Improving the Benefits of IT Compliance Using Enterprise Management Information Systems

Renata Paola Dameri
University of Genova, Italy
dameri@economia.unige.it

Abstract: During the latest years, IT governance has become more and more important. More of the attention on IT Governance is captured by compliance, owing to the recent financial scandals and the severe rules regarding information systems audit and control. Companies need to comply with these rules, but it requires important investments, considered not only strategic but necessary (Remenyi et. al. 2000). However, companies should analyse the compliance requirements to implement an IT governance system, not only to comply with legal rules, but also to improve the strategic alignment between IT and business and to optimise value creation by IT compliance investments (Ventrakaman and Henderson 1996, Van Grembergen 2003).

However, companies have difficulties in implementing IT compliance initiatives, because they are complex and require an integrated approach all over the organization. But IT compliance initiatives often lack an integrated, strategic approach: they only try to comply with the increasing rules affecting IT operations, thereby limiting the value of compliance investments.

To optimise IT compliance, companies should develop an IT compliance strategy, aiming not only to accomplish with regulations, but also to bring processes into compliance. That is, to realise a full integration between operations, risk control, data reliability. To reach this result, compliance automated solutions are indicated, like GCR (Governance, Risk and Compliance) applications. However, standard solutions fail to support specific problems and the individual value proposition of each company: an EIMS (Enterprise Information Management Systems), developed in house, allows automatically managed processes, data and information security, to access control and system performance and to improve data usability, in accordance with company specific organisation and needs.

In this paper, IT compliance is introduced, to define how to orient it to value creation; GRC systems. EIM systems are described, with their different cost and benefits for companies. The aim of the paper is to define how to develop compliance automated systems, to save money and enhance information integration and value. Observations and conclusions derive from practical experience of the author, participating to a project of EIM implementation in a major Italian company.

Keywords: IT governance, risk management, accounting information systems, IT compliance, knowledge management

1. Implementing IT compliance

IT compliance is a required activity for public companies. Indeed, owing to important financial scandals occurred in the past few years, stock exchange authorities all over the world issued regulations to grant higher affordability to financial disclosure. The most known regulation about these topics is Sarbanes-Oxley Act (SOx), issued by USA in 2002 and pursuing a more strict internal audit on accounting and financial documents issued by public companies. All the most industrialised countries issued similar regulations, to regain the trust of investors in financial markets.

Regulations about financial disclosure and internal auditing also affects information systems, because nowadays all the accounting processes are highly computerised. It is impossible to audit accounting without auditing the accounting information systems; it is impossible to grant the affordability of financial disclosure without facing the risks deriving from the use of IT systems.

So, regulations about financial disclosure aim to grant affordability and correctness of financial data and documents issued by public companies; they require an intense activity of audit and control about all the accounting practices. Also information systems should be submitted to the same auditing, and specific controls on IT systems should be implemented to comply with regulations (ITGI 2004).

These duties are really heavy for companies, because all the accounting activity and all the IT systems regarding accounting should be strictly controlled and controls should also be documented, proved and periodically assessed. It requires a big effort to map all the accounting processes, define controls, apply them and report about their functioning. This effort is not efficient if it is focused only on compliance with regulations; it should be important that companies find synergies between IT compliance initiatives and IT strategic goals, to improve the return expected by the implementation of IT compliance framework (Damianides 2005).

Dameri, R. P. “Improving the Benefits of IT Compliance Using Enterprise Management Information Systems.” *The Electronic Journal Information Systems Evaluation* Volume 12 Issue 1 2009, pp. 27 - 38, available online at www.ejise.com

To accomplish with regulations, companies should define a complex framework, structuring all the controls necessary to realise the required audit about accounting information systems. These controls are of two types:

- IT general controls;
- IT applications controls.

IT general controls regard the functioning of the IT infrastructure; they should reduce the risk of systems failure, unauthorised access to programs and data, but also assure the systems integrity after operations such as acquisition, implementation, configuration and maintenance of operating systems, database management systems, middleware, communication software and utilities that run the system and allow financial applications to function.

IT applications controls aim to verify the correct functioning of financial applications, but also of ERP systems and of each other process software producing accounting entries. These controls assure completeness, accuracy, authorization and affordable disclosure for each financial information.

