



Deliverable 1.2

Control: Organisational Control

3.6.2007

Christian Liesegang, SAP AG
Mathias Kohler, SAP AG
Andreas Schaad, SAP AG

ORKA is funded by the German Ministry of Education and Research (BMBF) as part of its Software Engineering 2006 programme.



Contents

1 Introduction	4
1.1 Related Work	5
2 Organisational Control Systems	6
2.1 Organisational Types of Control	6
2.2 Control Principles	8
2.3 Organisational Maturity Models	10
3 Implementing Organisational Control.....	12
3.1 Organisational Control Framework.....	12
3.2 Organisational Control Architecture	13
3.3 Authorization Communication Sequence	14
4 Conclusion	16
4.1 Outlook.....	16
5 References.....	17

Introduction

Control is a central organisational function and results out of decentralization efforts. It is the means by which activities and resources are coordinated and directed towards the achievement of an organisation's goal and implies a degree of monitoring and feedback [6]. Salaman et al. argue that "Control means that members of the organisation have their actions, [...] determined, or influenced, by membership of the organisation." [19]. It is impossible to consider organisational control without considering the nature of power within organisations, how it is distributed and how it originates [19]. Figure 1 illustrates the three kinds of control defined by Hopwood [14].

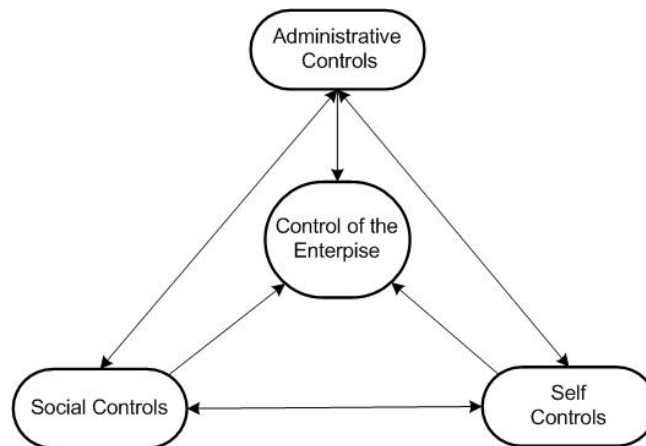


Figure 1: Types of Organisational Control

- Bedford described administrative controls as "Administrative controls relate to the structural composition of the organisation and the formal policies and procedures within the firm [...]. Structure is generally defined as relationship patterns within the organisation, and includes the configuration of business units, formal lines of authority and accountability, patterns of communication and information flows, and systems of corporate governance [...]. Policies and procedures conventionally relate to previously delineated concepts of personnel and behavioral control mechanisms, and include processes such as standard operating procedures, human resources management, management supervision and codes of conduct" [21].
- Self controls emphasize behaviors and actions that are encouraging the use of intuition through playfulness. It facilitates error detection and error correction instead of compliance and adherence with rules. Self-control focuses on the development of a large response to suggest not only alternative solutions, but also different approaches for executing those solutions [7].
- Social controls have been defined by Alvesson et al. [20] as "[...] efforts to persuade people to adapt to certain values, norms and ideas about what is good, important, praiseworthy, etc in terms of work and organisational life". These systems are particularly important in large organisations where communication of organisational purpose becomes increasingly difficult. Typical examples of belief or value systems include mission statements, statements of purpose, and corporate visions.

However, the focus of the ORKA project is on administrative controls, which may be defined as “..those mechanisms, techniques and processes that have been consciously and purposefully designed in order to try to control the organisational behavior(s) of other individuals, groups and organisations.” [22]. Two means by which administrative control may be achieved is through output control and rules and procedures.

Rules and procedures are the most explicit form of administrative control. One specific context in which such rules become inherently apparent is in the analysis and definition of business processes [15], commonly referred to as workflows. Here tasks can be broken down and be ultimately captured in the form of rules and procedures constraining the range of members’ behavior; increasing the predictability of their actions; and increasing the probability that perceived organisational requirements dominate that behavior [22]. Specifically with the recent trend to establish (partially) automated workflows such as credit applications, insurance claims, material ordering etc., this form of control has gained in importance [23].

On the other hand when it is not possible or feasible to define rules because of the complexity and unpredictability of the tasks that are performed, then output controls need to be established. The everyday accomplishment of tasks is left to the members’ judgment and discretion. This requires the ability to define and measure these outputs, as well as taking appropriate corrective or adjusting actions.

1.1 Related Work

In this section we focus on the discussion about the shift from the traditional administrative organisational control towards a more self-controlled, adaptive environment in organisational control systems.

