INFORMATION SYSTEM QUALITY ASSURANCE IN FINANCES

Building the Quality Assurance into Information System Architecture

Dragutin Vukovic
INKUS Ltd., R. Boskovica 67, Velika Gorica, Croatia

Krešimir Fertalj
Faculty of Electrical Engineering and Computing, Unska 3, Zagreb, Croatia

Keywords: Quality, information system, governance, cell architecture, client, server, service.

Abstract: Key goals in assuring information system quality are continual improvement of IT performance, to deliver optimum business value and ensure regulatory compliance. Practices that support these goals are strategic alignment, asset and resource management, investment and portfolio management, risk management and sustained operational excellence. These are all about governance. While most organizations select a specific framework and apply it on the existing architecture, this may hinder them in taking a more holistic approach to IT governance. This paper discusses governance reference model and frameworks, and proposes a holistic approach in which prerequisites for quality assurance are built-in into information system architecture.

1 INTRODUCTION

Quality assurance means giving complete satisfaction - providing customers with what they want, when they want it, at a price they can afford. "Fitness for Purpose" is the phrase which best explains the concept and employs the principle of "Get it right, first time, every time" (Al-Hakim, 2007)

Quality assurance is essential to the success of business. To make a difference, good quality practice must be embraced by senior management and instilled within an organization's culture. Quality is not just about implementing a system or working towards a set standard. It is an attitude, a way of working, which not only improves businesses but the way people work and live.

Quality assurance is a companywide commitment to quality involving each employee from top management to the newest recruit, with the aim of making everyone aware of the importance of their own particular role and where it fits into the drive to improve total quality. It requires that "standards" are set for products and services and that a documented and workable system of management control is in place within the company to ensure that such product and service standards are met. It is a continuous process to ensure that quality of service is consistently maintained and in the most efficient and economic manner.

The demands on IT organizations, especially in finances, have never been higher. In addition to fulfilling their traditional responsibilities, IT organizations must now:

- Run IT like a business by forecasting and delivering results with accuracy and precision;
- Align IT spend with business priorities, rapidly adjusting as conditions change;
- Demonstrate measurable business value from technology investments;
- Take advantage of outsourcing, consolidation and other cost reduction vehicles;
- Communicate effectively with business partners and other stakeholders to create transparency, accountability and ownership;
- Operate in accordance with today's stringent corporate governance requirements.

Meeting these challenges requires a coordinated approach to IT Management and Governance.

Vukovic D. and Fertalj K. (2008).
INFORMATION SYSTEM QUALITY ASSURANCE IN FINANCES - Building the Quality Assurance into Information System Architecture.
In *Proceedings of the Third International Conference on Software and Data Technologies*, pages 355-360
DOI: 10.5220/0001892103550360

Enthusiastic to achieve their goals, many IT organizations launch projects to adopt and implement one or more management frameworks, such as ISO 20000 (ISO/IEC 20000-1:2005), ISO 9000 (ISO 9001:2000), or ISO 27001 (ISO/IEC 27001:2005). Although making their IT services more manageable, they generally fail in achieving such goals as required by business drivers and strategic objectives. Main reason for this failure lies in misconception of two terms: management and governance.

In plain words, we can say that management is decisions we make, and governance is the structure for making them.

Other organizations, with more sense in this distinction, will adopt further frameworks, known as governance frameworks, such as Control Objectives for Information and related Technology COBIT® (ITGI/ISACA COBIT, 2007) or Val IT™ (ITGI/ISACA ValIT, 2007). They will probably perform better but, from the business strategy point of view, results may be still unsatisfactory.

It is our belief that, with premature focus to specific framework, organizations can be deflected from taking a more holistic approach to IT governance, neglecting the changes in their information systems architecture needed to implement prerequisites for quality assurance into it.

In this paper we discuss the IT governance reference model, recognize its part which is likely to be implemented in information system architecture, and propose a concept of distributed computer system architecture tailored to support this implementation.

2 THE IT GOVERNANCE REFERENCE MODEL

A generally accepted definition of IT governance is to encourage desirable behaviour in the use of information and technology (Bloem et al, 2006). Behaviour constitutes both decision and action - not just making a decision, but taking action on it. IT governance consist of a set of formal and informal rules and practices determining how empowerment is exercised, how IT decisions are made and how IT decision makers are held accountable for serving the corporate interest.

