e-Informatica Software Engineering Journal, Volume 6, Issue 1, 2012, pages: 27–37, DOI 10.5277/e-Inf120102

Supporting Applications Development and Operation Using IT Security and Audit Measures

Katalin Szenes*

*Faculty John von Neumann, University Obuda

szenes.katalin@nik.uni-obuda.hu

Abstract

The market success of the enterprises depends on the ability to support their business processes. This involves the requirement of a seamless, well-ordered operation of the whole company. Operation is greatly affected by the quality of its IT support.

The information should be available, handled confidentially, preserving its integrity, have to be processed in a reliable, efficient, effective way, in compliance with the requirements of supervisory authorities.

Extending the scope of these information criteria to criteria determining operations quality and adding two business-level requirements to them makes possible to find preventive, detective and corrective, originally information security control measures, raised to the level of operational quality, that support the market success of the institutions.

1. A Method Based on IT Security and Audit for Supporting Corporate Governance

The goal is to facilitate the use of the originally information security and information systems audit ideas and tools in the area of corporate governance. In the followings the criteria characterizing such a corporate IT functioning, that is able to contribute to the compliance to a widely accepted set of requirements, are extended to the area of corporate operations. To operations belong every area, that supports business. Corporate finance, controlling, human resource management, and the like all belong here. Without them no business could operate.

In order to improve IT processes ISACA (Information Systems Audit and Control Association) was probably the first organization, that collected all these criteria. If we extend the scope of the measures by which some of these criteria can be fulfilled, to other business-supporting areas, then these criteria can also be raised to the level op corporate operations. This possibility of discussing the problems in a greater arena then before, will be illustrated here on a special application, on the service-oriented architectures.

2. Business Goals and Information Security

Seamless operation is one of the basic factors of the corporate market success. Improvement of operational quality, and compliance to the requirements coming from government and other authorities are vital. IT applications are non-separably interwoven into the everyday and even into the strategic level activities of every company. Thus to the fulfillment of the strategic business goals, computer applications have to support the – often contradictory – aspects of operation and compliance.

An efficient IT of a professionally operating firm follows best practice methods. Good examples are the methodologies of such prominent organizations as ISACA, or the ISO standards. ISACA and ISO both require the availability, confidentiality and integrity of corporate data. In its methodology ISACA appends to these the requirements of effective, efficient, reliable processing, and compliance to the authorities' prescriptions [1].

To this set two business-level requirements are to be added, according to my experience. One is appropriate functionality of every IT system, meaning, that the business-, or any kind of end-users are asked to confirm, that the systems help them reaching their strategic and business goals. The other is keeping order in every aspect of the company life.

The functionality requirement, that means actually involving the end-users into the development process, can directly be translated to a lower level goal to be set to IT: the deliveries of every milestone of the systems development lifecycle should be approved by the responsible organizational unit.

One of the necessary conditions of maintaining order in a company is to do so in every department. Doing so, involves specifically, among other requirements, up-to-date documentation, and configuration & change management of the whole IT architecture. An important factor of order is, of course, planning the other supporting, and what is more important, the business activities, too, before acting [2].

If we extend to operations our seven criteria originally set by ISACA as a best practice for IT, and add to them IT systems functionality, and order in every corporate activity, then we get a list of conditions usable in the improvement of operational quality.

Applying these conditions to different targets taken from the company life we get a generalization of the notion of IT "control objective". Information systems auditors and security professionals refer to best practice management objectives set to IT activities as "control objectives". Let us call these as "IT control objectives", and extend this notion to such best practice management objectives, that the operational areas have to achieve. This way we get the "operational control objective" and we will call this as "control objective" in the followings. (This will not arise disturbance, as IT control objective is a special case of operational control objective.)

To reflect the intentions of the top management in devising (operational) control objectives this term was extended to mean any kind of goals that can be derived from the corporate strategy [2]. Actually the scope of the original control objective is extended from IT to the broader arena of corporate operations.

Using this terminology, the above considerations mean, in other words, that lower level operational control objectives help the company to achieve one of its most important, high level control objective: raising the level of company operation so that it supports corporate success as well as possible.

The weights of these often contradictory, even if perhaps not completely independent requirements are always to be balanced, of course, according to the requirements of the given situations. The actual weights to be assigned have to depend on the business requirements. To find an optimal balance, that suits to the business goals the best way, risk management methodologies can be used [3].

