process exists of 7 basic activities:

- Impact analysis new requirements
- Register RFC
- Approve RFC
- Prioritize RFC
- Execute changes
- Implement changes
- Improve and report

The activities in these phases will be described in detail in chapter 9.1.

7.2 [BC] Release Management

Releases introduce consolidated changes to software and hardware. These changes can originate from the Change Management process, but often are new developments that are not related to RFCs. Changes in functionality or the authorization structure are likely to have impact on IAM technology or the role model and should be documented in the Software Requirement Specifications and Functional Design.

The release RFC must specify the changes to these documents and changes required to the acceptation or production environment that are not part of the release. This includes requests for changing the role model.

Further planning and coordination of changes required for implementing releases in acceptation and production environments will be performed within the Change Management process.

7.3 [BC] General projects

To ensure no unauthorized changes are introduced in projects, each project must create change specification documents. The change specification document contains a detailed analysis of the impact on business process models, application architecture and technical architecture. The description of impact on the Role Model, Software Requirement Specification and Functional design is included in the Change Specification. For changes on IAM technology and the role model, this includes:

- Change Specification document template: explicitly define changes on authorization functionality in the system or application and explicitly define changes on the role model.
- Software Requirements Specification document template: explicitly define authorization requirements.
- Functional Design document template: explicitly define how system privileges are mapped to actors and use cases and which system privileges are used (e.g. application, oracle database, etc.)

7.3.1 [BC] Project Monitoring & Control

Project Monitoring & Control is a process of the Solution Delivery department. Monitoring will not include evaluation of project deliverables based on subject matter knowledge. But, monitoring will include evaluation of project management processes, project execution and project deliverables according to planning, standard procedures and controls. Within this process it is possible to include controls on project deliverables. For the purpose of role engineering, the following controls have to be implemented:

- All projects that have impact on (IAM) technology, connected systems and the role model should be managed by Solution Delivery.
- The impact analysis is defined as standard project deliverable and only accepted if all relevant parties have signed for approval. Relevant parties for role engineering are: AO, Role Engineer and the SDM.
- The test plan is defined as standard project deliverable and only accepted if all relevant parties have signed for approval. A relevant party for role engineering is: Risk & IS (See 9.1.5.3)
- Changes to hardware or software must only be implemented through the Release Management or Change Management process.

It is advised to include impact analysis requirements for IAM technology and the Role Model in the standard project document templates.

7.4 [BC] Security Management

Implementing access control is one of the activities within the Security Management process. The role model is the central access control model for connected systems and is maintained by the role engineer. The Security Management process consists of the following general activities:

- Define Control and Security Policy

- Define Security Plan
- Implement Security Plan
- Evaluate Security
- Maintenance
- Improve and Report

The Role Engineer is involved by creating an initial role model for a business unit, or changing the role model at request of Change Management.

The activities will be described in detail in chapter 9.3.

8 [BC] Use Cases

Use cases are defined to give an overview of the most frequent and relevant changes that will be handled by the Change Management process and role engineering activities.

The changes defined in the use cases can have an impact on multiple processes and IT systems. The impact is only determined for IAM related processes and technology: HR processes, HR application, ITIM, connected systems and the Role Model ('kruisjeslijst'). This is sufficient for the evaluation of the process, but for actual use in practice the impact analysis should be performed more in-depth.

Frequently occurring use cases that have medium/large impact should considered to be optimized. For example by standardizing procedures for these use cases and automating manual tasks.

8.1 [BC] Changes related to users

The use cases in the following table are changes related to users, their organization environment and the way they are stored in IT systems.

Use Case		Freq.	HR	HR app.	ITIM	Conn. S.	Role M.
01.	new/closing store	low	X	F	T	T	-
02.	changing store type of a store	Very low	X	F	T	T	-
03.	new/closing franchise store	low	X	F	T	T	-
04.	changing franchise store to owned store and contrary	low	X	F	T	T	-
05.	new/closing store type	Very low	X	F	T	T	X
06.	new/closing function in stores (e.g. 'Store Manager')	medium	X	F	T	-	X
07.	new/closing function in franchise stores (e.g. 'Store Manager')	medium	X	F	T	-	X
08.	changing organizational structure in HR administration	Very low	X	F	T	-	-
09.	changing the definition of user attributes (e.g. syntaxes, semantic or attribute name/data format)	high	X	F/T	T	-	-
10.	changing technology in HR systems (e.g. changes in messages, databases or integration systems)	high	-	T	T	-	-

Table 1. Use Cases

(X) = impact
(F) = functional impact
(T) = technical impact

8.2 [BC] Changes related to permission

The use cases in the following table are changes related to permission, how permission is modeled in roles, how roles are linked to functions and how permission is mapped on system privileges.

Use Case		Freq.	HR	HR app.	ITIM	Conn. S.	Role M.
06.	new/closing function in stores (e.g. 'Store Manager')	medium	X	F	T	-	X
07.	new/closing function in franchise stores (e.g. 'Store Manager')	medium	X	F	T	-	X
11.	new/closing role	medium	-	-	T/F	(T)[1]	X
12.	new/closing permission	high	-	-	T/F	(T)[1]	X
13.	changing mapping of permission on roles	medium	-	-	T/F	(T)[1]	X
14.	new/closing/changing rules for access	low	-	-	T/F	(T)[1]	-
15.	changing mapping of permission on system privileges	high	-	-	(T)[1]	T	-

Table 2. Use Cases

[1]The impact depends on how permission is configured in the connected system or application. E.g. are business roles configured in applications or only system privileges?

8.3 [BC] Changes related to system privileges

The use cases in the following table are changes related to system privileges, the applications providing functionality which is accessible through system privileges, the authorization structure that is used by the applications and how system privileges are mapped on permission.

Use Case		**Freq.**	**HR**	**HR app.**	**ITIM**	**Conn. S.**	**Role M.**
15.	changing mapping of permission on system privileges	high	-	-	T	T	-
16.	new/closing connected system or application	medium	-	-	T	T	-
17.	new/closing/changing functionality within an application	high	-	-	T	T	X
18.	changing authorization structure (system roles, system privileges)	medium	-	-	T	T	X

Table 3. Use Cases

9 [BC] Role Engineering Activities

The role engineering activities are part of the general Change Management en Security Management processes. The specifics for IAM and role engineering will be discussed for each process activity.

9.1 [BC] Change Management

The use cases require technical changes to ITIM, HR app. and connected systems. For some use cases, role engineering has to take place, to adapt the role model.

9.1.1 [BC] Impact analysis new requirements

Description

For large functional changes Business Programs develops a business case based on validation requirements by Architecture and Planning, estimation by Solution Delivery, and impact analysis by Service Delivery. (ITGOV2008)

☞ Common requests for changes in IAM technology (e.g. new stores) can be handled by standard procedures. This does not require the full CM procedure. It is advised to create standard procedures for these use cases. Optimally, some requests could be automated by ITIM using digital messages from the HR app. Standard requests will be discussed in paragraph 9.2.

Input

- new requirements
- impact analysis
- time/effort estimation
- validation of requirements against business controls
- validation of requirements against architectural standards

Output

- business case
- RFC document (based on standard template)

Actions

- new requirements
- intake/business case
- impact analysis
- time/effort estimation
- validate requirements

9.1.1.1 [BC] New Requirements

The functional requirements for changes related to permission (Table 2) are defined by the business units and should include but not limited to:

- Which roles will be assigned to the function? (use case 6 and 7)
- To which users will the role be assigned? Based on the selection of attributes from HR information. (e.g. function, department, location, etc.) (use case 11)
- Which functionality and information can the user access, if the permission is assigned? (use case 12)
- Which permission will be assigned to which role(s)? (use case 13)
- How should role assignment or role usage be constrained? (e.g. segregation of duty, time constraints, location constraints) (use case 14)
- How should system privileges on IT systems be configured to allow access according to the defined permission? (Requires in-depth knowledge of IT systems) (use case 15)

And any combination of use cases is of course possible, the functional requirements of the combined uses cases need to be described.

