Separation, Review and Supervision Controls in the Context of a Credit Application Process
–
A Case Study of Organisational Control Principles

Andreas Schaad
Information Systems Assurance & Advisory Services
Ernst & Young LLP
1 More London Place, London, SE1 2AF
Email: aschaad@uk.ey.com

Jonathan Moffett
Department of Computer Science
University of York
York YO10 5DD, United Kingdom
Email: jdm@cs.york.ac.uk

ABSTRACT
This paper presents a case study of the organisational control principles present in a credit application process at the branch level of a bank. The case study has been performed in the context of an earlier suggested formal framework [6] for organisational control principles based on the Alloy predicate logic and its facilities for automated formal analysis and exploration [2].

In particular, we establish and validate the novel concepts of specific and general obligations. The delegation of these two kinds of obligations must be controlled by means of review and supervision controls. The example of a credit application process is used to discuss these organisational controls.

Categories and Subject Descriptors
H.1 [Models and Principles]

Keywords
Management, Security, Control Principles, Review, Supervision, Delegation of Obligation, Roles.

1. INTRODUCTION
Organisational control principles, such as those expressed in the separation of duties, delegation of obligations, supervision and review, support the main business goals and activities of an organisation. A framework has been presented [1, 6] in which organisational control principles can be formally expressed and analysed using the Alloy specification language and its constraint analysis tools [2]. Specifically the delegation of obligations and arising review obligations have been treated in detail [3]. Much of these earlier discussions were influenced by the insights gained into the working and administration of the access control system of a major European bank and the involved control principles [4].

This paper attempts to close our investigations by presenting a case study about the control principles involved at a particular branch of that bank[1]. In particular, it validates the concept of specific and general obligations. These allow for the explanation of review and supervision as controls on the delegation of obligations in the context of a credit application process.

This rest of this paper is structured as follows. Section 2 provides some background information on the specific branch of the bank and the different types of control. Section 3 will then provide an initial description of a credit application process. The established framework for control principles is then informally summarised in section 4, specifically making the distinction between general and specific obligations which is required for establishing the concepts of review and supervision. Section 5 then summarises our findings of modelling and analysing the credit application process in the context of the control principle framework.

2. Background
The particular branch of the bank we investigated is a medium-sized branch with respect to its annual turnover and amount of customers. It provides services for some thousand individual customers, as well as for companies with several dozen to hundreds of employees. The monetary assets that are involved easily exceed a few million Euro and control over business activities such as share trading, credit or mortgage management is a stringent requirement. About 30 Employees work in the branch. Apart from the general Clerk there are specific roles that may be informally described as *Head of Branch*, *Private Customer Advisor*, *Business Customer Advisor* and *Mortgage Advisor*.

Different kinds of control are enforced at different conceptual levels. For instance, we found simple integrity checks encoded in the application logic and user interface; controls enforced through a specific workflow sequence and separation of tasks; controls in the form of the assignment of an employee to a specific group and role; as well as post-hoc controls through the internal audit department. Before we consider the credit application process in more detail, we will give some general examples of the kinds and levels of control that we observed.

ACM SAC '04, March 14-17, 2004, Nicosia, Cyprus.

[1] This work has been performed entirely at the University of York and is not linked to the first author's current work at Ernst&Young, London.

2.1 Controls enforced through application logic and interface design.

One example we have seen is that of a stock trading application. Here a financial advisor cannot buy or sell stocks without appropriate funds. The application will refuse to execute the order. This may sound obvious, but there are in fact specific trading techniques where this control might not be desirable. For example, depending on the seniority of the advisor, he may buy shares for a customer although the customer does not have the appropriate funds at that current moment. This is possible because the advisor knows that, for example, the interest of the customer's government bonds will be due the next day. The advisor may thus give the customer a 24 hour credit. Specific dual controls are in place to cater for such situations.

We also know that this share trading application is able to analyse the trading activities of an advisor. If suspicious patterns emerge, the application may automatically notify a different advisor for reasons of dual control.

2.2 Controls enforced by organisational structure and workflow design

Apart from controls such as two required signatures or other forms of dual control, various forms of separation controls and Least Privilege principles are applied. One example is that of an advisor only having the authority to view accounts of customers of the branch he works for. A different kind of operational separation is that an advisor selling a packet of shares for a customer may not transfer the equivalent amount of money to any other account than the current account of the customer. Otherwise he might sell shares and transfer the money to an account he owns himself. Any transfer to other accounts needs to be done by a different person. In this particular case we observed that this person was in fact located outside the branch in the regional headquarters.