Methods taken from the knowledge base of information security and audit, will be shown here to be able to help a lot in satisfying these control objectives, in order to illustrate how information security and audit are able to serve directly corporate strategy through the improvement of the quality of operation. It should be noted, that for managing risks the same or similar information security & audit ideas and tools could be exploited, as the ones presented here [3].

Having chosen our control objectives, the next step is to find measures, so-called "control measures", that can help reaching them. If the control measures are categorized, then to find the appropriate one will be easier. As the goal is operational excellence, the proposed categories are based on the three basic pillars of corporate operations [2]:

- organization,
- regulational system,
- technics.

The control measures will be presented here together with the control objective they help achieving, or the problem they help solving. We must not forget, that all these control objectives – at least in a balanced way – are necessary to supporting the business, but they are not enough. Without them the business users will not have a clear and exact picture on the present state of their tasks, but reaching these control objectives is not enough, will not totally transform the company. The other value of information security and audit ideas will be just the control measures. All of them, by themselves, will help the company towards a better organized way of living. However, it should be noted, that the complex process of identifying those strategic goals that help best the company to market success can not be spared. There are systems analysis methods for this purpose, that we have no room to discuss here.

To illustrate how these measures support the business goals, such a practical example was chosen, as an extension of former information security considerations [4], that belongs to an emerging area of application development: the service oriented architecture, SOA.

3. Implementation of Business Intelligence Using Service Oriented Architectures

This already for years fashionable architecture can be considered as a set of business processes performing business functions. The processes are implemented by so-called services, programs usually written in Java. These processes are "loosely coupled" to each other. This relation means either direct communication or a kind of orchestration – cooperation, that provides for the scheduling of process execution. For implementing this loose coupling different, complex ready-made products are available.

The processes are known to each other or to the outer world only through their communications so newly built and old, legacy applications can be packed together into this architecture and then the individual applications will be reached through this common platform.

According to ISACA researchers choosing this type of architecture positively affects the return of IT portfolio because of its promising cost / efficiency of solution delivery [5]. The SOA system is stated to reduce systems complexity, implementation and maintenance costs, and to enhance test effectivity at the same time.

This architecture is not an off-the-self product, but rather an approach to problem solving that supports a new way of thinking which is very useful in building such complex structures as e.g. enterprise portals that collect information from various background information sources.

SOA is on the way to contribute to the alignment of IT to the business processes by the means of a transparent and integrated application, service and process landscape. The technical processes can directly be derived from the business process models by the means of an integrated enterprise-wide meta repository of the available components. This is a repository of such services from which a complete IT projection of a business model can be built.

On the level of the reference model, however, SOA is a collection of distributed capabilities, that are created by people or by organizations and are needed by somebody to solve a problem. SOA is said to be "a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains" [6].

The idea originated in the middle nineties with the ambitious goal to share the business logic of an enterprise between its different computer applications and to facilitate a kind of multi-threaded execution of these applications, even if some of them operate on the same database.

The step that surely leads beyond the limits of the enterprise architecture integration is the spreading of the applications systems components all over the internet. The 21th century SOA consists also of loosely coupled, in a way individual parts, but these parts are now so-called web services, such services, that can be made available, or, in other words, can be invoked, either from the corporate intranet or from the internet and they use these two media for communication.

Not only the system components can reside on different nodes of the world wide web, but the users of the system, too. Nowadays when employees have to access the corporate applications practically from anywhere, the availability of an application system from the outskirts of the company is a very important point. Thus the service orientation turned into web service orientation both from the viewpoint of its build and that of its way of using.

4. SOA Main Features

The architecture of these new systems presents a unified surface to their user but their services might

– reside on different network nodes of the corporate network or even those of the internet,
– are diversified and run on different hardware, software – operating systems and database platforms,
– are developed by different vendors, using different methodologies.

To satisfy availability, confidentiality and integrity of the information, to process it effectively, efficiently, reliably, taking the requirements on compliance, order and functionality into consideration, is not at all trivial, with these complex applications, having parts spreading over the internet. To make matters even more difficult, when we pack new and old applications together as if they were individual services but called from a central entry point, this diversification of users and services, and the possibility of incorporation of the legacy systems into a brand new applications architecture at the same time, together with the loose coupling of so different components, by communication and scheduling, arouse new problems, preserving – due to the components – the traditional difficulties just as well.