Here we propose an abstract multilayered reference model of IT governance. Layers of the model are as follows.

Business Drivers. For any business, once in place, there will be a set of key factors which essentially 'drive' it forward. Different businesses have quite different drivers. Business drivers are external or internal influences that significantly impact and/or set direction for organization’s strategy. Identifying and prioritizing these are the critical first step in creating the strategy map, goals, measures and initiatives.

Internal Environment. Cultural and operating climate should be established to promote effective IT governance. Culture should exhibit leadership represented in value statements, mission statements and guiding principles. Value statements represent main philosophies and beliefs that influence organization's vision and mission. Guiding principles should encapsulate the role IT will play and how decisions will be driven, enacted by controls in the form of policies, standards and procedures.

Entrustment Framework. Ensures accountability for desired outcomes, as well as decision authorities (individuals, committees, boards) empowered to make and ratify decisions regarding the use of IT. The framework should also include organizational structures and functional interrelationships.

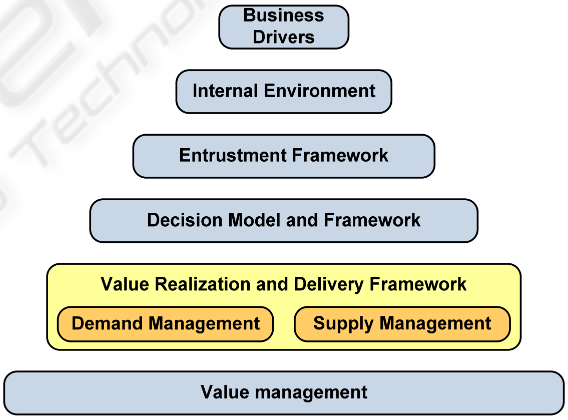

Figure 1: The IT Governance Reference Model.

Decision Model and Framework. Enables sound and informed decision making, ensuring that IT decisions are coherent and consistent with the corporate direction and aligned with the overall business strategy. The goal should be to make decisions based on a more manageable set of possibilities by eliminating choices that are in conflict or inconsistent with the guiding principles and policies. Decision factors might include cost-benefit analysis, risk identification, scope definition, financial impact, time to delivery, and efficiency and effectiveness of delivery.

Value Realization and Delivery Framework. This layer is generally viewed as having two parts, demand management and supply management. Demand management includes the activities involved with generating demand for the products and services offered by the organization. Supply management consists of the activities that are directly involved with provisioning and supplying the products and services offered by the organization.

Building on the idea proposed by the IT Governance Institute (ITGI) we will further split this layer into five areas, as shown in Figure 2: value creation, value delivery, risk management, resource management, and performance management.

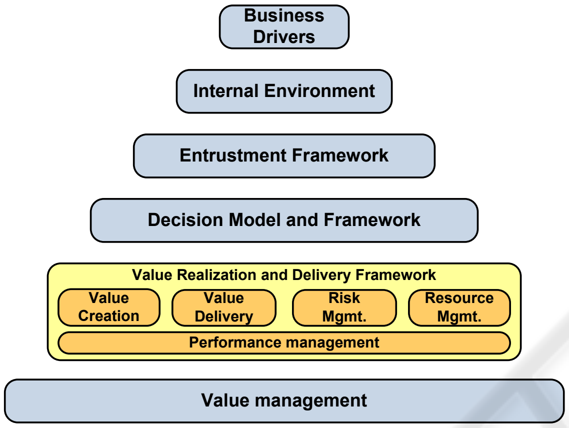

Figure 2: Decomposition of value realization and delivery framework layer.

Value Management. Main concern in this layer is the delivery of business value from IT investments, its objective being to ensure that organizations maximize value by optimizing the benefits of investments throughout their economic life cycle within defined risk tolerance thresholds. To objectively assess the relative business value of alternative IT investment planning decisions a "value framework" should be established. This can be achieved in various ways, e.g. by mapping business KPIs to IT KPIs and developing an appropriate set of balanced scorecards that link business and IT KPIs.

3 INFORMATION SYSTEM ARCHITECTURE QUALITY REQUIREMENTS

We will now take a closer look at the Value realization and delivery framework layer of the reference model.