Obviously, all companies already have such controls, because they want to secure the correct functioning of their information systems and accounting systems, independently by the new regulations. But SOx and other laws about financial disclosure requires both a more stringent control and documentation, prove and assessing of their effectiveness; few companies already have such an IT control framework, that is, all the information systems auditing should be totally redesigned.

To reach the result of a well conceived IT compliance framework, companies should primarily define a roadmap, describing the processes and activities to exploit, to reach the desired result. This roadmap includes the following steps (Fig. 1).

1. *To define the scope of IT compliance*. Regulations about the reliability of financial disclosure involve information systems only regarding accounting entries. The scope perimeter includes therefore only applications producing or processing financial data. However, enterprise systems create integrated databases and sets of applications, so that almost all the IT applications are included in the scope of IT compliance. It means that the scope of IT compliance is very large and controls should be wide-ranging respect to the information system.
2. *To map and document in-scope IT components*. After defining the IT compliance perimeter, companies should map all the operations composing the processes and document them, outlining the processing regarding each financial data. This map of the accounting information system could be already available in the company, or it could be a good occasion to produce it.
3. *To design the controls*. Companies should then assess the existing risks and threats for data integrity and design a specific control to prevent each of them. Controls are developed and integrated into the accounting applications or in the security systems. All applied controls should be clearly documented, both to demonstrate their existence and to permit their evaluation and monitoring.
4. *To evaluate controls*. Companies should evaluate the good functioning of each control and the solidity of the whole IT compliance framework. It needs to notice the application of controls and to detect malfunctioning of IT systems and accounting applications; it is also necessary to evaluate if controls are able to remediate to systems failure, unauthorised accesses or human mistakes in accounting. It requires to define an evaluation system, but also a responsibility and accountability schema, to attribute the malfunctioning to the manager responsible for it.
5. *To report about the IT compliance activity*. All the IT compliance activities should be reported and documented and results should be clear and available both inside and outside the company. It requires the complete traceability of each computerised operation regarding accounting and financial disclosure.

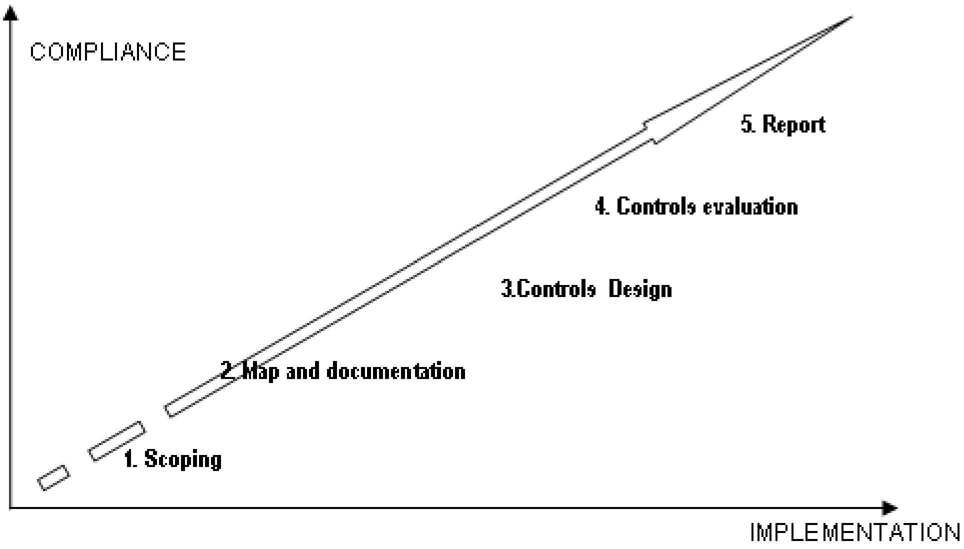

Figure 1: The IT compliance roadmap

2. The standard for IT compliance: they are not the answer

The IT compliance activity is really complex, especially for large companies, with subsidiaries in different countries and listed in different stock exchanges. To support IT compliance, standards are available, to drive companies in doing the right things saving money. These standards are COSO and COBIT.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a USA private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

COSO framework is designed for internal auditing, but it well supports also IS auditing and drives towards the accomplishment of regulations. Indeed, also for IS auditing it is necessary:

- to asses risks regarding both IT infrastructure and applications, to understand the range of the required IT compliance effort;
- to design not only controls, but a control environment that governs IS security and compliance in an integrated way;
- to define controls and control processes, well explaining the duties to follow and the goals to reach;
- to inform company's people about the compliance activities and to communicate efforts, activities and reached results to external stakeholders and financial markets;
- to monitor the effectiveness of IT controls and to use information about it to review the risk assessment and to continually improve the IT compliance framework.