2.3 Controls enforced through internal audit and supervision

Post-hoc controls in the form of internal audit are probably the most common form of control, as they do not obstruct or delay any specific business activity. For example, the bank will monitor if shares are traded for an employee of the bank in order to detect any insider trading. A different example is that the head of the branch is automatically notified of customers not paying back a credit. If he does not acknowledge that these 'foul' credits were brought to his attention, the next superior will be notified, and the case will receive a higher escalation number until it is resolved. The general rule is that the higher the sum at stake the more controls are enforced.

3. A credit application process

A standard service provided by a bank is that of offering credits to its customers. This may take various forms such as extending the overdraft limit on a current account; providing mortgages for buying a house; or simply offering a fixed sum of money the customer may use at his discretion. Depending on the specific kind of credit, the application process will differ in the principals involved and data that need to be considered. In fact, the specific type of credit requested will have a direct effect on the involved controls.

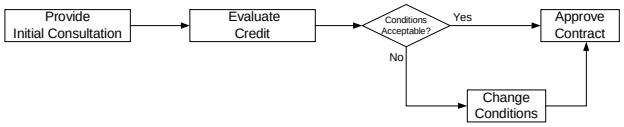

Figure 1: Credit Application Process

In the following we provide a simple example of a customer applying for a credit supported by figure 1.

A customer applies for a sum of 10,000 Euro. Together with his advisor he will fill out a credit application, usually in an electronic form. Apart from his personal details, this form will require information about his financial situation, e.g. current salary, any offered securities or other assets. The application will then gather information about the customer's credit history using an external credit database. Interestingly, German law requires the customer's consent for this in the form of a signature. Advisors may not obtain this information at random, an example of an external, law-enforced, control. The application will then use the data that were obtained to evaluate whether the customer should be granted a credit and under which conditions this should be done. If the decision is positive, then a contract is generated which becomes legally binding with the customer's signature. In this case, control and credit approval is solely enforced through the application logic.

There are, however, situations which require other forms of control. We consider the following two examples. In the first example, the customer is rejected the credit of 10,000 Euro by the application. The advisor may, however, still provide the credit since there are circumstances on the customer's side which, in accordance with the organisational regulations, satisfy its approval.

The second example may be that the application approved the credit, but the advisor agrees to lower the interest rate by a certain percentage. In both cases the control described in the following paragraph is enforced.

Any transactions which show deviations from normal business practice will be brought to the attention of the advisor's superior. This is done in the form of a new entry in the superior's monitoring application. This monitoring application will keep a general list of transactions that require his attention or approval. In fact, this application will provide detailed information about the involved employees, kind of transaction and priority of the transaction. The superior may approve the transaction through a mouse click. Since he has been fully authenticated to the machine and application, this approval is binding on him. We have no knowledge of the immediate effects of his approval or rejection. However, it is likely that certain transactions will only commit with his approval, while other transactions will commit without his approval and some kind of correction is performed in case of the superior's rejection. Speaking to staff at the branch, they asserted that a high level of informal trust is part of a superior's and subordinate's relationship, which is in fact perceived as part of the corporate culture. In the case of the credit application scenario this means that the advisor will only agree to provide a credit under conditions he knows his superior will approve. Likewise, a superior will usually rely on the integrity of his subordinate's decisions.

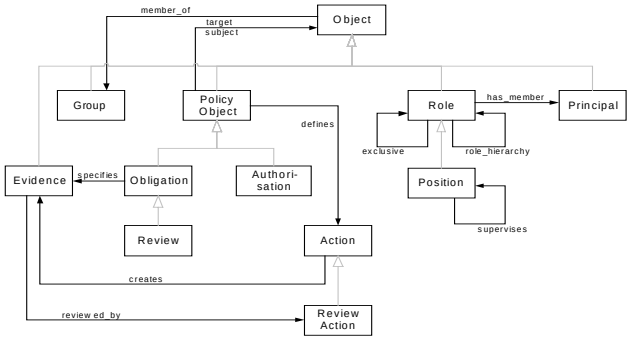

Figure 2: The Control Principle Framework

This system of approval is, however, not always based on an existing superior-subordinate relationship. Certain transactions only require approval from a peer, a basic dual control. We could not obtain information how far this approval and monitoring system is linked to the notion of roles as described by us in [4]. Also, there is no single hierarchical role structure for this branch, but several hierarchies exist for different purposes. For example, the head of the branch is the general superior for the branch staff considering general disciplinary measures. This does, however, not necessarily allow him to give specific orders to the senior private customer advisor. This advisor is subject to the directives of a superior in the Bank's regional headquarters with respect to his daily duties as an advisor. We have discussed this issue of multiple role hierarchies in the more general context of automated enterprise administration in [5].