9.1.1.2 [BC] Intake/Business Case

The Change Management process provides the central desk for registering and managing changes. The intake will be carried out by Business Programs. The RFC document and optionally the business case will be created; involved parties are consulted for any input needed. (The input needed is listed above in par. 9.1.1.)

9.1.1.3 [BC] Impact Analysis

For the impact analysis domain specialists will be consulted, represented by the SDM. For the Role Model, the Role Engineer is consulted. The impact analysis of a change related to permission includes the following dimensions:

- Number of users affected (e.g. in stores this can be tens of thousands for a role)
- Criticalness of actions performed by the users in this role.
- Security requirements on information or functionality that this role holds permission for. (Confidentiality, Integrity, Availability)
- Complexity of the mapping: HR information – role – permission – system privileges.
- Technical impact on IT systems.

> ☞ Include impact analysis requirements for IAM technology and the Role Model in the RFC document template. The current template includes checks for involved/impacted processes and systems. IAM technology and the Role Model should be added to the checklists.

9.1.1.4 [BC] Time/effort Estimation

Like all other changes, changes to IAM technology and the Role Model can require a considerable amount of time and effort. For example a role change in stores will impact thousands of employees, which requires a full test-acceptation-pilot-implementation cycle. Solution Delivery will give an estimation of time/effort and deviation from project plans, while consulting Service Delivery.

9.1.1.5 [BC] Validate Requirements

Requirements are validated on 2 levels: enterprise architecture and business controls including financial and security controls. These validations are performed by A&P, AO and Risk & IS. For changes on IAM technology or the Role Model they include:

A&P

- Are the new requirements inline with standards and policies for applications, information and technology?
- Are the new requirements inline with architectural security requirements?

AO / Risk & Information Security

- Are the new requirements inline with business strategy, goals and corporate policies?
- Are the new requirements inline with segregation of duty policies or other constraining business policies?
- Are the new requirements inline with the security classification of the affected information?
- Is the granularity of the newly required roles/permission suitable for the level of risk involved when disclosing functionality and information through applications?

9.1.2 [BC] Register RFC

Description

The change is registered by Business Programs or in case of hardware changes by SI. (ITGOV2008)

Input

- RFC Document
- Business Case

Output

- RFC Document
- Business Case

Actions

- The RFC is documented using standard forms.
- The RFC is accepted for registration if it is complete and correct according to standards.
- For every RFC a list of approvers should be selected from involved or impacted parties. (The list of approvers must include the business unit that is responsible for the role(s) involved)
- The RFC is categorized, based on impact and urgency.

9.1.3 [BC] Approve RFC

Description

Filtering the RFC's and accepting them for further consideration. (ITGOV2008)

Input

- RFC Document
- Business Case

Output

- Approved RFC Document

Actions

- Approval of new requirements
- Approval of RFC

9.1.3.1 *[BC] Approval of new requirements*

Before formal evaluation by the approvers, the new requirements must be approved by the requester. The original requirements can be influenced by the reviewing parties and requirements validation. The requester must be sure that the requirements unambiguously reflect its needs. For changes on IAM technology and the role model, the requirements include the items mentioned in paragraph 9.1.1.1.

9.1.3.2 *[BC] Approval of RFC*

A cost-benefit analysis can be made, based on the business case and RFC. Approvers will filter the RFCs, considering multiple aspects, such as:

- constrains on budget, time, resources;
- cost-benefit;
- the impact on processes and technology;
- the requirements validation and advice of A&P, AO and Risk&IS.

9.1.4 [BC] Prioritize RFC

Description

- *Detailed impact analysis on functional RFC's to assess project or enhancement.*
- *Risk assessment if change may have negative impact on services.*
- *Sorting the RFC's by category and priority.*
- *Consolidate changes.*
- *Plan and approve development of changes, including standard requests. Update the change calendar.*

(ITGOV2008)

Input

- Approved RFC document
- Change Specification by domain specialists
- Service Risk Assessment
- Security Risk Assessment

Output

- Approved Change Specification document
- Accepted Risks
- Sorted and consolidated RFCs

- Updated change calendar

Actions

- Detailed impact analysis
- Service Risk assessment
- Security Risk assessment
- Sorting the RFC’s by category and priority.
- Consolidate changes.
- Plan and approve development of changes, including standard requests. Update the change calendar.

9.1.4.1 *[BC] Detailed impact analysis*

In this stage the Change Specification document needs to be created, with detailed analysis of the impact on business process models, application architecture and technical architecture. The description of impact on the Role Model, Software Requirement Specification and Functional design is included in the Change Specification. For changes on IAM technology and the role model, this includes:

- Change Specification document template. Explicitly define changes on authorization functionality in the system or application and explicitly define changes on the role model.
- Software Requirements Specification; explicitly define authorization requirements.
- Functional Design; explicitly define how system privileges are mapped to actors and use cases and which system privileges are used (e.g. application, oracle database, etc.)

> ☞ Include impact analysis requirements for IAM technology and the Role Model in the document templates.

The creation of the Change Specification is coordinated by Business Programs and domain specialists are consulted for specific domains. For roles and permission, the Role Engineer is the specialist to be consulted.

9.1.4.2 *[BC] Service Risk assessment*

Changes on IAM technology and the Role Model can have impact on a large number of users and/or critical services. A risk assessment should give insight in possible unwanted side effects of implementing the change. If the risks are known, appropriate measures can be taken. The service risk assessment is to be carried out by domain specialists, represented by the SDM.

9.1.4.3 *[BC] Security Risk assessment*

Security is one of the main drivers for implementing access control (RBAC). To decide whether new requirements for roles/permission are acceptable secure, risk needs to be assessed. Security risk assessments are performed by Risk & Information Security. It’s up to the approvers to accept the risk or reject the new requirements.

9.1.4.4 *[BC] Plan and approve development of changes, including standard requests. Update the change calendar.*

The change specification document contains the details of the change and its impact on processes, technology and documentation. Together with the outcome of the risk assessments, a well informed decision can be made. A final financial, technical, operational and business approval is needed from the approvers.

The aspects of this approval include:

- Financial aspects: sponsors, cost-benefit, financial risk.
- Technical aspects: impact, feasibility, architectural and security requirements.
- Operation aspects: coordination by project or Change Coordinator, planning, priorities, operational risk.
- Business aspects: business requirements and strategy, security risks. For IAM, this includes: acceptance of a business role, permission, rules with business requirements and acceptance of potential risk involved.

9.1.5 [BC] Execute changes

Description

- *Ensure that the required resources are available.*
- *Coordinating the building, testing and implementation of the change. When necessary adjust calendar and communicate changes to parties involved.*

(ITGOV2008)

Input

- Approved Change Specification document

Output

- Project deliverables
- Updated SRS and FD document
- Updated CMDB
- Project documentation (project plan, test plan, etc.)
- Review outcomes of documentation and test plan

Actions

- Change coordination
- Execution
- Review of project documentation and test plan

9.1.5.1 [BC] Change Coordination

Changes can be coordinated in 2 ways, by the Change Coordinator or by project management. This depends on certain criteria, like time/effort, impact, cost, involved or impacted parties. These criteria are documented yet. Standard requests (see 9.2), which are execute according a standard procedure are suited for coordination by the Change Coordinator.