The Control Objectives for Information and related Technology (COBIT) is a set of best practices for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company. The COBIT framework aims to supply an integrated set of instruments to manage all the stages of the life cycle of information systems: plan and organize, acquire and implement, deliver and support, monitor and evaluate.

Applying COBIT, a company could realize a well conceived and integrated control system, able to manage all the processes regarding IT. It is easy to include IT compliance in a COBIT framework, because:

- processes are mapped and documented;
- policies and activities regarding IT and applications are defined and formalised;

- responsibilities and duties are assigned and accountability is assured;
- a detailed monitoring and evaluation framework is applied.

To implement both COSO and COBIT, it is necessary to put together the two frameworks and to link them with the regulations requirements, for example SOx requirements, as in Fig. 2. It means that to realize a secure IT compliance framework:

- regulations requirements define the scope of the compliance;
- COSO components describe how to do;
- COBIT controls define what to do, that is, the IT management processes interested by the compliance activities.

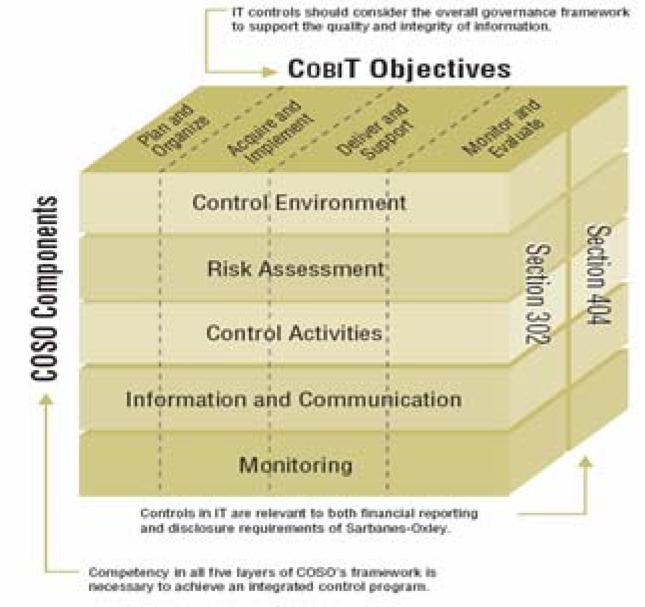
IT controls should consider the overall governance framework to support the quality and integrity of information.
CobiT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Section 302
Section 404
Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.
Competency in all five layers of COSO's framework is necessary to achieve an integrated control program.

Figure 2: SOx, COSO, COBIT: an integrated framework

Despite the effectiveness of COSO and COBIT, it is not easy to implement them. Companies trying to realize an IT compliance framework designed reflecting COSO and COBIT found it very expensive and hard to do.
COBIT is a very complete instrument to obtain a strictly managed and controlled IT environment, but it means:

- to reengineer all the processes of the IT life cycle;
- to formalize all the activities related with IT, submitting them to the strict control of a fixed procedure;
- to standardize each operation on IT, adapting it to the COBIT practices.

The result is:

- on one side, a well formalised, standardized and evaluated IT management system;
- on the other side, a rigid, unspecific and muddled framework, forcing IT people and managers to uncritically execute the established procedures, without opportunity to adapt them to changes or specific situations.

It is therefore important to understand if it is really necessary to implement COSO and COBIT, or if it is possible to use these frameworks to analyse the specific needs and characteristics of a company, and to define a tailored IT compliance environment, able to better fit the business information systems and the unique IT strategic goals of each enterprise.

3. How much does IT compliance cost?

One of the more important consequences of IT compliance duties is the cost of an IT compliance framework.