These latter come from the legacy systems, that their users do not want to part with. These systems are independent islands in the enterprise information system. Their services are completely satisfactory to their users who are accustomed to them. Unfortunately, they frequently rely on obsolete databases, and are written in out-of date programming languages. Their documentation, if it ever existed, has been lost long ago. However, these drawbacks are the problem of the IT personnel while the end-users insist on preserving these systems. A solution is the wrapping of a legacy system in such a way as if it were a black box affecting the state of its environment only by its input / output. To find ways to implement this wrapping became a subject of interest already in the end of the last century [7].

Some experts consider the service oriented concept as a successor or an improvement of the idea of enterprise architecture integration. This integration wanted to provide for a common framework connecting every application of an enterprise [8]. This connection usually provides for a common entry point for the applications, too, so it can serve as a front-end system. One of the tasks of a front-end is to authenticate the users of the package of application systems behind it, then, according to their roles, the users are authorized. This authorization determines, how they will be able to use the systems of this package. As a next step, according to their authorized access rights the front-end offers the users the services of the systems. For the end-users this functionality looks like a menu system. This is the first thing they meet having authenticated themselves to the operating sytem of their computer.

The front-end systems of such heterogenous and giant corporate applications as the accounting systems of financial institutions are built quite frequently according to this structure. The users in the bank connect to the application portfolio – customer accounting systems, treasury, brokers' systems – through a menu system. At this menu the users have to be authenticated and then authorized to perform different functions – to invoke menu points – according to their work roles, that is defined by their job descriptions. Thus this is a point where confidential access of the employees to the set of applications behind the menu can be enforced. Besides confidentiality the fulfillment of other requirements can also be illustrated on front-end systems and service-oriented architectures.

The vulnerabilities and other issues concerning any architecture can be grouped in different ways. A possible classification of the SOA vulnerabilities can be, that to one group belong those, that are caused by the SOA architecture itself, for example by the difficulties involved in planning such a system, and the other group can be formed from those, that the operation of the SOA systems yields. The lack of considerate planning and / or that of the perfunctory implementation can undermine, of course, either the structure or the operation.

It will be marked here, which control objective, by what kind of control measure can be fulfilled, and to which – organizational, regulational, or technical – pillar does that control measure belong to. Our example will set mostly IT-related goals, but the measures will be on operational level, classified according to these three proposed pillars of operation.

5. Architectural Issues

A first step in finding the weak points of this architecture might be to explore, what is that mentioned loose coupling, that keeps its parts together. The parts are the so-called web services, that implement such activities, usually one service by one activity, that the business processes invoke. The business processes serve the business goals directly, the services perform usually one step that helps achieving the business goals. In order to make cooperation possible between these parts a kind of communication is necessary.

The services do not call each other in a subroutine-calling way. They communicate, using mostly XML, and the other connection between them is a kind of organization of their cooperation, the so-called orchestration of the web services, or rather the orchestration of their quite various functionalities. The orchestration and the communication together provides for the loose coupling, that makes a SOA from the components. The orchestration is to

- implement the business logic that connects the business processes to each other, and
- contribute to the building of such an application system from these various web services that is able to serve the current business goals set by the end-user.

Practically the execution of a SOA structure is based on an integrated handling of resources, together with such an administration of these resources that yields the satisfactory provisioning of the resources. This requires:

- choosing the appropriate web service, invoking it, and managing the passing of the control from one service or administration function to the other according to the needs of the user
- the management of the communication between users, system, auxiliary components.

To achieve the high-level goals of the orchestration described above different solutions are available. The so-called enterprise service bus (ESB) was one of the most popular among them. It collected references of the available services into a kind of registry from where they could be chosen in case of need [9]. These ESBs became collections of such business service capabilities that could be invoked.

Compliance of the Application System to Business' and Authorities'
Requirements. Served by:
Regulational Pillar Type Control Measure – Involves Administering Order

Authorities here mean those government and other institutions that have the authority to demand compliance to their requirements.

Such a compliance can only be based to have regulations on preliminary planning and on the continuous documentation of the satisfaction of both the users' and the compliance requirements at the different phases of development and throughout the whole life-cycle of the application. Planning before doing anything, and preparing documentation are both preventive control measures, they might parry quite a lot of problems.