9.1.5.2 [BC] Execution

This action includes the actual execution by designated parties. For role engineering, the actions are performed as part of the Security Management process (see 9.3).

9.1.5.3 [BC] Review of project documentation and test plan

The structure of access control consists of all relations between: HR information – role – permission – system privileges. To ensure effective access control, the whole access control structure must be properly documented and tested in projects. This must be reviewed by AO / Risk & IS.

Centralized access management is performed within the Security Management process and includes documentation of HR information – role – permission relations. But when implemented in applications and systems, the documentation is system dependant. For example the relation between permission and system privileges is application dependant and not centrally controlled by Security Management.

To ensure correct access control on the system level which is often out scope of the Security Management process, the following points should be reviewed:

- Does the application or system implement access control on role, permission or system privilege level? (See 10.1.5)
- Depending on the level of access control implemented in the application or system, is the system dependant part of access control properly documented in the Change Specification, Software Requirements Specification and Functional Design?
- Has the Role Engineer approved the documents? The implementation should match the central Role Model, managed by Security Management.
- Are the access control requirements from the Software Requirements Specification explicitly tested in the test plan? This is essential to verify that the required access (permission) matches the actual access (system privileges). Tests should confirm access to functionality and information is not less or more restricted than specified.

9.1.6 [BC] Implement changes

Description

- *Implement the change according to schedule. This includes formal approval in Change Advisory Board and chairing the Change Advisory Board.*
- *Emergency changes need to be implemented promptly; therefore regular process change management will be followed after implementation.*

(ITGOV2008)

The pilot tests mentioned in the process model is typically for stores. This step can be skipped if not applicable.

No further special considerations are required for implementing changes in IAM technology or the Role Model. This step is mentioned for completeness.

9.1.7 [BC] Improve and report

Description

- *Determining if each change was successful and learning lessons to improve the process. This also includes KPI reporting. (ITGOV2008)*

No special considerations are required for reporting about changes in IAM technology or the Role Model. This step is mentioned for completeness.

9.2 [BC] Standard Requests

If RBAC is used in dynamic environments like the headquarters, roles and permission are likely to change more often and business units are smaller. The impact of changes can be too small for a full Change Management process. For this kind of changes a shorter procedure must be followed, where the business owner, the role engineer, Risk & Information Security and the Change Coordinator can decide on direct implementation of a role and permission.

For this procedure the following principles can be used:

- The requester must be the business owner or delegate of the involved business processes and data.
- The business owner is aware of the possibility of accidental disruption of service, because of the direct and not thoroughly tested implementation.
- The following criteria apply to the request:
    - The request only has impact on the role model, no changes to applications or systems are needed.
    - The request only has impact on the processes and data of the business owner.
    - The requests must have clear and predictable impact.
    - The involved processes are not time critical.
    - The involved data is not classified as confidential or secret.

9.3 [BC] Security Management

Access control is an integral part of each activity in the Security Management process. In the following chapters the specifics for IAM will be highlighted for each general activity.

> ☞ It is advised not to allow change requests for roles and permission directly to the Security Management process. This would allow changes to the operating environment, without proper overall management and control by the Change and Release Management processes. Impact and interference with other systems and developments can not be properly analyzed by Security Management. Change requests for roles and permission must be directed to the Change Management process. Standard change requests should allow fast and controlled execution by Security Management.

9.3.1 [BC] Define Control and Security Policy

Description

- *Defines security policy as framework for security management. Also approval of improvement plans, improvement cycle. (ITGOV2008)*

The security policy must include policies for access management, representing business needs and requirements. Specific IAM controls must be included in the control framework.

Input

- Business plans, strategy, requirements
- Architectural security requirements

Output

- Security policy
- Control framework

Actions

- Define access control policy
- Define control framework

9.3.1.1 *[BC] Define access control policy*

The business requirements for the access control policy are defined by Business Programs and AO / Risk & IS. They include the following items:

- Relevant legislation and any contractual obligations regarding protection of access to information or applications.
- Classification policy for information and related applications.
- Business risks associated with information and related applications.
- Enforce consistency of classification policies and access control between different networks and systems. E.g. the same information can be stored in different physical systems. Access control should be consistent between the different systems.
- Access control policies related to security classification of information and applications. E.g. For a critical application containing classified information more strict security requirements apply than other applications.
- Segregation of duty policies or other constraining business policies E.g. time or location constrains on access to systems.
- The granularity of roles/permission in relation to the acceptable level of risk. E.g. principle of least privilege (high granularity) for access to critical applications, less strict (low granularity) roles for normal applications.
- Preferred access control model for business units: RBAC, request based (central) or self regulation by business unit.
- Formal access request procedure, including criteria for access removal and the following authorities:
    - Who may request roles and permission and for which classification level of the involved information and applications?
    - Who may approve requests and for which classification level of the involved information and applications?
    - Who may approve requests which are exceptions to the Role Model?
- Requirements for review of assigned access. E.g. periodic review of assigned system privileges on user accounts.
- Reporting requirements (see chapter 11)

9.3.1.2 *[BC] Define control framework*

Controls specific for IAM are described in a separate chapter, see chapter 11.

9.3.2 [BC] Define Security Plan

Description

- *Create Security section for SLA*
- *Create underpinning Contracts*
- *Create Operational level agreements*

(ITGOV2008)

Include access control activities, such as role engineering, and IAM technology in the SLA and OLA.

> ☞ In ITGOV2008 the activity ‘implementing security’ is outsourced to a third party. Third parties must be prepared and capable to manage IAM technology (e.g. ITIM) and integrate with IAM processes.

> ☞ Outsourcing role engineering can be difficult, because of the close involvement in business processes. The activity ‘role engineering’ should ensure a secure, functional, effective and maintainable role structure. In stores, the roles are not likely to change very often, but in future applications of IAM (e.g. distribution centers, headquarters) roles will be added, removed and changed on a daily basis. Role engineering in this kind of dynamic environments requires specialist expertise and good insight in processes of business units. Business processes need to be analyzed and modeled into roles and permission.

9.3.3 [BC] Implement Security Plan

Description

- *Classify and managing of IT applications*
- *Implement personnel Security*
- *Implement Secure Management*
- *Implement Access control*

(ITGOV2008)

The implementation of access control is in fact the execution of operational tasks related to IAM. The security policy, controls and SLA form the framework to which these tasks must adhere.

Input

- Security policy
- Control framework
- SLA and OLA

Output

- Role Model
- Updated user - role/permission administration (request based assignment)
- Actual State - Desired state comparison reports
- Accounts and system privileges that are candidate for removal

Actions

- Implement Access control:
    - Role engineering (defining and modifying permission)
    - Assigning/closing permission or roles
    - Reviewing and reporting of assigned, modified or closed permission

9.3.3.1 [BC] Role Engineering

The activity 'role engineering' should ensure a secure, functional, effective and maintainable role structure. In stores, the roles are not likely to change very often, but in future applications of IAM (e.g. distribution centers, headquarters) roles will be added, removed and changed on a daily basis. Role engineering in this kind of dynamic environments requires specialist expertise.

External to the Security Management process, the role engineering activity can be initiated in 3 ways:

- By the Change Management process.
- By the Release Management process.
- Within projects, creating an initial role model for a business unit or applications.

As integral part of the Change and Release Management processes, the Role Engineer must analyze the Change Specification, Software Requirements Specification and Functional Design to determine the impact to the following parts of the Role Model:

- Changes in the relation between HR information (e.g. person, function, position) and roles.
- Changes in the relation between roles and permission.
- Changes in the definition of permission.
- Changes in the definition of system privileges.
- Changes in the relation between system privileges and permission.