Traditionally, organisational control is defined a priori. Thus, the underlying organisational goals have been predefined and there exists predefined procedural guidelines that need to be followed by the employees for achieving the company’s goals [7]. Systems are designed to enforce these guidelines.

Nalder [8] argued that these designed guidelines could result into locked-in behavior patterns resulting in a reduced organisational performance. Organisational control is considered as inhibiting creativity and initiative [9] by enforcing task definition, measurement, and control. A control system based on such measurements is considered to be rewarding maladaptive behavior leading to a decline of organisational performance. [8]

An opposed control model emphasizes the self-control principle. This principle is build upon the argument of changing environments and thus organisations have to behave experimentally and dynamically. Thus, organisational access control has to support experimentation and be easy to re-arrange and adapt with the changing business environment [10].

Malhorta [11] described a successful implementation of organisational control systems as driven by the simultaneously processes of ongoing learning, examination of assumptions behind best practices and reinterpretation of this information. They stated that the simultaneous processes are needed for assuring the optimization based on the current best practices. Thus, the design of an organisational control system needs to take into consideration ambiguity, inconsistency, multiple perspectives, and impermanency of existing information [10].

This section indicates the shifting from an administrative controls model towards a mixture of administrative control and self-control. Therefore, in the following section we will focus on the organisation control system itself and technological indicators demonstrating a potential shift from an administrative control system towards a more self-controlled system.

2 Organisational Control Systems

Figure 2 illustrates two different natures of control for organisation control discussed in the literature. The *loose* control system emphasizes self-control as the driver of human actors' behavior and actions across all organisational decisions, tasks, and processes. Self-control is based on the argument “[...] considering administrative control over employees as ultimately self-imposed” [12]. The other control system emphasizes a stable and predictable organisational environment with specification of rules and procedures according to the administrative control principle.

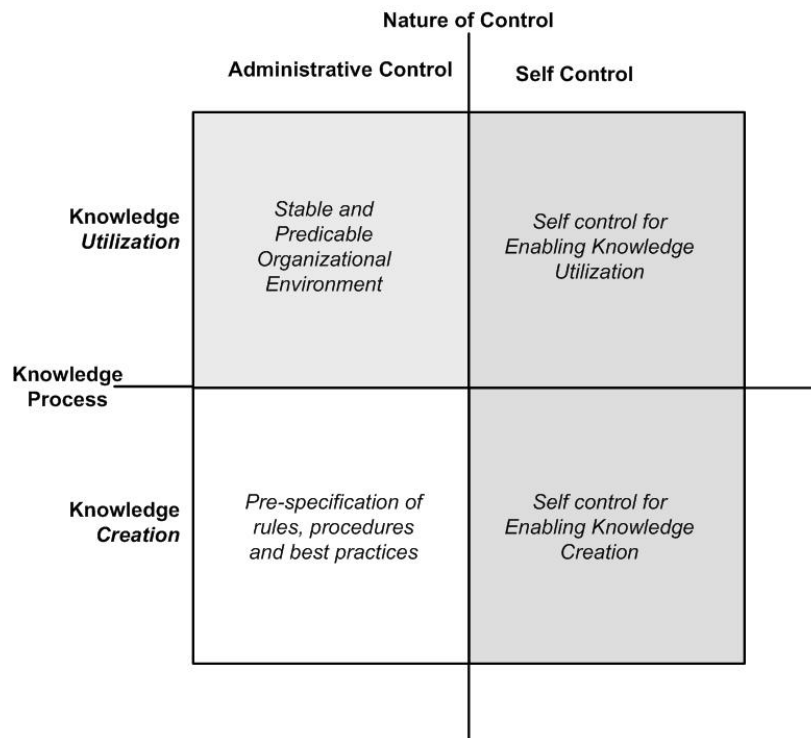


Figure 2: Contrasting external control vs. self-control [7]

2.1 Organisational Types of Control

In [7] it is described how the world economies move from the traditional model of workers to the new model of autonomous “free agents”. Thus, emergent organisations will need to nurture self-regulation as emphasis shifts from the external and administrative compliance control towards self-control, enhancing the competitive capabilities of an organisation with respect to the organisational goals and vision. The organisational information systems have to adopt these changes as well. The administrative organisational control system is based on the principles of:

- Knowledge Utilization as the Antecedent
- External Control as the Consequent
- Stable Environment
- Incremental Change
- Continuous, Predicable Nature of Change,
- Single Loop Learning
- Static View of Knowledge: Rules, Procedures & Policies
- Knowledge resides with the Management

Process-driven environments, process semantics, and service-oriented architectures reflect the change from the static administrative organisational environment towards a flexible, ad-hoc, and collaborative environment. Therefore, one vision of the ORKA project is to emphasize the shift from the stable environment to a more flexible self-controlled organisational structure and their information systems.