Availability. Served by: Regulational Pillar Type Control Measures;
Change Management, Configuration Management

As it was already mentioned, documentation, change management and configuration management are vital information security measures both in developing and in operating any kind of applications [2, 10].

Changes of the application development projects, either shifting the goals, or adding/revoking resources, or any other event should be rigorously managed. This involves, among others, the documentation of the change requests, that of the permissions of the competent officers before the change is actually committed, etc. Otherwise sooner, than later the application becomes inconsistent with the information available about it. This results in chaos, in incompatibility of the running environment with the actual needs, in impossibility of administering any further corrections or impossibility of tuning the system to the business users' requirements, as nobody will know where is the point to be corrected, etc.

If we turn for advice to the COBIT methodology of ISACA, the description of the "Major Upgrades to Existing Systems" process of the domain Acquire and Implement says that if we carry out a major change to our application then we should "follow a similar development process as that used for the development of new systems" [1].

Without configuration management the current state and the whereabouts of the IT facilities will be unknown, and then the maintenance and other tasks to be executed can not be allocated. The instructions concerning documentation, change and, of course, release management should be part of the regulational system of every institution.

Availability of the Application.
Served by: Technical and Regulational Pillar Type Control Measures

The availability of the SOA architecture can be unpredictable when incompatibilities between the parts of the applications are realized too late. It can happen that the repositories used do not seem to be able to handle the services of other suppliers and then these services will be unreachable.

Even if the application doesn't always require the presence of every service at the same time, every service should be available. Some consider the asynchronous, publisher/subscriber way of communication to be a flexible possibility [11]. In this case the services are invoked in an event-driven way.

The ideas behind the SOA methodology and the building tools are changing, every day new issues arise. So many enthusiastic professionals began dealing with this new promising land that to track every direction would be hopeless. The variety of building blocks is very rich and these blocks are even developed according to different quality standards, if any are used at all.

In order to ensure the interoperability of these security solutions the Liberty Alliance [12] was founded by the suppliers. If a product complies with the requirement set of the generally accepted version of the Security Assertions Mark-up Language (SAML) then it is compatible with the products of other suppliers.

The other organization, where the security of communicating web services are widely discussed is XML Protocol Working Group of the W3C – World Wide Web Consortium [13].

Presently the service oriented architectures operate mostly in a client-server way so the services have to be present, too. For implementing the details of interaction a widely accepted standard should be chosen and then ordered to be followed. These are technical, and regulational control measures at the same time. Having them executed, we will have compliant products that are able to cooperate with each other.

6. Operational Issues

Here we follow an imaginary operation of a front-end system based on SOA technology. Looking for weaknesses in the execution of a front-end system, when we find one, then we look for appropriate control measures. Our palette of vulnerabilites to be cured will be here far from complete, of course, books could be written on this subject.

Preserving Confidentiality at the End/Abort of Service Execution

– Locating Point of Termination.
Served by: Technical Pillar Type Control Measure

One vulnerable point when these program systems begin operating is surely common. This is the flexible way of calling this set of services by a simple click that incurs all of the threats that usually endanger a remote connection. This connection can be invoked either from the more or less defended corporate network or remotely from the outside and the point of termination can be anywhere in the internet.

It would be desirable, if the requestor of the service could decide, when and how is the requested service to be terminated. Without predefined plans and painstaking programming this is not possible. Should anything go wrong otherwise, then, besides doing something unplanned, the service might go astray, carrying along some valuable business / personal data or logic.

Balancing Between Control Objectives: Availability Versus Confidentiality Balancing between the requirements is very important as the SOA applications usually support rich and complex functionality.

In this case, against unathorized outsiders the sensitive data could be encrypted but then availability might suffer as encryption / decryption will decrease performance. Business requirements are to decide, which opportunity is to be chosen.

First Confidentiality Issue in Operation – Provisioning for the Users' Access Rights. Served by: Organizational, Regulational, and Technical Pillar Type Control Measures

Some years ago the so-called middlewares began replacing the ESBs. These are able to extend the business support capability by a facility of access right management [14].

This means that here we can use an important organizational control measure: the tasks of the organizational units and those of the employees are to be clearly defined in the job descriptions in such a way that the duties are appropriately separated.

This organizational control measure should be written into a rulebook. Having put then this rule into effect we have built a regulational control measure.