The Role Model must define the complete relation chain between HR information – role – permission. The relation between permission and system privileges is system dependant and must be defined in the Software Requirements Specification and the Functional Design. To be able to define these relations, the Role Model must adhere to the following requirements:

- For each role, criteria must indicate to which employees the role is automatically assigned, based on HR information. E.g. in stores the function and position of an employee and the store type determine the roles that are automatically assigned to the employee. This must be documented in the Role Model.
- Roles must be related with permission statements and not with system dependant technical system privileges. The abstraction will keep the Role Model more flexible in complex environments.
- Each permission statement must be fully described in terms of the process. This can not be completely defined in a Software Requirement Specification, because one permission statement may overlap multiple applications or systems. A flexible Role Model is not system dependant and has a higher abstraction. If assumptions are made, discrepancies will occur between the functional requirements for access and the actual technical implementation. E.g. if the Role Model contains a term which has always been used for a certain functionality and the functionality in the application is extended in a new release, it's hard to verify if the permission is still valid according to business needs.

9.3.3.2 [BC] Assigning/closing permission or roles

In this activity the requesting, evaluating, assigning and closing of permission is performed. As a result, on the technical level accounts and privileges are created, modified or removed.

> ☞ The central desk for access requests is the Request Management process. Frequently recurring and similar requests can be standardized and fully processed by request management. Other requests will be handled by the Security Management processes.

The whole life-cycle of access is automated when using roles that are related to HR information, such as the function of an employee. IAM technology will create, close or modify accounts and permission automatically according to the Role Model. Exceptions to the Role Model must be requested and handled manually following the request procedure.

In the request procedure information is registered to enable evaluation, assignment and closure of permission. The information that needs to be registered consists of:

- the concerning permission or role;
- the user for which permission is requested;
- the requester;
- the reason for the request (business need);
- risk assessment;
- needed approvals;
- criteria for closure of the requested permission.

Only if the request is made by an authorized requester and is approved by an authorized approver, the request can be processed. A clause defining the authorized requesters and approvers should be part of the Access Control Policy (see paragraph 9.3.1.1). Based on the user, business need and risk the responsible information or system owner can approve for the requested permission. Before approving the risks and business requirements have to be considered (e.g. segregation of duty requirements). Risk & IS must perform these assessments. Optionally an assessment is only performed for classified information or applications and not for standard requests.

It is important to have permission defined in terminology of organizational level and not in technical terminology. Permission defined only in technical terminology makes evaluation difficult, because it requires that the evaluators have in-depth technical knowledge of the systems.

Based on the criteria for closure of the requested permission, a periodic review on the validity of permission can be done. When the criteria for closure are not registered, this check is very difficult and time consuming.

9.3.3.3 [BC] Reviewing and reporting of assigned or closed permission

In this activity the validity of assigned permission is reviewed and a check is performed on accounts and privileges on the system level. The goal is to minimize invalid (e.g. expired) permission that was requested by Request Management. The second goal is to validate the integrity of system privileges, which should correspond with the Role Model maintained by Security Management. More specifically, this includes verification of the information registered in the request procedure, verification on the correct execution of the procedures and if all accounts and system privileges do actually correspond to users and assigned permission. The last part is called an ‘actual state – desired state’ comparison.

☞ A tool for reporting on accounts and system privileges already exists within the organization. This can possibly be used as input for the checks and comparison mentioned above.

Periodic review of request based assigned permission or roles must be performed to determine if the request is still valid, based on the criteria for closure that are defined in the original request. The most commonly used criterion is expiration date on a permission or role assignment. When using expiration date, this check can be automated by comparing all expiration dates to the current date.

Requests must be monitored for trends, e.g. recurring requests from the same requester, same permissions or roles. These kinds of requests can be handled in two ways:

- Similar and recurring requests can be standardized and fully delegated to Request Management.
- Recurring exceptions to roles in the Role Model are an indication for the need of a new role or role change. These exceptions should be monitored for such trends.

9.3.4 [BC] Evaluate Security

Description

- *Self assessment*
- *Internal Audit*
- *External audit*
- *Evaluation based on security incidents*

Assessments and audits are needed to determine if the current access control structure is still effective and sufficient. Impersonation a malicious person with fraudulent behavior will uncover vulnerabilities that are overlooked in the design and implementation of access control.

Input

- Role Model
- Access control policy

Output

- Vulnerability reports
- Audit reports

Actions

For access control the following tests are relevant in assessments and audits:

- Does the mapping between permission and system privileges as implemented in the application, match the functional requirements as defined in the Role Model?
- Can access controls be circumvented?
- Can malicious use of valid access lead to fraud? If yes, was the valid access given by automatic role assignment or by request? If request, was the risk properly analysed and were segregation of duty requirements checked?

9.3.5 [BC] Maintenance

Description

- *Maintenance of security elements in Service level agreements*
- *Maintenance of security elements UC*

No further special considerations are required. This step is mentioned for completeness.

9.3.6 [BC] Improve and Report

Description

- *Continuous process improvement*
- *Reporting on KPIs*

Reporting and controls specific for IAM are described in a separate chapter, see chapter 11.

10 [BC] Process roles and Responsibilities

10.1 [BC] IAM process roles

10.1.1 [BC] Requester role

The requester role is often fulfilled by the business owner of the impacted process and information, but others can request changes too. Everyone has their own responsibility in communicating changes in the organization, processes or technology that impact IAM technology or the role model. The awareness of this responsibility is important, if this communication is omitted access to systems and applications can become non-functional.

Responsibility

- Communicate changes in the organization, processes or technology that involve authorization in general (e.g. roles, permission or access to systems) and may impact IAM technology or the Role Model.
- Provide information for the RFC, such as: request, requirements and objectives, shortcomings of current situation, change proposal and priority.
- Verify requirements in registered RFC.

Authority

- Approve or reject requirements in registered RFC.

10.1.2 [BC] Approver role

The goal of the approver role is to get full consensus on all financial, technical, operational and business aspects of a change. The approver role is fulfilled by authorized representatives of the involved and impacted parties. For Standard Requests a predetermined and fixed selection of approvers will process the request, for other requests a selection of approvers need to be determined in the registration step. In general the selection of approvers will include all parties that are responsible for the impacted organization, processes and technology. Common approvers are: the business owner(s) of impacted processes and information, Service Delivery Manager, AO and the Change Coordinator. These parties could already be part of a Change Advisory Board, which is the main authority for approvals.

Responsibility

- Ensure all financial, technical, operational and business aspects of a change are supported by the responsible parties.
    - Financial aspects: sponsors, cost-benefit, financial risk.
    - Technical aspects: impact, feasibility, architectural and security requirements.
    - Operation aspects: coordination by project or Change Coordinator, planning, priorities, operational risk.
    - Business aspects: business requirements, strategy and security risks. For IAM, this includes: acceptance of a business role, permission, rules with business requirements and acceptance of potential risk involved.

Authority

- Approve or reject new request for change
- Approve or reject start of development
- Approve or reject start of pilot
- Approve or reject start of delivery

10.1.3 [BC] Business Consultant role

The first four steps of the Change Management are performed by Business Consultants within the Demand Management process, which is a process of the Business Programs department. The goal is to translate business demands into requirements for information technology.