Administrative organisational control architectures are designed to support organisational structures, such as roles and departments. Activities related to a specific business goal are assigned to organisational roles and functional units. The control architectures and their control models, such as RBAC [1], are designed to reflect these static control paradigms. With the shifts to short-lived, flexible and changeable organisational environments the control models have to become more flexible, as well. New models, such as CoSAWoE [16], xoRBAC [18], or TMAC [2] are designed to be more flexible and support dynamic changes in the organisation and its environment. Processes and process choreographies replace traditional work division by procedures, ad-hoc collaboration, and best practices. With emerging trends such as adaptive and semantic process modulation [13], business activities are leaving the path of predictable work execution towards self-controlled knowledge activation. While these concepts are well developed for business-based interaction and collaboration, the underlying organisation control systems still stick to the administrative principles and do not keep pace with this evolution.

Therefore, the ORKA project emphasizes to provide an enabling administrative organisational architecture that is capable of accommodate principles of self-control, such as delegation, review, evidence, and revocation. While direct support for the self-control principles is definitely out-of-scope of the ORKA related implementation. The overall design of the ORKA architecture will provide mechanism to support self-control principles in some future work. Hence, the ORKA organisational control architecture will act as an enabler between control principles of administrative control and self-control.

2.2 Control Principles

A list of control principles and their related constraints in the current literature provides an overview of needs that have to be taken on by today's organisational control systems. Various types of requirements can be identified in an organisation's system landscape. The types of control requirements arise from different system domains, for instance, in database systems common control requisites are based on roles to restrict the access to the system, its tables and stored data. Also, operating systems rely on a user-role assignment to manage access authorizations. Control requirements for business processes are driven by activity related constraint types, e.g. four-eyes-principle or binding of duties. We have identified various types of control principles in recent publications. We list them along with a general description, and an illustrative example in Table 1. In [3], a classification model of access control requirements is given for organisational administrative control. As illustrated in Figure 3, besides classical static control requirements, new dynamic requirements emerged with process-driven and orchestrated business activities.

Table 1: Access Control Principles

Principle Type	Description
Authentication, Identification	Constraints that a subject must be identified before authorization are granted. <i>Example:</i> Subject has to present an identification certificate.
Cardinality	Restricts the amount of executions of a certain task or activity. <i>Example:</i> A task in a certain business process may only be executed five times by the same subject.
Business Roles (authorization based on roles)	Restricts permissions according to the role a subject is member of. <i>Example:</i> Only subjects being member of role X are allowed to access object Y.
Binding of Duties	Obligation to perform a certain activity resulted by (omitting) the execution of a previous activity. <i>Example:</i> A subject is obliged to perform task t if it did task t'.
Separation of Duties	Constraint which prevents a subject performing exclusive activities. <i>Example:</i> Task t and t' may only be performed by different subjects.
Environment Attributes	Constraint which restricts access based on environmental attributes. <i>Example:</i> A task may only be performed between 8 a.m. and 5 p.m.
Subject Attributes	A constraint which grants/restricts access based on attributes of a subject. <i>Example:</i> Subject A is allowed to perform task X if there exists no family-relationship between subject A and subject B.

Authorization Classes	Dynamic Authorization	Activity Authorization	Separation of Duty Binding of Duty Cardinality
		Environment Authorization	Environment Attributes Subject Attributes
	Static Authorization	Ontology Authorization	Business Roles
		Authentication	Identification

Figure 3: Classification Model for Access Control Principles

Considering self-controlled organisational control principles, introduced in the previous section, control principles cover more than this list of administrative control principles given in Table 1. A lot of theoretical work is done in [4] focusing on the formal definition of the concepts of delegation, review, evidence, revocation and the possible schemes and their practical feasibility embracing self-control for organisational control systems. Supporting these concepts is vital for the utilization of existing knowledge. Control principles for self-control processes imply the possible delegation, review, evidence, and revocation of activities due to knowledge utilization without the direct interference of the management.

We will now describe the concepts behind these self-control principles for organisational control in more detail:

- Delegation may be used as a term for describing how duties and the required authority propagate through an organisation, usually in terms of the refinement of a high-level organisational goal into manageable policies which eventually lead to the execution of some task [5].
- Evidence determines what the later discharge of a delegated duty has to produce to convince the delegator that the duty has indeed been performed [5].
- Review is understood as an obligation referring to a previously delegated obligation which has to examine the results of the discharge of this delegated obligation. The holder of such a review policy has then to make sure that the obligation he delegated has been carried out satisfactorily [5].
- In general, revocation of duties and the required authority is based on its previous delegation and thus requires information, such as the actors involved in previous delegation, when this delegation took place and the actor that received the delegation. In the literature several types of revocation are identified, such as strong and weak revocation related to delegation chains between several actors and hierarchies [5].