If the access rights are assigned in such a way, that everybody is permitted to reach those and only those data that are necessary to perform their duties, then the application built on this middleware will support the confidentiality requirement.

Segregation or separation of duties is considered to be appropriate according to the best professional practice, if it satisfies at least the two most important basic requirements [1]. The first is, that there is no employee with too big power in modifying the corporate data, e.g. nobody has development and operation responsibility at the same time. The second is that there is no employee who has to supervise himself / herself. This way the business secrets and other, e.g. for privacy reasons sensitive data will have a chance to be confidentially handled.

Second Confidentiality Issue in Operation Identification and Then Complete Authentication of the User Who is Asking an Entry Permission.
Served by: Technical and Regulational Pillar Type Control Measures

When the application system is based on a SOA architecture then the user authentication process is even more important with all the internet connections involved. To one customer different companies might provide for web services that cooperate with each other and the user has to be known to every service.

As first step of the authentication, the user has to be identified by the means of a user identifier that is valid according to the records kept by the operating system. If this identity is accepted, then he/ she has to be authenticated in order to ascertain if this identifier really belongs to the user who has given it. After the successful authentication the user will be authorized to go forward, according to the settings belonging to this user identifier.

The threats entail the necessity of a really rigorous identification – authentication – authorization process that is advised to be extended towards federated identity management if more than one companies are involved in the provisioning of the web services comprising the SOA. Federated is the identity management if it supports a check throughout different companies by the means of strong authentication tools.

Federated identity management raises the level of the user authentication from that of the individual web services to a level of a synergy of these services. Serving the end-user these services have to communicate and have to pass the control to each other. The user has to be identified by all of the services that have anything to do in fulfilling his / her needs. Federated identity provides for a single sign on facility at the entry point of the SOA. This is the control point where the access rights of the user are to be set according to his / her role in the company. Having the user authenticated the services can communicate with each other on behalf of the user.

Federated identity management is described by OASIS [6], a non-profit organization, that develops standards and specifications to support e-business.

The strong user authentication requires more information pertaining to the user than a simple user password. Biometrical tools can be used to provide some personal characteristics. Tokens, smart cards, and the like devices, that are based on possessing something can also be used to enhance security.

These technical control measures, of course, have to be described by regulations. The processes of authentication and authorization are to be defined. The requirements of a successful authentication have to be clearly stated.

Third Confidentiality Issue in Operation: Authorization of the Authenticated User. Served by:
Technical, Regulational and Organizational Pillar Type Control Measures

After the successful authentication the computer system has to authorize the user according to his/her organizational roles in the corporate. Having clicked onto the entry point of the SOA the user encounters a menu. This again is a possibility to administer defensive measures. After the successful identification and authentication of the user, the access right management system should authorize him/ her exactly according to his/her role in the organization.

Some of the bases of authorization were already mentioned. Summarizing the most important ones:

- regulations concerning the enrolment, and
- termination of the employees,
- their job description
- the process of asking for and then
- confirming permissions
- the revocation of the permissions

The facilities of the system offered usually as menu points are to be just those options that he/she is permitted to use. The range can be properly set only if an exact job description is available which:

- is aligned to the organizational structure
- defines the tasks to be performed
- takes the segregation of duties principle into consideration.

The users should have access to

- those and only to those systems and within them
- to those systems functionalities and
- data, that are necessary in order to perform the duties given in their job description.

Devising organizational diagrams, defining the tasks of the organizational units and the employees, their job descriptions, in such a way, that their duties are properly segregated belong to the organizational type of the control measures. All of these are preconditions of a well-planned authorization process.

Fourth Confidentiality Issue in Operation: Defending Important Business Data. Served by: Technical, Organizational and Regulational Pillar Type Control Measures

The data of the information systems are resources, necessary to perform that functionality of the SOA system which satisfies the user's request.

To illegal program modification more internal knowledge and skills are needed then to attack data directly. According to its function the data can be:

- applications data – these relate to the business of the institution
- management data – needed to the administration of the information systems.

To the management data belong:

- the databases containing the user identification, authentication and authorization information – e.g. password tables, some of these might be embedded into different access control systems
- the data supporting the operations of the SOA and that of the IT infrastructure.