4. A control principle framework

Before investigating the identified control principles in more detail, the framework established in [1] and [6] needs to be revisited. This is done in an informal manner without any formal Alloy specifications or examples of automated constraint analysis. The structure of the conceptual model we use as the basis for the specification, analysis and exploration of control principles is displayed in figure 2. This representation gives only a first overview of the most basic elements and relationships and must not be mistaken for the entire model. Each box represents an object type which is called a signature in Alloy and the open headed arrows represent type extension.

Objects can be members of Groups. A group is itself an object and may thus also be a member of some other group. A Principal is an object representing a human user or automated component in the system. A Policy Object is an abstract representation of a rule determining the behaviour of principals in the system. A policy object is either an Authorisation or an Obligation and can have subject and target objects it applies to. This is an established concept in the policy community and we refer to [12] for a more detailed discussion. Policy objects may be related to a principal either directly or through a Role he is a member of, since policy objects may have principals or roles as their subject. Policy objects define a set of Actions. In the case of obligations these are the actions that have to be performed and in case of authorisations the allowed actions. Execution of an action may create Evidence which is specified by an obligation such that it can be investigated whether the obligation was satisfactorily met. A Review is a specific kind of obligation and results out of the previous delegation of an obligation. Review Actions are a specific kind of action and evidence is reviewed by them. Two role specific relations allow for the formation of role hierarchies and the definition of mutually exclusive roles. A Position is a specific kind of a role with some associated, context-dependent, attributes describing the more permanent and long-lived representation of a principal in an organisation. Positions can be part of supervision hierarchies.

4.1 Authorisations and obligations

Authorisations state what a principal is permitted to do on the basis of using the actions defined by the authorisation. In this context only positive authorisations are considered since policy objects do not have any explicit modality (compare, e.g. [2]). Obligation policies are an abstraction for defining the actions that must be performed by a principal on some target object when some specified event occurs. While this definition reflects our understanding of obligations, it requires a more detailed discussion on the requirements this raises with respect to the Alloy specification.

To begin with, this specification is mainly concerned with structural properties. The possibilities to model dynamic behavior are limited to simple sequences of states. This means that there is no event architecture as in, for example OASIS [7], that would allow us to explicitly model triggering events. This, and the current representation of obligation policies does at this stage not allow us to clearly represent:

- what it means for a principal to hold an obligation;
- how obligations relate to roles.

We consider a general obligation policy which specifies that clerks have to process customer orders for money transfers. The defined event on which the obligation arises might be the arrival of an order in the clerk's inbox. When this event occurs, the clerk now has the specific obligation to process this order.

The problem is that the control principle model we have developed so far is primarily a structural model, using roles as a convenient administrative shorthand over which to relate principals and policy objects. It does at this stage not allow us to describe situations such as the previous order processing example. Additionally, it is not yet clear how principals are related to obligations when roles are involved. If a principal is a member of a role, he then has the authorisations of that role at his discretion. Since several principals may be a member of the same role, this means that the same authorisation applies to several principals. This does not raise any conceptual difficulties. However, in the case of obligations this relationship requires further clarification as there initially seem to be two contradicting requirements. On the one hand it is desirable to specify an obligation that applies to several principals and roles appear to be the ideal structural means for doing so. On the other hand an obligation should be clearly related to one principal only, such that it can be assessed who can be held to account at any time. Also the same actions must not be performed twice. This is of even more importance when considering the delegation of obligations.

The problems described in the previous section can be resolved on the basis of the general assumption of this model that a distinction must be made between general and specific obligations. This means that principals may have the same general obligation through a common role, but the specific obligation instances of this general obligation must be directly related to exactly one principal. The sharing of specific obligations between principals is therefore excluded. This elegantly supports the delegation of obligations, since a specific obligation can only be delegated between principals subject to the same corresponding general obligation. To summarise, the following requirements and assumptions have been discussed in this section and we refer to [6] for a more detailed and formal discussion:

- A distinction between general and specific obligation policies needs to be made.
- General obligations may be shared between roles or principals, but a specific obligation must always be related uniquely to a principal.
- Specific obligations have been created based on some general obligations. There is no explicit architecture to model triggering events and this creation is outside the scope of this model.