These concepts allow human actors to utilize their knowledge by delegating specific activities to others that are more suitable for specific tasks, because of valuable knowledge the management is not aware of. Self-control principles foster proactive reactions without consulting or involving the

management in emergency or unexpected situations. Therefore, organisational control systems have to support such concepts optimizing a priori defined restrictions actively.

2.3 Organisational Maturity Models

The degree of required as well as realizable control within an organisation depends on the relative maturity of the organisation. Organisational maturity models such as C2 [29] identify levels of organisational maturity which in turn describe the ability of organisations to interoperate. The five identified levels as indicated by Figure 4 are (0) independent; (1) ad hoc; (2) collaborative; (3) combined; (4) unified.

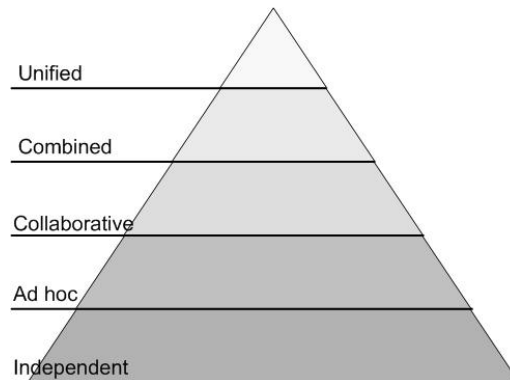


Figure 4: Organisational Levels [29]

- **Independent** - Independent organisations that would normally work without any interaction other than that provided by personal contact are described by the interoperability level 0 [29].
- **Ad hoc** - At this level of interoperability only very limited organisational frameworks are in place which could support ad hoc arrangements. Interoperability will be described by some guidelines. Interoperability occurs, but essentially the specific arrangements are still unplanned [29].
- **Collaborative** - Collaborative organisations are still distinct, but recognised frameworks are in place to support interoperability. Shared goals are recognized as well as roles and responsibilities and are allocated as part of on-going responsibilities [29].
- **Integrated** - The integrated level of organisational interoperability is one where shared value systems and shared goals are in place to foster a common understanding and a preparedness to interoperate [29].
- **Unified** - A unified organisation is interoperating on continuing basis. The basis describes which organisational goals, value systems, command structure/style, and knowledge is shared across the system [29].

Four attributes have been identified as the enabling attributes of organisational interoperability, such as [29]:

- **Preparedness** - This attribute describes the preparedness of the organisation to interoperate. It is made up of doctrine, experience, and training.
- **Understanding** - The understanding attribute measures the amount of communication and sharing of knowledge and information within the organisation and how the information is used.
- **Command Style** - The management and command style is the attribute that describes how decisions are made and how roles and responsibilities are allocated or delegated in an organisation.
- **Ethos** - The ethos attribute is concerned with the culture, trust, and value systems of the organisation and the goals and aspiration of the organisation.

Such models may further motivate the need for workflow systems that allow organisations to collaborate and advance in maturity. At the same time such workflow systems may also serve as the context providing source for interpreting organisational control policies. Table 2 summarizes the organisational interoperability levels and attributes:

Table 2: Summary of Organisational Interoperability Reference Model [29]

	Preparedness	Understanding	Command Style	Ethos
Unified (4)	Complete – normal day-to-day working	Shared	Homogenous	Uniform
Combined (3)	Detailed doctrine and experience in using it	Shared communication and shared knowledge	One chain of command and interaction with home organisation	Shared ethos but with influence from home organisation
Collaborative (2)	General doctrine in place and some experience	Shared communication and shared knowledge about specific topics	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose; goals, value system significantly influenced by home organisation
Ad hoc (1)	General guidelines	Electronic communication and shared information	Separate reporting lines of responsibility	Shared purpose
Independent (0)	No preparedness	Communication via phone ect	No interaction	Limited shared purpose

3 Implementing Organisational Control

In this section we discuss the underlying conceptual model for control principles and develop a first design of an information system supporting control principles introduced in the previous section.