Information system itself cannot produce value. Value creation is a process driven by people working with information system. In finances, value is deposited in data stored throughout information system. Stored data is the most valuable asset of any financial organisation. To ensure against deterioration of this asset value and quality, information system shall provide for integrity of data.

Value is delivered by means of information system, as a set of data relations retrieved upon the user query, and delivered to the user in consistent and timely manner. Information system shall provide for availability of data to authenticated and accredited user in his/her security context.

Information should not be presented to users not accredited and entitled to see it. Information system shall provide for data confidentiality, to mitigate risks of data misuse.

These three requirements comprise well known trinity of information security management, known as CIA; confidentiality, integrity, availability (Khadraoui and Herrmann 2007). But, having been inclined to governance, we shall also take into consideration resource and performance management, so as to achieve synergetic effect of optimal business results with suboptimal IT resources.

This will conclude the round-up of general requirements which we deem to be candidates for integration into information system. Below we will propose a concept of multilevel cell distributed computer system architecture which shall implement functions to satisfy these requirements.

4 MULTILEVEL CELL DISTRIBUTED SYSTEM ARCHITECTURE

Cell-based distributed system architecture is a development from the architecture based on communicating proxies. (Lerner et al, 2002) Cells are distributed computer systems built of computers not necessarily of the same functionality, with the possibility of having the whole cell functionality contained in the single computer. Cell has three general function groups: connection, traffic management and information system support.

In logical sense, cell functions can be divided vertically into three functional levels (network, system and business), and horizontally into four

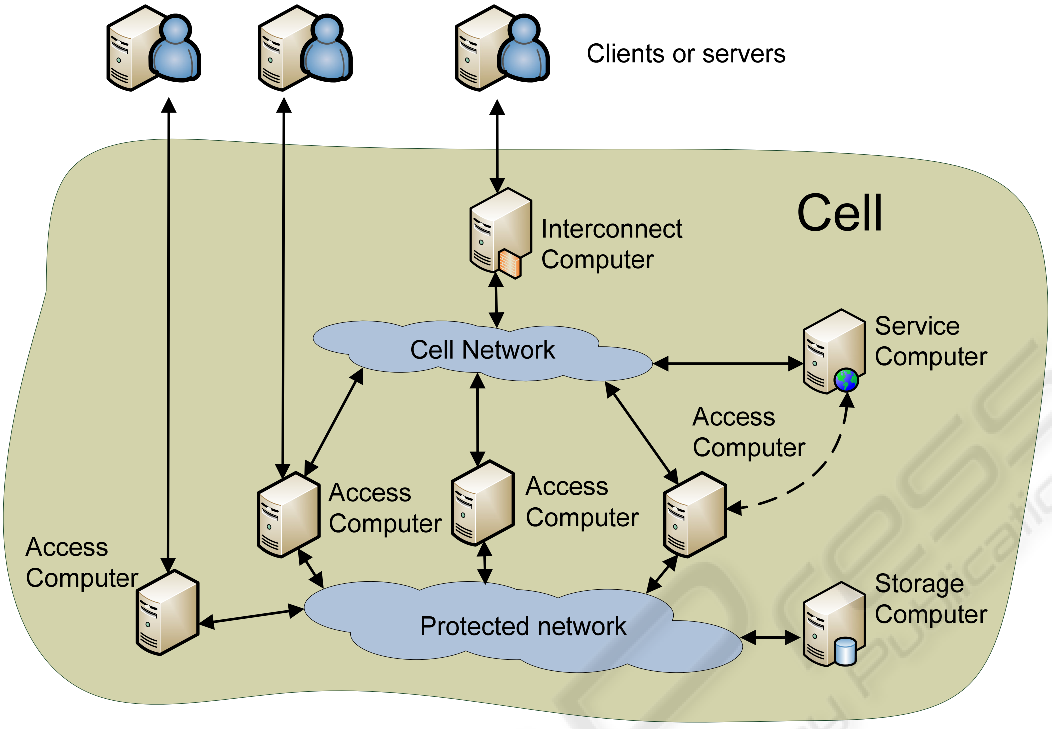

Figure 3: Cell's internal architecture.

functional elements (access, interconnection, storage and service).