4.2 Delegation of obligations

Limited organisational resources (e.g. time) require the delegation of obligations. We distinguish between the

- the delegation of specific obligation instances;
- the delegation of general obligations.

The first kind of delegation is what we considered as an ad hoc form of delegation, allowing individual principals to distribute obligations more efficiently. The concept of review controls this form of delegation. The second form of delegation is perceived as a management activity with the aim of creating a more permanent form of organisational structure through the distribution of work. We believe that the concept of supervision is a control principle that supports this form of delegation.

4.2.1 Review and evidence

When an obligation is delegated, it may be made subject to a review obligation. A review is defined as a specific type of obligation by using Alloy's object extension mechanism for the review signature as graphically indicated in figure 2. It has a previously delegated obligation as its target through the target relation of the policy object it is extended from.

Evidence determines what the later discharge of such a delegated obligation has to produce to convince the delegator that the obligation has indeed been performed. At this level, evidence serves as an abstraction for what eventually has to be produced, but not that it has been produced. The later would require a notion of discharging and enforcing obligations (compare, for example, [8]) which is not part of this framework.

The natural question to ask is how this concept of a review integrates with the definitions made in the previous section 4.1, that consider the distinction between general and specific obligations. Alloy does not initially assume that an extended signature is disjoint from the signature it is extended from. This is used as a convenient way of capturing that there may also be general and specific review obligations. Not having defined a review to be disjoint, a review may thus assume the type of an obligation or obligation instance.

What are the effects of these assumptions? It must have been defined earlier how a review is performed. 'Earlier' in this case means that at the time a general obligation is assigned, the corresponding general review is assigned in parallel if delegation and review have to be supported. Thus, when an obligation instance is delegated, a review instance is created on the basis of the corresponding general review obligation. This instance now defines what review actions have to be performed on some evidence. As a result, the review may generate some evidence as well.

4.2.2 Supervision

In case of a principal delegating a general obligation he should still be held accountable for his delegation, not only with respect to any existing obligation instances that may have consequently been delegated, but also any possible future obligation instances that may arise for a principal on the basis of this delegation. We propose to capture this accountability for a delegated general obligation explicitly in the form of a supervision control.

We define supervision as the general obligation of a principal occupying a position to review the obligations of principals in supervised positions. This supervision relationship is the result of some prior delegation of general obligations.

The supervision relation between positions has little meaning by itself, unless there are some supporting review obligations. We illustrate this in the following example where we consider a company in which a principal Jon processes outgoing shipments. The company grows and with it the amount of shipments. Soon, Jon is not able to handle this task anymore. Two new employees Clara and Bill are hired. Jon now delegates his obligation to process shipments to these two new employees. More precisely, positions are created to handle the growth of the organisation, and Jon in his new position as a Senior Shipment Manager delegates the general obligation to process shipments to the position Junior Shipment Manager occupied by the two new employees. With the continuing expansion of the company there will be further delegations and refinements of such obligations. The Senior Shipment Manager position supervises the Junior Shipment Manager position. This means that through his position, Jon has an obligation to review that Bill and Clara process shipments correctly. In this case Jon might have to review the dispatch of a shipment 48 hours after the initial order.

5. Modelling and analysing the credit application process

Having described the suggested control principle framework, we have used the established concepts to model and analyse the controls involved in the context of the credit application process described in section 3. We believe that the 'business process' is the underlying concept needed for any kind of successful policy-based systems or security management. We identified this as one main component of organisational structure. Once such a process and the involved principals and objects have been identified and analysed in a given organisational context, obligations can be derived from it. In our context this process

has been abstracted and described in terms of figure 1. Here each step in the process corresponds to an obligation. Once the obligations have been defined, we then derive the authorisations required to fulfill these obligations. Specifically with respect to our framework and the distinction between general and specific obligations, we can say that the identification of the underlying business process is the basis for creating the general obligations of a principal, while the actual running of the process creates the specific obligations instances.

There is no space in this paper to further document the analysis of the credit application process in this context and we refer to [6] for a detailed description of:

- The formal and methodical modelling of the involved roles, positions, policy objects and principals;
- The formal modelling of the credit application process;
- The formal modelling of delegating obligations in this process;
- The static and dynamic analysis and exploration of the identified separation, review and supervision controls.