Examples for management data are: the data that are necessary to the scheduling of the web services or to operating the network devices or managing intrusion detection systems. Lots of other data set are vital to a well-functioning operations support. To the user databases belong those that are needed for the entry to the corporate network. This user information, unfortunately, can not be stored in one central collection but is usually spread all over the corporate network. These data describe, among others:

- PC users who are permitted to connect to the corporate network – this is usually an operating system table
- the users of the different applications – stored usually in the applications themselves
- the users of the different devices and facilities, etc.

The applications user groups are normally part of the group of PC users. Those firms that are strong enough financially to melt these groups into a single – sign – on user community have a chance to strive for a central user administration.

All of these data have to be defended against stealing. Defense involves hiding the users' identification and authentication data. We can not detail here, how to choose a safe solution, but we mention that one of them is encryption. Encrypted data can, of course, be decrypted, so such algorithms have to be chosen that cost / effectively defend the data.

In Windows-based networks Microsoft Active Directory is rather frequently used for storing the authentication informations of users' groups. To its advantages belong the more or less ready availability of the systems engineers who are Windows experts. Their cost is usually less than that of a skilled Linux / Unix professional where the openness of these operating systems requires considerable inside knowledge besides management & maintenance experience. This wider requirement set might make the company quite dependant on these employees.

One of the most important drawbacks of the Active Directory is the lack of a facility to maintain the history of the access rights of the users from the point of time they were employed till the termination of their employment. Active Directory shows always the present state only.

The risk of this lack of control can be mitigated sometimes on application level. Enterprise integrated system SAP is a positive example. It is able to track its users' access right history throughout their life in the company from entering till termination. Without such an application the organized and regulated tracking and archiving of the changes in the access rights might be a feasible solution. The respective tasks should, of course, be allocated, thus this is both regulational and organizational control measure.

As far as the access control on database level is concerned a considerable improvement of some of the database systems seems to be necessary in the near future. In some cases there are ready solutions available.

If there is no such control of every field of a record that the system could log the employee who modified something then the suppliers of these database system and the customers have to find other solutions. Confidential data can be locked from trivial access, e.g. the data can be put in a kind of vault. Some of the database systems facilitate fine-tuning of access rights according to the roles in the organizational units and to the sensitivity classes defined for the data [14].

There is a possibility to control field level access in such a way that the database administrators do not have full access rights full time but they get the access right necessary to complete their work from a security administrator just for the time interval when they need it. Field level access might improve the data processing performance of the applications and facilitates the fine tuning of access rights at the same time.

It must be noted, that the control measures defending the data should usually be supplemented by application level control procedures. These latter depend partly on the specific features of the given database system [15]. If these control measures are still not enough then come the organizational level control measures that usually define rules concerning the personal behaviour of the employees. These measures should be explicitly described in procedural rulebooks.

Fifth Confidentiality Issue in Operation:
Screening Users' Legal Activities;
Tracking the Unauthorized Access Attempts. Served by:
Technical, Organizational, and Regulational Pillar Type Control Measures

Should an auditor want to ascertain if the data are safe or not then he /she might want to compare the actual activities to the documented permissions. Another important question is: what do the users do with their legal permissions?

The logging of the users' activities and those of the data base administrators is not only a detective control measure but might help these employees to prove their innocence in case of security incidents. Of course, the logs provide for authentic proofs only if they can not be tampered with from that point of time when they were created. The solution is to sign digitally the log records, and to stamp them with the point of time of their creation, and doing so immediately at creation time. Digital signature means – roughly speaking – the creation of a so-called hash code. This code is composed from the bytes of the record to be preserved intact in its original form.

To log the activities the logging facility has to be set on – if the target system has such a facility at all. But all of these efforts are worthless if the log records are not managed, that is they are not archived, handled, etc., and if the collection of logs of different systems is not analysed, taking into consideration, of course, their relations to each other. All of the log records should be introduced into a central log management system. These are called as SIEM – Security Information and Event Management Systems.

Besides the users' information other equally important data are the log records of the various IT infrastructural elements. Infrastructural elements are the different hardware, operating system, databases, or even computer applications, the network devices, the defense systems and other special facilities such as those that participate in providing for the internet service: the proxy servers, the web servers and the like. Some of these devices are able to give signs about their current, or sometimes even about their future state in the form of log records. (Some of them can "complain" that it will go wrong within a short time.) The appropriate use of this information should be included in the maintenance regulations.