3.1 Organisational Control Framework

Authorizations are used to provide control mechanisms within the organisation. Policies describe the underlying rules, such as who might perform some business activity. Thus, in this section we present a conceptual model organisational control principles are based on. The modeled entities will appear in any information system supporting access control. The following entity-relationship diagram shown in Figure 5 is taken from [6]. The elements will be described in detail below:

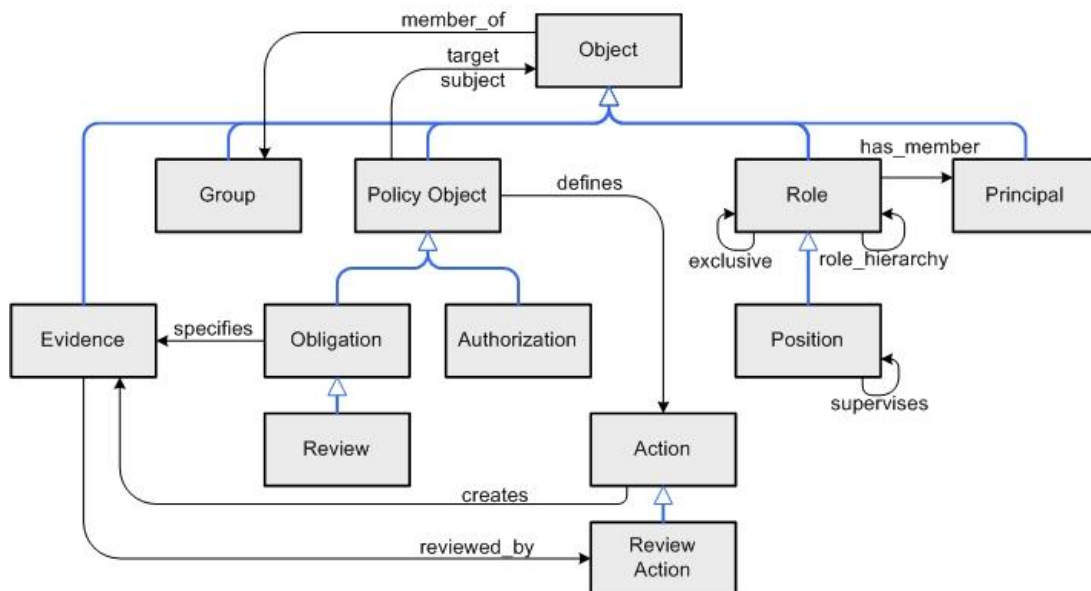


Figure 5: Conceptual Control Principle Model [6]

All entities are extended from a general object entity. Objects can be members of groups. Because a group is derived from an object, the group itself may be a member of another group. A principal is an object representing a human actor or an automated system component. A policy is a representation of a rule determining the behavior of principals. A policy can be differentiated into an obligation or an authorization. Policies apply to subjects, e.g. an individual principals or role, and targets. Policies define actions that have to be performed (obligation) or may be performed (authorization). Evidence is created whenever an obligated action is performed and represents some kind of investigable proof whether the action was performed or not. Review actions investigate evidences and are created when an obligation is delegated. Roles are composed out of hierarchies and mutual exclusivity. Positions are context enriched roles used to describe supervision relations through the inherited role hierarchy relation.

3.2 Organisational Control Architecture

The previously presented control principle model allows describing several types of access control principles, such as dynamic separation of duty aspects, obligations, exclusive roles, role hierarchies, delegation, revocation, review, and evidence. Figure 6 presents a conceptual model of system entities that implement organisational control based on the control principle model. Four major components can be derived according to the conceptual control principle model, such as the Policy Manager, the Organisational Context Provider, Authorization Engine, and the Business Activity Manager. Together these four components build up an organisational control architecture described in detail in the following paragraph.