Responsibility

- Ensure all RFCs are handled according to the procedures.
- Ensure new business requirements are documented clear and unambiguous.
- Coordinate and execute impact analysis on new requirements.
- Maintain RFC registration.
- Coordinate RFC Approval.
- Coordinate and execute the writing of the Change Specification.
- Coordinate Risk assessments.
- Prioritize and consolidate changes to reach optimal balance between business demands and cost.
- Report to the requestor and other stakeholders about the progress and status of every change.
- KPI reporting.
- Optimize Change Management process.

Authority

- Decide about optimal priority and consolidation between demands of multiple business units.
- Initiate meeting of approvers/CAB.

10.1.4 [BC] Change Coordinator role

The Change Coordinator is responsible for the coordination of the execution and implementation of approved changes. If the change will be executed in project form, the Change Coordinator is only responsible for the coordination of the implementation.

Responsibility

- Maintain change calendar.
- Coordinate execution of changes.
- Coordinate implementation changes.
- Manage resources and support communication between involved parties.
- Report to the requestor and other stakeholders about the progress and status of every change implementation.

Authority

- Claim resources for execution of changes according to schedule.
- Change the Change Calendar.

10.1.5 [BC] Role Engineer role

The Role Engineer is the owner of the Role Model and is responsible for maintaining the Role Model. The goal is to ensure a secure, functional, effective and maintainable role structure.

Responsibility

- Ensure a secure, functional, effective and maintainable role structure by analyzing business requirements and supporting role design.
- Write change specifications for changes in the Role Model. (Relation chain between HR information – role – permission.)
- Perform detailed impact analysis by reviewing the Change Specification, Software Requirements Specification and Functional Design.
- Maintain descriptions and functional design of roles and permission.

Authority

- Optimize Role Model.
- Request restructuring of roles and permission.
- Define design principles for roles and permission.

10.1.6 [BC] Risk & Information Security

The tasks of the departments AO and Risk & Information Security include advisory and support on implementation of controls and risk management. These tasks are performed for ITGOV2008 in general, including IAM related processes. The goal of the role Risk & Information Security is to have optimal process control regarding business requirements and enable informed decisions about security and risks.

Responsibility

- Verification of business controls in new requirements
- Review of change and project documentation, including RFC, Change Specification, SRS, FD, Test plan. The focus of the review is verification of business controls, financial and security risk assessment. Legal or regulatory risks are delegated to specialists.
- Risk assessment on request based role assignment and exceptions to the Role Model.
- Review and support on the definition of the Access Control Policy.

Authority

- Risk&IS can give support and advisory, no authority to veto decisions.
- Risk&IS is able to escalate to higher management if stringent advisory is ignored.

10.2 [BC] External actors

10.2.1 [BC] Responsibilities for data maintainers (HR app.)

All parties editing and maintaining data in the HR app. can possibly impact IAM technology or the role model.

- All editors in the HR app. are aware and understand the consequences of changing data. The data is automatically processed by ITIM; changing syntax, semantics or the structure of data (using functionality of HR app. and connected applications) can lead unpredictable and unwanted results in ITIM and connected systems.
- Data changes that are known to require a change to ITIM or the Role Model must be reported via the Change Management process.

10.2.2 [BC] Business Units

Business units are internal departments, but external companies that edit data on connected systems are considered too (e.g. franchise organizations and the external accounting organization). The business units often are process owners and data owners. The following responsibilities result from that:

- Business units are responsible for their human resources. They have to deliver current and correct information about employees, temporary staff and contractors. Next to the normal administrative use (e.g. salary payments), this information is used for automatically assigning permission to the employees. In stores an application is used to enter employee information, which is imported into the HR app.

  ☞ Business units can decide to restrict the assignment of high risk functions. For example in stores, the store manager function can only be assigned by the regional office. The store manager can assign all other functions within the store.

- Business units are responsible for delivering current and correct information about changes in the organization. There should be permanent awareness of organization changes (Table 1) that affect permission assignment and need to be communicated with Change Management.

10.2.3 [BC] HR

Information about employees and the organization is maintained in the HR app. by HR. With IAM technology roles are automatically assigned to users, based on HR information. Specific for IAM the basic responsibilities of HR are:

- HR is responsible for the representation of the organization in the HR app. (e.g. stores, store types, available functions)
- HR is not responsible for employee data that is imported from other sources into the HR app. (e.g. personal data of the store employee and function assignment is imported)
- HR only delivers data, but is not responsible for assigning roles/permission to users or other use of this data.

Because HR maintains data in the HR app, the ‘Responsibilities for data maintainers’ apply (See paragraph 10.2.1). For the use of IAM, some additional responsibilities need to be addressed:

- HR must ensure that information in the HR app. is up-to-date and complete. HR must also ensure that the information feed from business units is up-to-date and complete. (e.g. organization structure change or a franchise employee quits)
- At the moment, the HR app. is the only source of employee information connected to ITIM. HR must ensure that every employee (internal, franchisers, etc.) for who access is managed, is registered and maintained in the HR app. This means that persons must be registered who are actually not employees.

> ☞ Technical accounts on systems (e.g. accounts for IT administrators, applications or services) are not managed by ITIM. It is advised to manage and report about those accounts too, because of the high risk authorisations often associated with those accounts. To realize this, an administration of these identities (can be non-human 'users') needs to be set up. It is advised not to integrate this with HR processes, because of the technical context. A separate administration, possible using the HR app, needs to be established within the Security Management process.

10.2.4 [BC] Finance & external accounting organization

The current cost centre structure in the HR app. is maintained by the finance department and the external accounting organization. This financial structure is used by ITIM to represent stores, store types and to link employees to stores. The messages from the HR app. to ITIM include cost centre information.

Because Finance and the external accounting organization maintain data in the HR app, the 'Responsibilities for data maintainers' apply (See paragraph 10.2.1).

In the stores, the financial structure matches the organization structure. For example, a store is a cost centre and the employees belong to a cost centre.

> ☞ It is advised to use the organization structure from the HR app. maintained by HR for feeding ITIM. Using the organization structure has three advantages over using the financial structure:
>
> - The financial structure is not guaranteed to be the same as the organization structure, especially in distribution centres (DC) or headquarters (HQ).
> - The organization structure gives more information about manager positions and employee relations. This is useful for implementing IAM in DC or HQ.
> - The information is maintained by HR, an internal department already involved by maintaining employee information. One party maintaining all information gives better control and less complex Change Management procedures.

11 [BC] Control & Reporting

11.1 [BC] IAM Controls

All IT processes, including the processes related to IAM, must adhere to the General Control Objectives. In the following table specific IAM controls are defined for each relevant General Control Objective.

☞ Applications and systems of stores are formally not in scope of the GCO. This was decided before the implementation of IAM. It is advised to reconsider this decision with the implementation of IAM.

General Control Objectives	IAM Control Objectives	Controls
10.1 Applications are designed to meet the businesses control needs of completeness, accuracy, validity and authorized access.	Systems and applications managed with IAM do not contain unregistered user accounts or invalid system privileges.	Actual state – Desired state comparison, review of assigned permission.
	Roles and permission assigned to users match the system privileges assigned to user accounts.	Actual state – Desired state comparison
	Manual access requests and exceptions to the role model are requested, evaluated, assigned and closed by formal procedures.	Request Management / Security Management
	Exceptions to the role model are kept at minimum; structural and valid exceptions are prevented by adapting the Role Model.	Review by AO is part of the request procedure.
	Business rules for access (e.g. segregation of duty) are enforced by the Role Model. Exceptions to the Role Model are validated against business rules before approval.	Business rules are part of the Access Control Policy. The Role Engineer is responsible for defining the Role Model in line with the Access Control Policy. Review by AO is part of the request procedure.
	System privileges (actual access) on systems or applications are not more permissive or restrictive than defined in the functional definition of the related permission.	Defined in Software Requirement Specification and Functional Design. Required part of Test Plan.
10.2 Documentation is adequate to support ongoing operations, problem resolution and future application maintenance.	Permission is described in functional terminology, clearly defining access to functionality and information according to business requirements.	Requirement of Role Model, responsibility of Role Engineer. Requirement of Change Specification in Change Management process.
	Access functionality of systems and applications is clearly documented.	The SRS and FD of connected applications include adequate description of authorization functionality and the defined authorizations.
10.3 Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.	Changes to roles, permission and system privileges are handled by formal procedures that include approval, acceptance and pilot testing.	Changes on roles, permission and system privileges are handled by the Change Management and Security Management processes. Unauthorized changes to roles, permission and system privileges are prohibited.
	Changes to roles, permission and system privileges do not break any business rules (e.g. segregation of duty).	Business rules are part of the Access Control Policy. The Role Engineer is responsible for defining the Role Model in line with the Access Control Policy. Review by AO is part of the Change Management process.