To implement an IT compliance system is indeed very expensive, because this framework does not impact on a sole application, but it regards a very large portion of the information system. The use of ERP and integrated management information systems, pervasive respect to all the organization, enlarges the scope of

IT compliance and forces to include in the compliance perimeter almost all the IT infrastructure and the applications portfolio.

Moreover, IT compliance cost is not a “one time cost”, but a “in progress cost”. Indeed, regulations requires to asses the IT risks impacting on financial disclosure in every time of the life of a company and to maintain the effectiveness of the control environment when information systems are changed, updated, expanded. It means that IT compliance is a continuous process and that its cost could be like a permanent fee detracting financial resources from the IT budget, that is from strategic, innovative IT investments.

Some researches are already available, to better understand which cost are generated by IT compliance, their amount and how to reduce them.

A survey realised by Financial Executive International in 2007 revealed that extra cost for IT compliance for companies listed at the NYSE are average 4,36 M US $ in the first year of implementation, about 39% higher respect to the companies expectation. The main cost driver is the audit activity, which requires a very high effort. Indeed, companies often have not enough competences to face this task by themselves and therefore they resort to consulting companies, even if their fees are very expensive.

Gartner in 2006 analysed the composition of IT compliance cost and stated that the main item is just the consulting cost, followed by cost for software acquisition or development and cost for staff training. The total amount of expenses for IT compliance is estimated about 1% of revenues and the cost of maintaining the IT compliance environment will amount at 7000 US $ a year per employee.

It means that:

- companies should invest very large amounts in IT compliance;
- if IT compliance initiative are developed only to accomplish duties, no return are expected from these investments, except to avoid sanctions deriving from laws and regulations;
- the IT compliance cost will be a continuous flow of unproductive IT investments during the time;
- IT compliance investments reduce the innovative IT investments or require to increase the IT budgets.

To face this, companies should see at IT initiatives not like a duty to accomplish, but like an opportunity to exploit, to improve their awareness of accounting information systems, to reduce IT risks, to enhance the value of financial information and to gain the trust of investors and financial markets. That is, companies should transform IT compliance from a cost driver to a value driver, aligning IT compliance initiative to their own IT strategic goals and investments.

In the meantime, companies should try to reduce IT compliance cost and expenses, both for the first implementation and for the maintenance of the framework. To reduce the first implementation cost, companies could regard at best practices, rationalise their processes and application portfolio, standardize accounting system, obtaining scale economies. To reduce maintenance cost, companies could learn from past business cases and create experience economies, but also computerise the IT compliance activities, both acquiring an on-the-shelf IT compliance software or developing it in house. Both the solutions, as we will see, have their pro and con (Fig. 3).

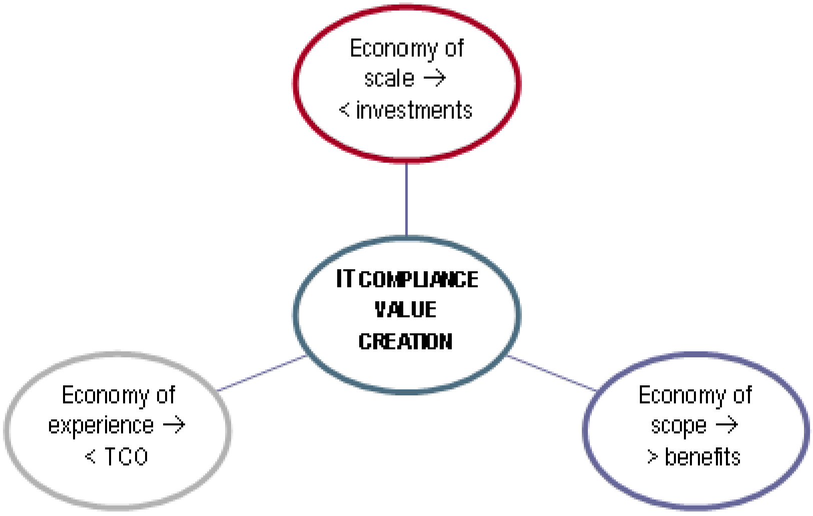
Economy of scale → < investments
IT COMPLIANCE VALUE CREATION
Economy of experience → < TCO
Economy of scope → > benefits

Figure 3: IT compliance and value creation

4. How to create value by IT compliance

If a company wants to create value by IT compliance, it should pursue three goals at the meantime:

- to monitor and reduce cost of IT compliance implementation;
- to improve the scope and benefits of IT compliance initiatives;
- to computerise the IT compliance process along time and space.