Although all functions can be implemented in single computer, it is recommended to implement different functional elements into different computers. Having this in mind we will call these computers, similarly: access computer, interconnection computer, storage computer and service computer. These computers comprise building blocks of the cell's internal architecture, as depicted by Figure 3.

Internally, cell has two networks: cell network and protected network. Cell network is semipublic network into which external computers (clients, servers or other cells) can enter through interconnect computer or access computer, so as to gain access to service computer or access computer. Protected network is unreachable for external computers, and only access computers can connect into it, in order to access the cell's data contained there on the storage computers which are also attached to the protected network.

5 CELL ELEMENTS

Access Computers are, by their function, proxy computers with some extended functionality. They are characterized by having at least two network interfaces. One interface connects access computer into the protected network that enables them to communicate with each other. Other interfaces connect access computers with external computers (clients, servers or other cells) either directly or through the cell network and interconnection computer.

Storage Computers are essentially database servers. They provide services, related to databases stored on them, to other cell computers, but only through access computers. Therefore data stored in the cell are not directly reachable by the external computers.

Service Computers are, by their functions, general servers. They provide services to other computers, internal or external to the cell. Service computer can be connected to the cell network or directly to access computer.

Interconnecting Computers enable communication with other networks and provide security boundary for the cell. They also run several other security related tasks such as registration, identification, authentication, accreditation, encryption/decryption, etc.

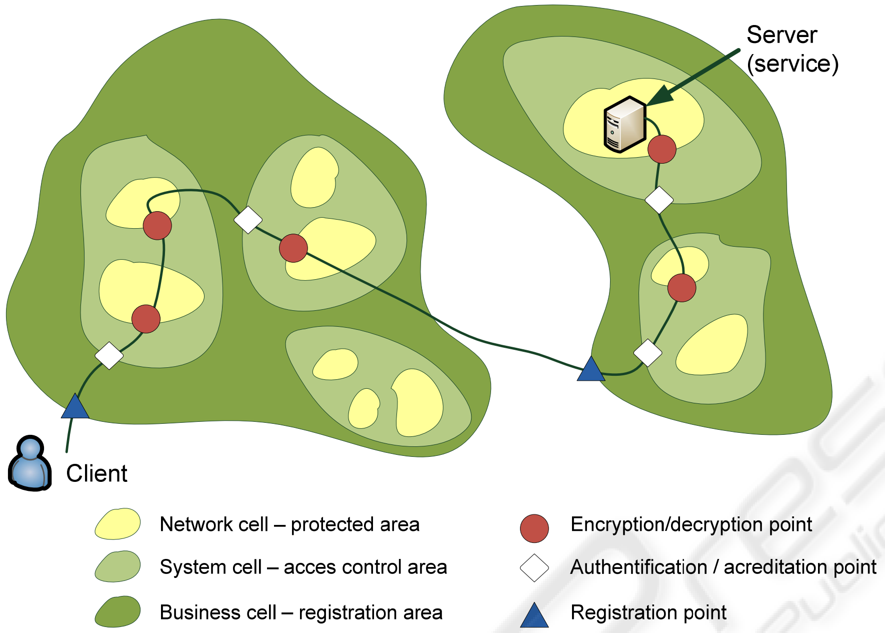
Server
(service)
Client
Network cell – protected area
System cell – acces control area
Business cell – registration area
Encryption/decryption point
Authentification / acreditation point
Registration point

Figure 4: User query traversing two business cells.

6 FUNCTIONAL LEVELS AND FUNCTIONAL ELEMENTS

Basic functional cell level is network. Cell in this level is called network cell. Network cell is based on locality of computers which constitute the cell. It is supposed that computers in the network cell all are contained in single building or several closely placed buildings, interconnected by private and physically secured network. Network cell centralizes functions such as traffic management, network management, quality of service management, messaging, etc.

Network cells are being connected together to form a system cell. If communication between network cells is not local and protected, there should be encryption/decryption function built into interconnecting computers. System cell centralizes functions of user identification, authentication and accreditation.

System cells are interconnected to make a business cell. Business cell centralizes the function of registration. To enter a business cell user has to register, and then his queries have to be checked for authenticity and access rights whenever they enter through system cell boundary.