11.2 [BC] Reporting

The purpose of reporting is to monitor effectiveness of role engineering, which is part of the Security Management process. The following key performance indicators are identified for the Security Management process and are specific for IAM.

% reduction in security-related incidents, which are enabled by unnecessary or invalid access

% reduction of unregistered user accounts and invalid system privileges relative to the total number of user accounts and system privileges

% reduction of system privileges assigned by request (exceptions to Roles) relative to the total number of system privileges assigned

% of system privileges assigned by temporary roles

12 [BC] Reference

Account	An instance of a user on a computer system or application. System privileges are assigned to an account. A user can have multiple accounts associated to it.
Access	The ability to use a resource or a service. Access should only be possible if permission is assigned to the user.
A&P	Architecture & Planning (ITGOV2008 Department)
AO	Administrative Organization
Risk&IS	Risk & Information Security
Change Management	The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization. (source: ITIL)
Connected Systems	Applications that are automatically provided with users and permission by ITIM.
HR app.	the HR application
Employee	A person in the service of the organization or franchisers, under contract or hire.
Function	The name of the position as assigned in the HR application
Identity	See User.
ITGOV2008 processes	Processes as described in the new IT process model
ITIM	IBM Tivoli Identity Manager, synchronization of users and permission from/to connected systems
Permission	The functional definition of access to information or services. Permission can be assigned to users.
Position	Defines the function and the actual placement within the organization.
RBAC	Role Based Access Control
Release Management	The goal of the release management process is to ensure the successful rollout of hardware and software releases, secure minimal unpredicted impact on operations and realize efficiency gains from combining change in release. (Source: ITGOV2008)
Role	A grouped set of permissions, which can be assigned to users. The grouping and assignment can be based on functions, departments, projects, etc.
Role Engineering	The activity that is needed to create and maintain roles. The goal is to ensure a secure, functional, effective and maintainable role structure.
Rule	Rules defined by the business that can be forced upon roles and restrict the assignment or activation of roles. E.g. two roles that must not be assigned to one user or a time restriction which

activates a role only within certain hours.

Security Management The goal of the Security Management process is to meet the security requirements of SLA’s and external requirements further to contracts, legislation and externally imposed policies and to provide a basis level of security, independent of external requirements.

SI Service Integrator

System privilege The technical configuration that is needed to enable access to information or services as functionally defined in the permission statement. System privileges can be assigned to accounts.

User The registration of a person in the HR application, which can be used to assign permission to.

13 Analysis & Conclusion

13.1 IAM Process model

The IAM process model (chapter 5) is designed to represent the most basic activities needed to fulfill business requirements and expectations in regard to the business drivers. The activities are modeled in a logical structure and order.

In the business case, the IAM process model was used as framework for the action plan and the workshop subjects. This worked out very well, because each of the four main activities could be discussed separate of the others and with other stakeholders in the process. The complexity of the whole process was divided and therefore easier to understand for the stakeholders; they didn't have to oversee the whole process to discuss the part they were responsible for.

The actual design of the IAM process came out very different than expected: not a single process such as described in the process model. The activities were completely integrated in the new IT process model of the customer, called ITGOV2008. The main activities were integrated into the following processes:

1. *Managing identity information*; only partly in the HR process, because the HR manager refused to take responsibility for the administration of access related attributes of the identities. As stated in paragraph 10.2.3:

   > Specific for IAM the basic responsibilities of HR are:
   >
   > - HR is responsible for the representation of the organization in the HR app. (e.g. stores, store types, available functions)
   > - HR is not responsible for employee data that is imported from other sources into the HR app. (e.g. personal data of the store employee and function assignment is imported)
   > - HR only delivers data, but is not responsible for assigning roles/permission to users or other use of this data.

   The consequence is that a separate organizational unit needs to be implemented for administrating identities, based on HR information.
2. *Defining and modifying permission*; this was integrated into the Change Management and Security Management processes. Role engineering and maintenance of the role model is performed within security management, but all other related activities (handling requests, planning and operations) are performed within change management.
   The link with technology, as described in paragraph 5.3.2, was totally integrated in the system design. Technical privileges are mapped to functional permission descriptions and documented in the Functional Design and System Requirements Specification. Projects and the System Development process needed to deliver the information needed (as mentioned in paragraph 7.3). This resulted in understandable and maintainable roles, because only functional terminology was used.

> *In another business case at a large Dutch bank, technical privilege statements are included in roles instead of functional permission statements. Technology is very complex and suspect to change, resulting in unreadable (even >20.000 statements per role!) and inconsistent roles. Keeping roles consistent with changes in technology is very hard if this has to be performed within the Security Management process, instead of the System Development process.*

3. *Assigning or closing permission*; as mentioned in paragraph 9.3.3.2, standard requests are handled by the Request Management process. This process handles all standard IT related user requests. The request procedure and the changes to accounts and privileges are automated by IAM software. (IBM Tivoli Identity Manager)
4. *Reviewing and reporting on permission modification, assignment or closure*; controls are implemented to maintain process and system integrity (par. 11.1). These controls are managed by the departments AO and Risk & IS, which are part of the high level IT Management and Control process.

One aspect that is forgotten in the whole IAM process model is the management of authentication means, like password or security tokens. This is a crucial part in the identity life-cycle, because the whole trust in "Who has permission to do what on which data and why?" starts with authentication. Management procedures need to be as secure as the technical authentication means itself, otherwise the security of the technology is undermined.

To summarize the conclusion regarding the IAM process model: it is very useful for dividing the complex structure of tasks into pieces that can be handled separately, but in practice the activities will often be part of other processes. The value and applicability of the term "IAM process" can be subject of discussion.

> *In the business case at a large Dutch bank, the IAM related activities were grouped and structured in an IAM process. The isolation of these activities in one single process contributed to the problems described above. Too much tasks that should have been executed in relating processes (System Development, Change Management) were executed within the IAM process.*

Should IAM activities be integrated into general IT management processes, for IAM to succeed? In this research we found reason to confirm this statement.'

13.2 Use of COBIT for IAM

In table 1 of paragraph 2, a summary of IAM process relationships is given. This summary is challenged in practice with the business case. In the following, the application of the relationships in the business case will be discussed.

PO2 Define the Information Architecture

In paragraph 9.1.1.5 the requirements of a change are validated. Changes include changes in roles, permission and system privileges. The validation includes Enterprise Information Architecture and information security classification. The placement of this validation at the start of the Change Management process ensures all changes in processes and technology are validated with the Enterprise Information Architecture.