4.1 To monitor and reduce the cost of IT compliance

Even if IT compliance is very expensive, it is possible to reduce its cost by applying some standards and techniques improving the efficiency and effectiveness of compliance processes.
Four key words define the cost reduction guideline:

- standardization;
- reuse;
- analysis;
- risk monitoring

The most important word is standardization: indeed, business processes standardization is very helpful to implement a good IT compliance framework, saving money in the meantime. However, standardization here doesn't mean merely to redefine all business processes pursuing a rigid and theoretical model; but it implies to analyse and to define all business processes and IT applications using a unique language. It seems very simple and granted, but it is not. Several companies have heterogeneous information systems, developed for several years or decades and never harmonized. In this case, each process, each software, each data flow, each operation should be controlled by itself, without the possibility to apply formalized and standard controls. Also the map of the information systems could be very difficult to delineate. In this scenario, to apply IT compliance controls costs really a lot of money! On the contrary, to apply controls to standard, harmonized and well designed processes, software and data flows is easier and cheaper.

Before to apply IT controls for compliance, is therefore better to standardize the conceptual models and representation languages to define IT operations because in this way the IT compliance activity could be formalised and executed faster and cheaper.

The second key word is reuse; if IT processes are standardized and IT compliance policies and activities well conceived and formalised, it is possible to implement them a first time in a case study and then to reuse them all over the company. This behaviour creates scale economies which contributes to reduce to cost of compliance. Indeed it optimises:

- the cost of processes analysis and mapping;
- the cost of software development;
- the cost of controls implementation and of staff training;

- the effectiveness and quickness of audit activities.

The third key word is analysis. It means that the first steps in defining the IT compliance framework are the most important, because it is crucial to design a well conceived compliance environment from the beginning. Indeed, a bad arranged IT compliance framework requires continuous maintenance and improvement, increasing the cost of its implementation. Moreover, it is very difficult to generate reuse and scale economy, if the first applications of the framework fail. A good and deep analysis of all the accounting information system and an exhaustive documentation about accounting processes and data flows are the better basis on which to built an effective IT compliance framework.

Last but not least, the fourth key word is risk monitoring: implementing IT compliance framework is useful to a better awareness and monitoring of all IT risks, not only the ones impacting on financial reporting. Processes mapping and documentation are valid instruments to support an effective risk management; synergies deriving from unifying IT compliance and IT risk management could contribute to reduce cost.

4.2 To improve the scope and benefits of IT compliance initiatives

To create value it is possible to increase the benefits deriving from the IT compliance investments. Indeed, IT compliance activities may have a larger scope, not narrowed by regulations and duties, but included in the IT vision of the company and oriented to value creation.

To pursue this goal, it is necessary to include IT compliance in IT governance; in this way, the same management practices applied to all the IT initiatives are applied also to compliance initiatives and harmonized into the company's IT initiatives portfolio.

To include IT compliance in IT governance means to follow a well defined behaviour to optimise the realisation of value from IT investments. This behaviour is summarized in the following principles.