Figure 4 shows an example of user query sent to the server located in another business cell. As shown, this query traverses several network, system and business cells. Figure depicts all encryption/decryption points as well as access rights control points and registration points.

Multilevel cell architecture based on different functional elements efficiently implements all three basic functions of distributed system: connection, network traffic management, and information system support.

To implement connection function efficiently, it should be founded on three general principles: knowledge abstraction, lazy calculation, and multiplication of data about clients and servers. All three principles are supported by cell architecture described here. Knowledge abstraction supposes construction of abstract model for unified representation of servers and clients in our computer system. In the first step, notion of *server* (physical entity providing a certain service) is replaced by more abstract term *service* (service itself) which cloaks physical characteristics of server computer. Thus, instead of *client/server* architecture, we are considering *client/service* architecture.

Lazy calculation of object characteristics supposes that neither all objects, nor all their attributes, are at every moment present locally in all cells of distributed architecture. Only when objects' characteristic is explicitly referenced the system will contact other cells to retrieve the needed information. This principle is supported by institution of global catalogue which collects all objects but only with some subset of attributes. Multiplication of data about clients and servers is achieved by partitioning and replicating objects into other cells. Replication topology and schedule should be designed carefully to optimize network traffic.

Cell architecture also supports efficient network traffic management, based on data replication as well as multiplication and distribution of functions.

Network cell manages and monitors traffic, sends massages to computers and group of computers, measures and allocates bandwidth, etc. System cell replicates system and server data, and distributes control and administrative jobs. Business cell redirects network traffic, based on information in registration databases, internally or towards other cells.

While majority of connection and traffic management functions are performed by network and system cells, fundamental business cell purpose is to provide support to information system By executing many of monitoring, security and administrative functions, business cell simplifies server and client operation and makes their connection efficient.

7 CONCLUSIONS

Key goals in assuring information system quality are continual improvement of IT performance, to deliver optimum business value and ensure regulatory compliance. Multilevel cell distributed computer architecture is capable of supporting these goals with functions built into information system as its integral part. It is not technology or platform dependent. It could be implemented in existing computing environment with minimal impact on physical configuration of systems, as a set of middleware.

Improvements in information system quality should be expected due to:

- Unified identity management;
- High security level;
- Implementation of “application as service” paradigm;
- Platform independence; and
- Efficient system management.

It is possible, and recommendable, to use of-the-shelf software products for implementation of certain functions.

ACKNOWLEDGEMENTS

"Publication of this paper was supported by grant # 036-0361983-3137 by the Croatian Ministry of science, education and sports."

REFERENCES

Al-Hakim, L., 2007, *Information Quality Management: Theory and Applications,* Idea Group Publishing, London

Bloem, J., Van Doorn, M., Mittal, P., 2006., *Making IT governance work in a Sarbanes-Oxley world*, John Wiley & Sons, Hoboken, New Jersey

Khadraoui, D., Herrmann, F., 2007, *Advances in Enterprise Information Technology Security*, Information Science Reference, New York

Lerner, M. Vanecek, G., Vidovic, N., Vrsalovic, D., 2002, *Middleware networks: Concept, Design and Deployment of Internet Infrastructure,* Kluwer Academic Publishers, New York

ITGI/ISACA COBIT, 2007,. - *Control Objectives for Information and Related Technologies, ITGI/ISACA (IT Governance Institute / Information Systems Audit and Control Association)*

ITGI/ISACA ValIT, 2007, - *Enterprise Value: Governance of IT Investments, The Val IT Framework, ITGI/ISACA (IT Governance Institute / Information Systems Audit and Control Association)*

ISO 9001:2000, *Quality management systems -- Requirements (ISO 9001:2000; EN ISO 9001:2000)*

ISO/IEC 27001:2005, *Information technology -- Security techniques -- Information security management systems -- Requirements (ISO/IEC 27001:2005)*

ISO/IEC 17799:2005, *Information technology -- Security techniques -- Code of practice for information security management (ISO/IEC 17799:2005)*

ISO/IEC 20000-1:2005, *Information technology -- Service management -- Part 1: Specification*

ISO/IEC 20000-2:2005, *Information technology -- Service management -- Part 2: Code of practice*

ISO/TR 13569:2005 - *Financial services -- Information security guidelines*