PO3 Determine Technological Direction

In paragraph 9.1.1.5 the requirements of a change are validated. Changes include changes in roles, permission and system privileges. The validation includes standards and policies for applications, information and technology. The placement of this validation at the start of the Change

Management process ensures all changes in processes and technology are validated with the standards and policies for applications, information and technology.

PO9 Assess and Manage IT Risks
Risk assessment is implemented at many instances through the process. Some examples in the Change Management process are Service Risk assessment of a change (par. 9.1.4.2) and the security risk assessment of a change (par. 9.1.4.3). The input of business risk assessment is also needed to create the access control policy (par. 9.3.1.1).

AI2 Acquire and Maintain Application Software
The application security controls specification, which is specified as output from AI2, is used to review the Software Requirements Specification in par. 9.1.5.3. The SRS must meet and include the security controls specification.

DS1 Define and Manage Service Levels
The requirements for the operating level agreements (OLA) regarding IAM are mentioned in par. 9.3.2, but not explicitly. The explicit impact of IAM for the OLAs should be researched.

DS8 Manage Service Desk and Incidents
In the business case, no explicit security incident definitions or other help desk instructions are described. Although it's not such an often recurring and critical relation, it's lacking and should be added.

DS7 Educate and train users
A security awareness program was already available. The input needed should be documented in this program; it doesn't have to be part of the IAM activities and related processes.

ME1 Monitor and Evaluate IT Performance
Controls and reporting on process performance is discussed in chapter 11.

AI6 Manage Changes
Change management is very critical. A large part of the IAM process (handling security changes) is implemented in change management (par. 9.1).

DS11 Manage Data
Security requirements for managing data on the system level are found too specific to include in the business case. It should be part of general security management.

Except for DS8, DS7 and DS11, all relations were included and fully adopted in the business case. They can be considered as critical. The relations with DS8, DS7 and DS11 didn't have a critical role in this business case and could be replaced.

There is a relation that was not mentioned in table 1. Obviously the strong relation with the HR process, that was already included in the process model. The HR process is more broaden than IT management and therefore not fully included in COBIT.

Overall, the conclusion is that the result of the 'research assignment' summarized in table 1 performed really well. This is remarkable for such a general framework (COBIT) that has such little explicit text in regard to IAM.

13.3 IAM problems in practice

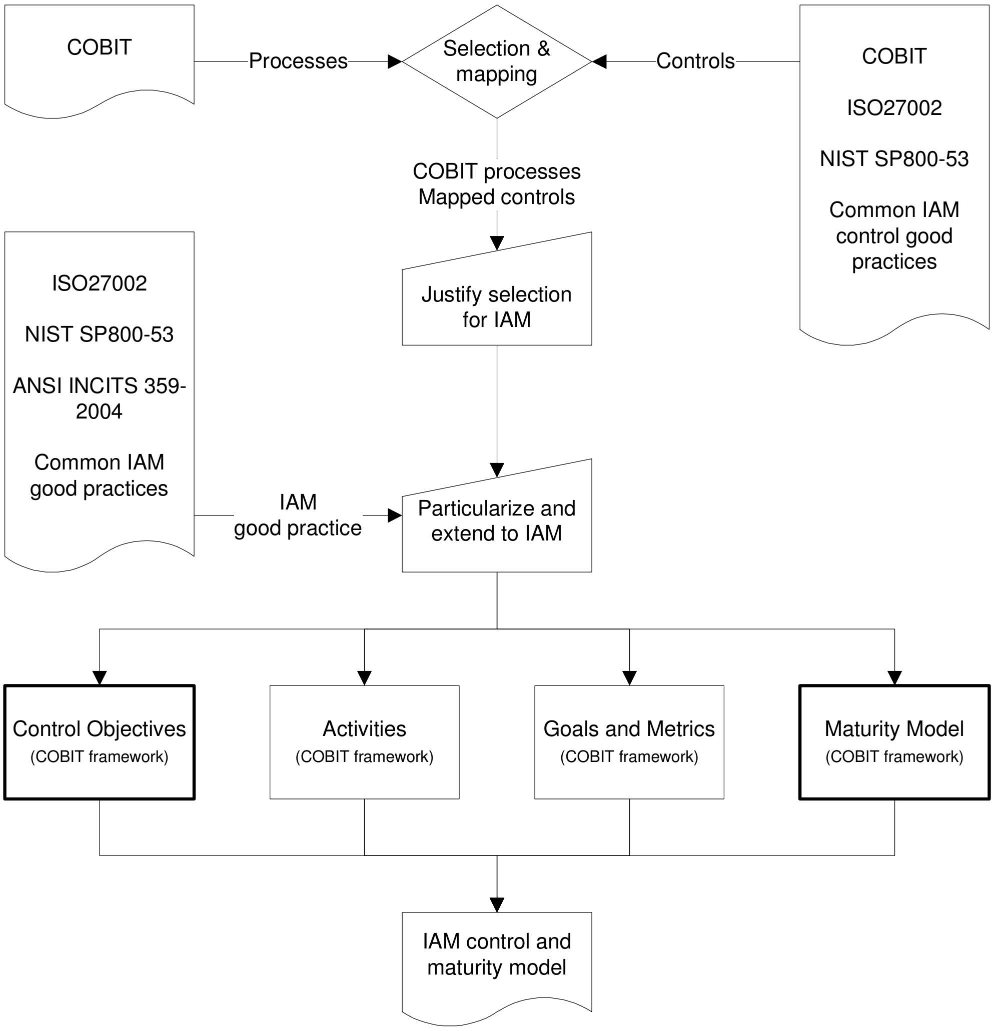
In this paragraph a summary of problems will be given, which were encountered in various business cases. It is not a conclusion, but a useful summary for later projects. An organization typically has multiple information systems, with different information owners. If an entity wants to use the system and have access to information in the system he has to apply for access by the information owner. When granted access, an account with privileges will be created for the entity. If this process is not well organized, the following security related problems could occur:

- Entities only gain permissions; they are withdrawn very late or not at all.
- Reporting and controlling the ‘who has permission to do what’ for all information systems and entities is cumbersome and insecure because of the following:
  - To be able to report or control permission, the ‘what’ should be described in a (natural) language that is meaningful in relation to the context of the process where the information is processed. But permissions are technical statements with system dependant syntax and semantic. It is hard to relate these different system semantics to the context of the process where the information is processed. This in turn makes it hard to derive or define what an entity is allowed to do with the information.
  - The functionality of permission statements must be implemented on the system level. This implementation in system privileges is system dependant and often does not exactly provide in what an entity must be allowed to do with the information as described in the context of the process. This can be seen as a functional requirement that the permission statement has on the system.
  - The ‘who’ is an entity, often defined by the information system as an account. But an account on an information system can be used by multiple entities, or an entity can use multiple accounts or accounts are not used at all. The entities using an account are not always deductable from the account registration. Which accounts on the various information systems are used by which entities?
  - The organization of many permission statements related to many accounts can be complex. Technical features like groups, tasks and roles are used to help organizing relating permission to accounts. But is it still possible to deduct the ‘net’ permission and is it still possible to relate this to the context of the process where the information is processed?
- Reporting and controlling the ‘why’ of permissions for all information systems and entities is cumbersome and insecure because of the following:
  - Information is not well protected if it’s not deductible why and for whom permission is granted.
  - The criteria on which permission is granted are often not defined. These criteria can for example be related to: organizational unit, job description, project member… or verbal qualities, trust and nice blue eyes. Without formal criteria, it is impossible to deduct why permission is granted.
  - Information is not well protected if there isn’t somebody responsible for the security and risk in respect to the information and functionality contained within the information system. (The ‘why’ as a risk management tool.) For example, who is creating and maintaining the criteria, who decides about granting permissions that are exceptional to the formal criteria?