- *Define policies*. To gain maximum value from IT compliance investments it is necessary not to uncritically apply regulations and standards, but to define a general policy driving the whole compliance processes, both at present and in the future. It permits to better focus the IT compliance initiatives on the strictly necessary measures to implement and to harmonize the IT compliance choices with the IT strategic vision of the company.
- *Assign responsibility*. One of the main principles of IT governance is to assign responsibility about decision making and reached results. Also for IT compliance it is important to assign power and responsibility in a very clear manner and respecting the segregations of duties. It permits to gain better results, because each manager is well aware of its own charges.
- *Apply accountability*. To verify reached results it is necessary to define an evaluation framework, to be applied to IT compliance initiatives. The more useful could be a Maturity Model, to understand the status of IT compliance framework and of its implementation. Maturity Model supports the identification of best practices and necessary improvements, from a disorganized process to an automated IT compliance activity. Moreover, the evaluation framework could include also performance goals and metrics, demonstrating how IT compliance processes meet business and IT goals. Accountability is the weapon to built a measurement-driven IT compliance activity, aiming not only to comply with regulations, but also to do that creating value.
- *Pursue the higher value from each IT investment, also in compliance*. IT value is the result if three dimensions: systems capability and coverage, control about risk and compliance, alignment with business mission and goals. Each IT investment should be optimised respect to all these three dimensions, not only one of them. Also IT compliance initiatives should be compared with the mission of the company, to search to better alignment, and the systems capability, to optimize the IT service quality.
- *Communication*. Communication is necessary to inform about IT compliance initiatives, both inside and outside the company. Communication inside the company aims to create awareness about compliance and obtain desirable behaviour from human resources involved in the compliance process; it produces a more effective compliance activity and better results at lower cost. Communication outside the company is intended to inform about the commitment of the company to assure affordable financial disclosure and produces a higher trust by investors and financial markets.

4.3 To computerise the IT compliance process along time and space

IT compliance activities are to be performed along the time; companies should therefore define durable processes to accomplish their duties. However, IT compliance is a repetitive activity, so that it could be computerised; using IT applications to automate compliance:

- reduces complexity, as it requires standardization of both business processes and accounting policies, and of IT compliance processes;
- lowers compliance costs, because creates scale economies deriving from the use of standard solutions for compliance implementation and maintenance;
- improves reliability, because compliance software are able to face the weakness of accounting operations.

IT compliance software are called GRC systems: Governance, Risk and Compliance Management Systems. They are complex solutions that encompasses the use of several IT technologies: content management, compliance reporting systems, workflow and controls automation techniques. All these instruments are used to support audit, financial management, operational risk management and reporting processes. GRC systems could especially automate three fundamental compliance activity: processes analysis, documentation, controls monitoring.

Two different solutions are available to automate IT compliance: to acquire standard solutions or to develop in house solutions. Both of them present benefits and costs, virtues and vices. In the following paragraphs, they are analysed and explained in details.

5. GCR systems

GRC systems are IT solutions aiming to automate all the activities related to: govern IT systems, prevent risks and accomplish with rules and regulations. Their scope is wide and they cover different aspects (Fig. 4):

- finance and auditing, supporting controls applied to accounting and financial disclosure;
- IT, realizing automated controls applied to IT infrastructure and applications;
- risk, implementing the risk management relating data access and authorization;
- industry specific, such as Basel II for financial institution, etc.

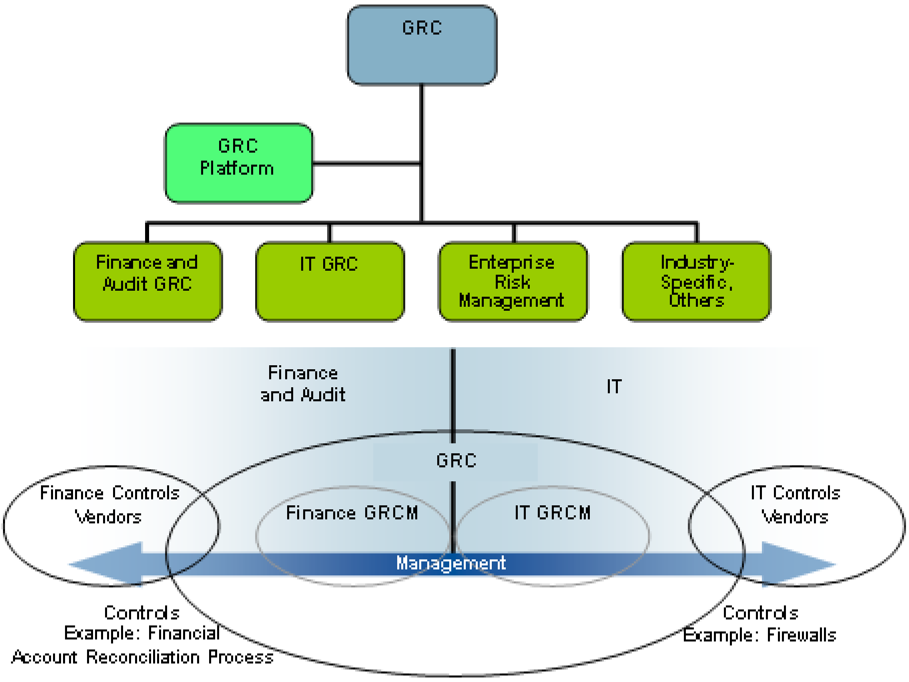
GRC
GRC Platform
Finance and Audit GRC
IT GRC
Enterprise Risk Management
Industry-Specific, Others
Finance and Audit
IT
GRC
Finance Controls Vendors
Finance GRCM
IT GRCM
IT Controls Vendors
Management
Controls Example: Financial Account Reconciliation Process
Controls Example: Firewalls