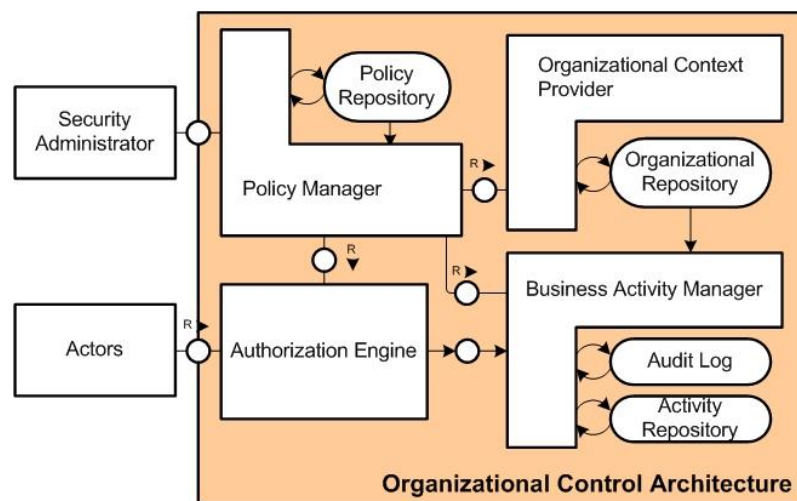


Figure 6: Organisational Control Architecture

- The Organisational Context Provider manages information about an organisation's principles, their role assignment, and role hierarchies. All this information is stored in an organisational repository. Such repository may range from simple file based storage to more sophisticated directory services, such as the LDAP or Active Directory service.
- The Business Activity Manager stores a repository containing all business related activities. Therefore, all activities used to achieve a certain business goal should be orchestrated in a workflow definition, describing what steps have to be performed in order to achieve a specific goal. An activity is an arbitrary complex entity hiding all involved application logic, backend systems, and access to resources (e.g. file access). In combination with an organisational repository each business activity is assigned to a single principal or a role. An audit log stores all business activity related audit data. Thus, information about what was done, when, and who performed the activity is available for monitoring and security purposes. In general workflow management and business process management systems, such as jBPM [24], SAP WebFlow [26], or Bonita [25], provide the necessary functionality of a business activity manager.
- The Policy Manager is used to define authorizations and obligations for specific activities by a security administrator. Policies are stored in a special repository. To provide basic organisational control policies, such as RBAC [1] or TBAC [17] the policy manager needs to communicate with the organisational context provider and the business activity manager. This allows importing organisational context and business information into the policy manager. The access to contextual information enables the definition of policies

based on user-role and role-activity assignments. Advanced security policies, such as delegation and dynamic separation of duty can only be defined with access to activity audit logs to allow runtime detection of policy violation, for instance to detect separation of duty violation.

- The Authorization Engine acts as a decision and enforcement point for access control policies. Whenever an actor wants to perform a business activity the access request has to be mediated through the Authorization Engine. Consulting the current state of the related business activities and based on policies defined by the policy manager the Authorization Engine may allow the request and grants access to the requested business activity and guarantees that all necessary permissions to complete the business activity are granted in the related backend systems and applications. If the policy evaluation results into a negative decision the request will be denied.

3.3 Authorization Communication Sequence

In this section we illustrate the message flow between the different components of the organisational control architecture that takes place, whenever some business activity is going to be performed by an actor.

Whenever an actor wants to perform a business activity that is protected by the organisational control architecture, all requests are intercepted by an authorization enforcement point. The authorization point is not capable of making an access decision on its own. Therefore, the authorization enforcement point will request a decision from the authorization decision point. To make a decision the decision point queries the policy manager for all policies that are affected to this request. Thus, all policies that apply to the identity of the actor, his role, and policies related to the requested activity and the corresponding workflow are prompted from the policy manager. The policy manager will browse through its policy repository and returns the set of affected policies to the decision point. Some of these policies may contain dynamic constraints depending on the current system state and process history. To get this information the decision point will ask the business activity manager for the current process state. The business activity manager selects all relevant state information and returns it to the authorization decision point. Now the decision point is able to evaluate the static and dynamic policies. Depending on the used rule base (e.g. deny overrides permit) the binary authorization decision is returned, i.e. *access denied* or *access granted*. In the case the access request is denied, the enforcement point will mediate this decision to the actor, for instance as some error message. In the case access was granted. The intercepted request is forwarded to the activity manager hosting all business activities. The activity manager will initialize the activity and passes the original request to it. The business activity is performed and it will be sending back potential results to the actor. The described message sequence is depicted in Figure 7.