14 Ongoing research

This research was an inspiration for further research, which is focused on creating a maturity model for IAM core processes and IAM related processes. Some general thoughts and concepts are described below. I would like to encourage anybody who is interested to contribute to the discussion.

To be able to use the general COBIT framework for specific topics, such as Identity and Access Management, the general descriptions need to be made specific. Specific IAM knowledge in the form of controls and good practices need to be imported into the framework. The following steps are followed to construct the IAM maturity model.


COBIT
Processes
Selection & mapping
Controls
COBIT
ISO27002
NIST SP800-53
Common IAM control good practices
COBIT processes Mapped controls
Justify selection for IAM
ISO27002
NIST SP800-53
ANSI INCITS 359-2004
Common IAM good practices
IAM good practice
Particularize and extend to IAM
Control Objectives (COBIT framework)
Activities (COBIT framework)
Goals and Metrics (COBIT framework)
Maturity Model (COBIT framework)
IAM control and maturity model

14.1 Selection and mapping

In the selection step is determined which processes and controls are related to IAM. Non-COBIT controls need to be mapped to COBIT processes, to be able to use the COBIT framework. Selected processes and controls should primarily pursue the general IAM business drivers, or should directly support the primary processes. The scope and usability of the model is very dependent of the regarded processes and controls.

In each business case where the model is applied, the relevance of the selected processes and controls should be regarded, in respect to the IAM business drivers of the specific business case. The priority of business drivers will have impact on the relevance of IAM processes and controls.

The selection is based on the following methods:

- Take the core of the IAM process in COBIT: Ensure Systems Security process (DS5) and in particular the control objectives: Identity Management (DS5.3), User Account Management (DS5.4). And select all inputs and outputs from/to other processes and control objectives.
- Identify the controls from the Code of practice for information security management (ISO 27002) that are related to IAM. Map these controls back to COBIT processes and control objectives, based on the 'Mapping of ISO/IEC 17799:2005 With COBIT 4.0' (study of ITGI)
- Incorporate experience from IAM projects and common IAM good practices to identify relevant missing COBIT processes or control objectives.

14.2 Justify selection

For the justification of the selected processes or controls, the following questions should be answered:

- How does the selected process or control pursue IAM business drivers?
  The relation can be direct or indirect, but should explicitly mention IAM business drivers and IAM processes or technology. It is not the intention to create another broad framework for IT governance, so indirect relations that do not have an explicit relation with IAM should be avoided.
- What is the relevance in respect to the IAM business drivers?
  The relevance can be expressed in the following terms: essential, important or supporting. Where essential expresses an indispensible relation and supporting is expressing a process performance improvement.
- For which circumstances or in which environment is the selected process or control most relevant?
  Examples of environments are: large/small organizations, large/small volumes of identities or applications in scope, expected growth of the IAM process scope, etc.
- What is the risk in respect to the IAM business drivers when the selected process or control is lacking?
  Risk is another expression of relevance, in terms of what can go wrong when the process or control objective is not in place. But, risk is very dependent of the organizational environment. The description of risk should provide enough information to identify possible risks and help organizations with their own risk analysis.

14.3 Particularize and extend COBIT

A selected and justified process or control needs to be combined with specific IAM knowledge to create a model that is usable in IAM projects. General statements need to be made specific for IAM and extended with IAM topics where appropriate. The structure of COBIT is followed.

14.3.1 Control Objectives

“A control objective is a statement of the desired result or purpose to be achieved by implementing controls in a particular process. A control is defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.” (7)

“IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. They:

- Are statements of managerial actions to increase value or reduce risk
- Consist of policies, procedures, practices and organizational structures
- Are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected” (7)

Control objectives need to be defined or reused from COBIT for the selected controls. Specific IAM controls can be introduced that are focused on IAM business objectives (directly following from the business drivers).

14.3.2 Activities

“Activities are the main actions taken to operate the COBIT process. In the COBIT framework, key activities and major deliverables are provided, and guidance on roles and responsibilities is also provided in a Responsible, Accountable, Consulted and Informed (RACI) chart.” (7)

For IAM, activities can be added that are main actions taken to operate COBIT processes, specific for IAM purposes. For example, creating deliverables that are needed to operate IAM processes or technology can be added as an activity.

14.3.3 Maturity Model

COBIT already has maturity levels defined for process management capability and internal control (COBIT 4.1 page 21 and appendix III), as is summarized in the following graph.

Figure 14—The Three Dimensions of Maturity

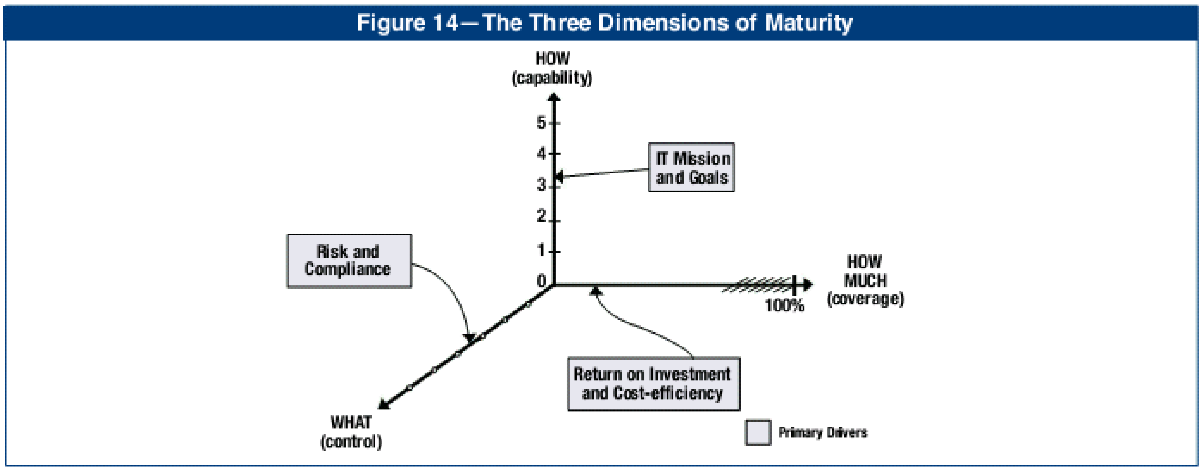


Figure 3 - source: COBIT 4.1, p. 19

These general levels can be reused, specific for IAM.

15 Bibliography

1. **Vleck van, Tom.** How the Air Force cracked Multics Security. [Online] Multics, 1993. http://www.multicians.org/security.html.

2. **Windley, Phil.** *Digital Identity.* s.l. : O'Reilly Media, Inc., 2005.

3. **Ministerie van Algemene Zaken.** Besluit voorschrift informatiebeveiliging rijksdienst 2007. *Staatscourant.* 2007, 122.

4. **IT Governance Institute.** *IT Control Objectives for Sarbanes-Oxley.* s.l. : IT Governance Institute, 2004.

5. **Weil, Steven.** HIPAA Security Rule. *securityfocus.* [Online] Security Focus, March 2, 2004. http://www.securityfocus.com/infocus/1764.

6. Quick and easy user provisioning. *Novell Identity Manager.* [Online] Novell. http://www.novell.com/products/identitymanager/provisioning.html.

7. **IT Governance Institute (ITGI).** *CobiT 4.1.* s.l. : IT Governance Institute (ITGI), 2007.

8. *SOX en Code Tabaksblat: tijd voor identity management?* **Best, Bart de.** 9, s.l. : ITbeheer, 2005.