We can summarise our findings of this analysis as follows:

- We identified and analysed a set of separation controls;
- We were able to validate the novel concepts of general and specific obligations in identified obligations such as obl_`evaluate_credit` or `obl_approve_credit`;
- We further clarified the notion of delegating these types of obligations by identifying where such delegation activities take place in the credit application process;
- We validated the novel concepts of review and supervision to control such delegation activities in the credit application process.

6. Related work

Our concept of authorisation and obligation policy objects has been adopted from the discussions in the area of policy-based systems management. In particular the Ponder language has influenced our work [12], but we point out that Ponder does not support the delegation of obligations as we discussed it. Clearly roles as a component of organisational structure have also influenced our design decisions, in particular the RBAC96 model [13]. Recently a renewed interest in the delegation of authority within this model could be observed, e.g. [14], [15], and we again point to [6] for an extended critical discussion. There we specifically distinguish between "ad-hoc" delegation between principals in non-administrative roles and delegation based on the ARBAC approach [16].

7. Conclusion

In this paper we have presented a case study about the control principles involved at the branch level of a bank. In particular, it validated the concept of specific and general obligations. These allow for the explanation of review and supervision as controls on the delegation of specific and general obligations. This now closes our investigations into organisational control principles which have been documented by us in [1, 3, 4, 6, 17, 18]. Although the entire framework has been formally defined and analysed using the Alloy specification language and its analysis tools [2], this paper did include any such formalisms.

8. References

1. Schaad, A. and J. Moffett. *A Framework for Organisational Control Principles*. in *18th Annual Computer Security Applications Conference*. 2002. Las Vegas, Nevada, USA.
2. Jackson, D. *A Micromodularity Mechanism*. in *8th Joint Software Engineering Conference*. 2001. Vienna, Austria.
3. Schaad, A. and J. Moffett. *Delegation of Obligations*. in *3rd International Workshop on Policies for Distributed Systems and Networks (POLICY 2002)*. 2002. Monterey
4. Schaad, A., J. Moffett, and J. Jacob. *The access control system of a European bank - a case study.* in *6th ACM Symposium on Access Control (SACMAT)*. 2001. Chantilly, VA, USA.
5. Kern, A., A. Schaad, and J. Moffett. *An Administration Concept for the Enterprise Role-Based Access Control Model*. in *8th ACM Symposium on Access Control Models and Technologies (SACMAT)*. 2003.
6. Schaad, A., *A Framework for Organisational Control Principles*, in *Department of Computer Science*. 2003, University of York.
7. Bacon, J. and K. Moody, *Toward Open, Secure, Widely Distributed Services.* Communications of the ACM, 2002. 45(6): p. 59-64.
8. Minsky, N. and V. Ungureanu, *Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems.* ACM Transactions on Software Engineering, 2000. 9(3).
9. Kuhn, R. *Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems*. in *ACM workshop on Role-based access control*. 1997.
10. Gligor, V., S. Gavrila, and D. Ferraiolo. *On the Formal Definition of Separation-of-Duty Policies and their Composition.* in *IEEE Symposium on Security and Privacy*. 1998. Oakland, CA.
11. Urwick, L., *Notes on the Theory of Organization*. 1952: American Management Association.
12. Damianou, N., et al. *The Ponder Policy Specification Language*. in *Policies for Distributed Systems and Networks*. 2001. Bristol: Springer LNCS
13. Sandhu, R., et al., *Role-based access control models.* IEEE Computer, 1996. 29(2): p. 38-47.
14. Zhang, L., G. Ahn, and C. B. *A Rule-based Framework for Role-Based Delegation*. in *6th ACM Symposium on Access Control Models and Technologies*. 2001. Chantilly, VA, USA.
15. Crampton, J. and G. Loizou. *Administrative Scope and Role Hierarchy Operations*. in *7th ACM Symposium on Access Control (SACMAT)*. 2002. Naval Postgraduate School, Monterey, CA, USA.
16. Sandhu, R., V. Bhamidipati, and Q. Munawer, *The ARBAC97 model for role-based administration of roles.* ACM TISSEC, 1999. **2**(1): p. 105 - 135.
17. Schaad, A. and J. Moffett. *A Lightweight Approach to Specification and Analysis of Role-based Access Control Extensions*. in *7th ACM Symposium on Access Control (SACMAT)*. 2002. Monterey, CA.
18. Schaad, A. Conflict Detection in a Role-based Delegation Model. in 17th Annual Computer Security Applications Conference. 2001. New Orleans.