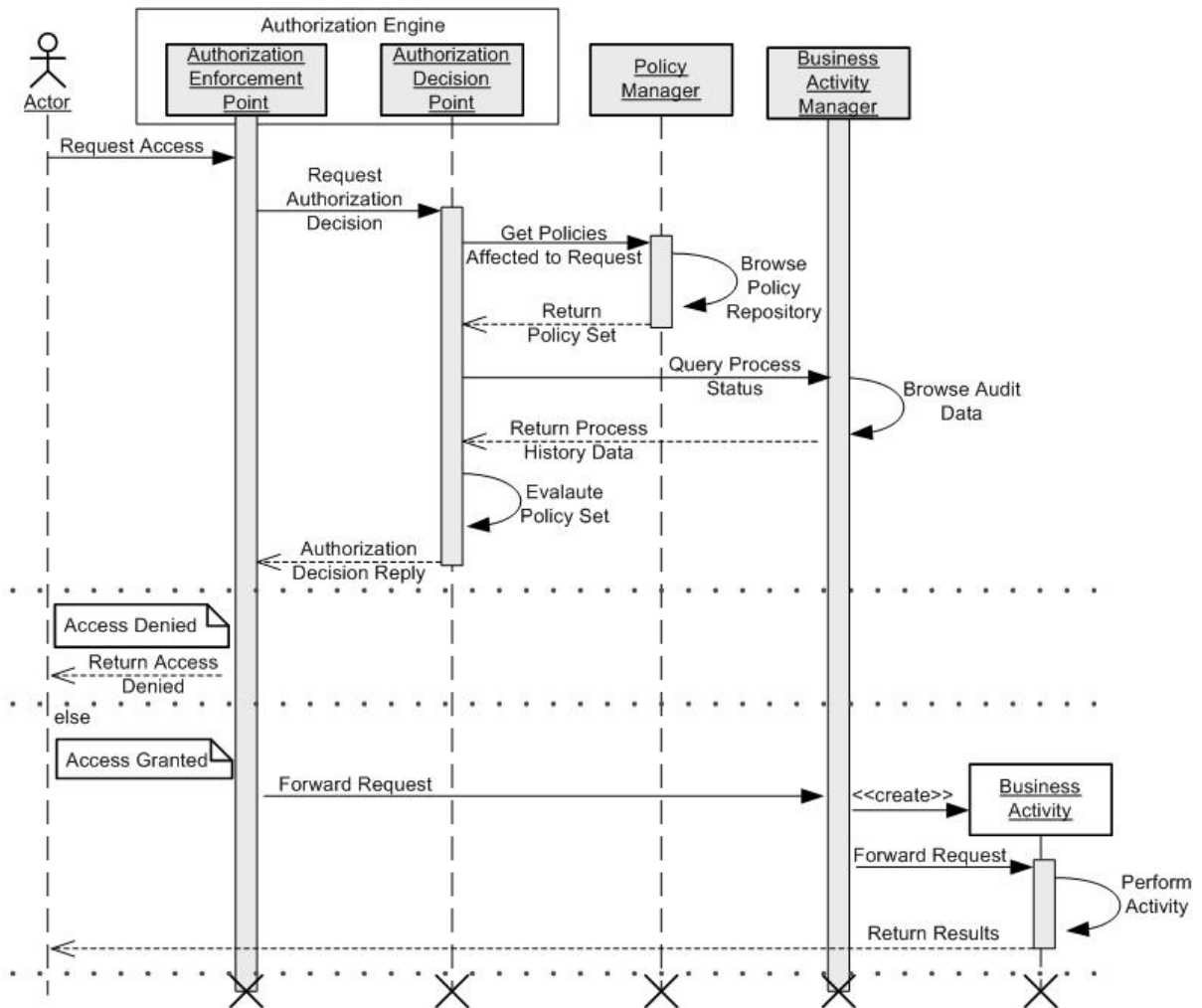


Figure 7: Authorization Enforcement & Decision Sequence

Figure 7 contains some assumptions and simplifications. For instance, we assume the actor's identity and organisational role is already known in the control architecture. Otherwise the actor has to identify himself against some trusted authority or authentication mechanisms. The first one could issue some kind of identity certificate that can be verified by the control architecture, the later one would request the actor's password before the access request will be accepted by the authorization enforcement component.

A second presumption is availability of organisational context data. This data would contain information about the roles the actor possesses and what activities can be performed by the possessed roles. Therefore, the querying of an organisation repository is omitted in this sequence diagram for purposes of clarity.

As a simplification we omitted the logging of audit data performed by the business activity manager while a business activity is requested, performed, and finished. Nevertheless, this information is mandatory with respect to the enforcement of dynamic separation of duty control principles, such as operational or history-based separation of duty.

4 Conclusion

In this paper we presented an overview about the basics of organisational control. We described three different types of organisational control, such as administrative, self-controlled, and social organisational control. While the later is generally not considered in the area of access control for human-centric workflows, the first two control aspects are well known and analyzed in the literature.

We listed various access control principles in the area of administrative access control, such as separation of duty, obligations, and organisational roles and their mapping to business activities arranged in workflows. On the other hand we discussed the slightly shift from sheer administrative control principles towards some self-controlled organisational control principles, such as delegation, review, and evidence.

Further, we presented a general conceptual model for control principles, first introduced in [6]. Based on this model we identified the essential entities and developed a first abstract model of an organisational control architecture supporting the conceptual model. The major components of our proposed architecture provide organisational context information, such as user-role assignments and role-activity assignments. A business activity manager orchestrates an organisation's business activities into workflows. The workflow definitions are necessary to support dynamic control principles, such as dynamic separation of duty. The authorization engine and the policy manager are used to define organisational policies and the enforcement of such policies at runtime.

A sequence diagram provided a first glimpse of the communication channels and the control flow within the proposed organisational control architecture. This work package is intended as a primer for ORKA's other subject areas, especially tailored for the subject area ENFORCE, ADMIN, and SPEC.

4.1 Outlook

In the subject area SPEC the conceptual model for control principles is used to analyze existing access control models and evaluate the expressiveness based on the matching of their underlying models and the conceptual model we provided.