All of the duties enumerated above have to be assigned to somebody – this is an organizational measure, and the measures are to be described and regulated, these are regulational measures. Making all this possible by the means of handling the log records is a set of technical measures.

7. On Other Issues to be Handled

Here we can only call the attention to some also very important SOA issues that are also to be taken into consideration. All the problems can not even be listed here, that are known to the professional community, and to which different departments of the company have to answer by detective, corrective or preventive control measures. Here we restrict ourselves to giving only a sample in the followings.

Managing the resources needed by the services to perform their business function arises the question of availability again. These resources are mostly data in databases but to the resources belong, in a broader sense, all of those infrastructural elements that support somehow the operation of the web services. There is a lot of type of them, that all have their identifiable role in the SOA infrastructure, just as in the case of any other program system architecture. The infrastructural elements are subjected to the usual threats characterized by the nature of the given element, thus the elements one-by-one, and the whole system too, has to be defended, as a complex structure. This defense involves physical and logical measures alike. To the latter belong numerous maintenance tasks for improving the availability, integrity, confidentiality of the information and the resources.

Besides the supporting architecture, problems can arise from using SOA, too. The communication of its components with each other, and with the user, the cooperation of the parts by a kind of deadlock-free scheduling have to be managed [4, 16].

The communication protocols used for these communications can be attacked. The lack of planning, or omitting systems analysis phase yield vulnerabilities in the production systems. Unfortunately, this organizational and regulational defect of the support of corporate strategy is quite frequent.

8. Conclusions

Informatin security and audit methodology used for many years successfully for IT Governance is being extended to the support of corporate governance [2]. As an illustration of this research ways of at least partially solving some formerly discussed problems arisen by the complexity of service oriented architectures [4] were discussed above.

To prevent, detect or correct such problems operational level organizational, regulational and IT technical level measures were suggested. Information criteria belonging to the toolkit of information security and audit were extended to the level of evaluation of corporate operations.

References

[1] "Cobit 4.1 framework, management guidelines, maturity models," 2007.

[2] K. Szenes, "It grc versus? enterprise grc but: It grc is a basis of strategic governance," in *Euro-CACS 2010 – Conf. on Computer Audit, Control and Security.* Budapest, Hungary: ISACA, Rolling Meadows, Illinois, USA, March 2010.

[3] ——, "Building a corporate risk management methodology and practice," in *EuroCACS 2002 – Conf. for IS Audit, Control and Security.* Budapest, Hungary: ISACA, Rolling Meadows, Illinois, USA, March 2002.

[4] ——, "On the intelligent and secure scheduling of web services in service oriented architectures – soas," in *Procds. of the 7th International Symposium of Hungarian Researchers on Computational Intelligence*, Budapest, Hungary, November 2006, pp. 473–482.

[5] P. Williams, J. Spangenberg, and S. Kovaleva, "It and shareholder return: Creating value in the shareholder industry," *Information Systems Control Journal*, Vol. 4, pp. 39–42, 2007.

[6] "Oasis – organization for the advancement of structured information standards," http://www.oasis-open.org.

[7] M. Yoshioka, T. Sodo, A. Yoshikawa, and K. Sakata, "Legacy system integration technology for legacy application utilization from distributed object environment," *Hitachi Review*, Vol. 47, No. 6, pp. 284–290, 1998.

[8] S. Bennett, S. McRobb, and R. Farmer, "Object-oriented systems analysis and design using uml chapter 12 system architecture," 2006.

[9] C. Nelson, J. Miller, W. Farrell, R. Reinitz, and K. Brown, "Implementing a service – oriented architecture version 1.0," 8 2005.

[10] D. Melancon, "Security controls that work," *IS Control Journal*, Vol. 4, 2007.

[11] J. van Hoof, "Client server versus publish subscribe," http://soa-eda.blogspot.com/2010/09/clientserver-versus-publishsubscribe.html.

[12] "Liberty alliance," http://www.projectliberty.org.

[13] "W3c – world wide web consortium," http://www.w3.org.

[14] C. Everett, "Oracle spreads into the middle infosecurity today," pp. 34–36, July/August 2006.

[15] J. H. White, "Important but often dismissed: Internal control in a microsoft access database," *Information Systems Control Journal*, Vol. 6, pp. 30–34, 2006.

[16] D. Perelman-Hal, "Ajax and record locking," *Dr. Dobb's Journal*, pp. 45–51, October 2006.