The subject area ENFORCE is going to start their technical analysis of existing enforcement technologies with respect to our abstract organisational control architecture. Onwards, different workflow management systems are evaluated for their capabilities to act as a business activity manager. Therefore, several workflow engines will be evaluated, such as jBMN, Bonita, or NetWeaver's WebFlow. Eligible directory services and resource management systems have to be evaluated for querying and extracting organisational context information by the authorization engine. In addition, policy administration frameworks such as Ponder [27] or the Parks Security Manager [28] are considered as potential policy management systems.

The conceptual model for control principles also influences the subject area ADMIN. Thus, expressiveness requirements can be derived from the model to support static control policies, such as user-role and role-activity assignments and dynamic control principles defined in the context of workflow-based activity choreographies.

5 References

- [1] D. Ferrailo, R. Kuhn, *Role-Based Access Control, 1992*, 15th NIST-NCSC National Computer Security Conference.
- [2] R. K. Thomas, *Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments*, RBAC '97: Proceedings of the second ACM workshop on Role-based access control, 1997
- [3] C. Liesegang, M. Kohler, A. Schaad, *A Classification Model for Access Control Constraints*, 2007
- [4] Andreas Schaad, *Revocation of obligation and authorisation policy objects*, 2005
- [5] Andreas Schaad, *An Extended Analysis of Delegating Obligations*, 2004
- [6] Andreas Schaad, *A Framework for Organisational Control Principles*, 2003
- [7] Y. Malhorta, *Organisational Controls as Enabler and constraints in Successful Knowledge Managemet Systems Implementation, 1998*
- [8] D.A. Nalder, R.B. Shaw, *Change leadership: Core Competency for the Twenty-First Centruy*, Jossey-Bass, San Fransisco, CA, 1995
- [9] C.A. Bartlett, S. Ghoshal, *Changing the Role of Top Management: Beyond System to People*, Harvard Business review, May-June, 1995
- [10] B. Hedberg, S. Jonsson, *Designing Semi-Confusing information Systems for Organisations in Changing Environments*, Accounting, Organisations and Society, 1978
- [11] Y. Malhotra, L. Kirsch, *Personal Constrcut Analysis of Self-Control in IS Adoption*, In the Proceeding of the first INFORMIS conference, May, 1996
- [12] D.J. Cooper, D. Hayes, F. Wolf, *Accounting in Organized Anachies; Understanding and Designgin Accounting Systems in Ambiguous Situations*, Accounting, Organisations and Society, 1981
- [13] Michael Adams, Arthur H. M. ter Hofstede, David Edmond, and Wil M. P. van der Aalst, *Worklets: A Service-Oriented Implementation of Dynamic Flexibility in Workfows*, 2005
- [14] A. Hopwood, *Accounting Human Behaviour*, Prentice-Hall, London, UK, 1974
- [15] H. Mintzberg, *Impediments to the Use of Managementt Information*, National Association of Accountants ,1975
- [16] Reinhardt Botha, *CoSAWoE – A Model for Context-sensitive Access Control in Workflow Environments*, 2001
- [17] R. K. Thomas, R. S. Sandhu, *Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management*, Chapman & Hall, 1997

- [18] Mark Stembeck, Gustaf Neumann, *An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments*, Vienna University, 2003
- [19] G. Salaman, K. Thompson, *Control and Ideology in Organisations*. The Open University Press, 1980
- [20] M. Alvesson, D. Karreman, *Varieties of discourse: On the study of organisations through discourse analysis*, 2000
- [21] D. Bedford, *Management Control Systems Configurations in Practice*, 2004
- [22] P. Johnson, J. Gill, *Management Control and Organisational Behaviour*. Paul Chapman Publishing, 1993
- [23] A. Cichocki, A. Helal, M. Rusinkiewicz, and D. Woelk, *Workflow and Process Automation*. Kluwer Academic, Boston, 1997
- [24] J. Koenig, *JBOSS jBPM*, 2004
- [25] M.V. Faura, C. Loridan, A. Geron, R. Perey, *BONITA Workflow Management System*, 2006
- [26] SAP Corporation, *SAP NetWeaver Security Guide*, help.sap.com
- [27] N. Damianou, N. Dulay, E. Lupu, M. Sloman, *Ponder: A Language for Specifying and Management Policies for Distributed Systems*, 2000
- [28] Parks Informatik GmbH, *Mit Sicherheit zu erhöhter Effizienz bei gleichzeitiger Kostenreduktion in der IT*, www.parks-informatik.de
- [29] T. Clark, R. Jones, *Organisational Interoperability Maturity Model for C2*, 1999