Figure 4: GCR systems scope

GRC systems integrate auditing aspects and IT aspects and cover all the processes in the enterprise, extending controls also outside the firm’s boundaries, to vendors and external partners.

The GRC solutions market is broad, with many different vendors using the term GRC to name their products, that are very heterogeneous in scoping and performance. A complete GRC solutions should cover these different tasks:

- user and operations management, implementing controls on access to the systems and on the correctness of data entry;
- records and data management, implementing controls on data security and database integrity;
- change management, implementing controls on applications life cycle and detecting changes impacting on the in scope operations;
- configuration and system management, implementing controls on the correct functioning of IT infrastructures;
- documentations, producing processes and activities maps and reporting about control activities.

A GRC system comprehends the following modules.

- Finance GRCM solutions support the management, workflow, dcumentation and reporting associated with financial controls.
- Audit Management system regards internal audit work papers, task management and workflow.
- Audit Data Extraction and Analysis is a set of tools for extracting data from business applications and running ad hoc analysis or queries.
- Segregation of Duties (SoD) is a system for ensuring that personnel do not have access to data in a way that creates the potential for fraud.
- Business Rules Management (BRM) liberates the logic governing operational decision making from individual applications, where it had been locked within programming code. It delivers substantial savings in application time to market and total cost of ownership. BRM implies monitoring transactional data in accordance with business rules established as controls. Business rules can be anything your organization uses to make an operational decision.

To acquire standard applications for GRC has several benefits: it reduces complexity and grant transparency and affordability, applying best practices and technologies. However, it requires companies to well align their specific risks with the GRC solution. This is not so easy: on one side, companies should well analyse their own risk profile and organization, mapping IT compliance goals and identifying key controls; on the other side, they should shop judiciously, selecting the best solution for their specific case, facing the complexity of GRC solutions marketplace. As GRC are not mature applications, they are still very heterogeneous and there are no well known standards to refer to. This spending is therefore a perilous step, to be done carefully.

6. EIM systems

IT components of standard GRC solutions are often not aligned with the specific control objectives of each company. On the contrary, the good alignment between GCR systems and business processes, compliance duties and IT mission is the basis for a successful IT compliance initiative. Moreover, may be GRC solutions don’t cover all the requirements a company needs; but companies should invest in complete solutions, not just in technology.

In this case, to develop an in house specific IT compliance application is the best solution. Companies could tailor their own IT compliance integrated model, able to cover their specific compliance duties and to govern the use of each piece of information available in the information system. The IT compliance application should be integrated in the Enterprise Information Management system: a system granting documents sharing and secure access to data, information and databases.

The EIM system integrates information, processes, people and IT services; its aim is to enhance the value of the business information repository, granting their security in the meantime. The EIM should efficiently manage the company’s knowledge base, authorizing access to information in a unique point.

The EIM system could be organized like in Fig. 5. The Enterprise Portal assure the unique access point to all the company’s information, both structured and unstructured data. The Enterprise Search Engine searches data and information inquired by the user; it also executes the audit data extraction and analysis tasks. The Collaboration Module manages documents and produces logs and report for the monitoring of in scope systems and processes. All the applications are integrated in the EIM systems, because all data and information are managed inside this framework; however, only some applications are in scope respect to compliance: Administration & Finance, Audit & Compliance, Process & Activity Management. The Process & Activity Management Modules automate processes analysis and mapping, also for IS auditing and compliance. The Audit & Compliance Modules exploit the Audit Controls and Segregations of Duty. The whole EIM system is framed in the Security system.

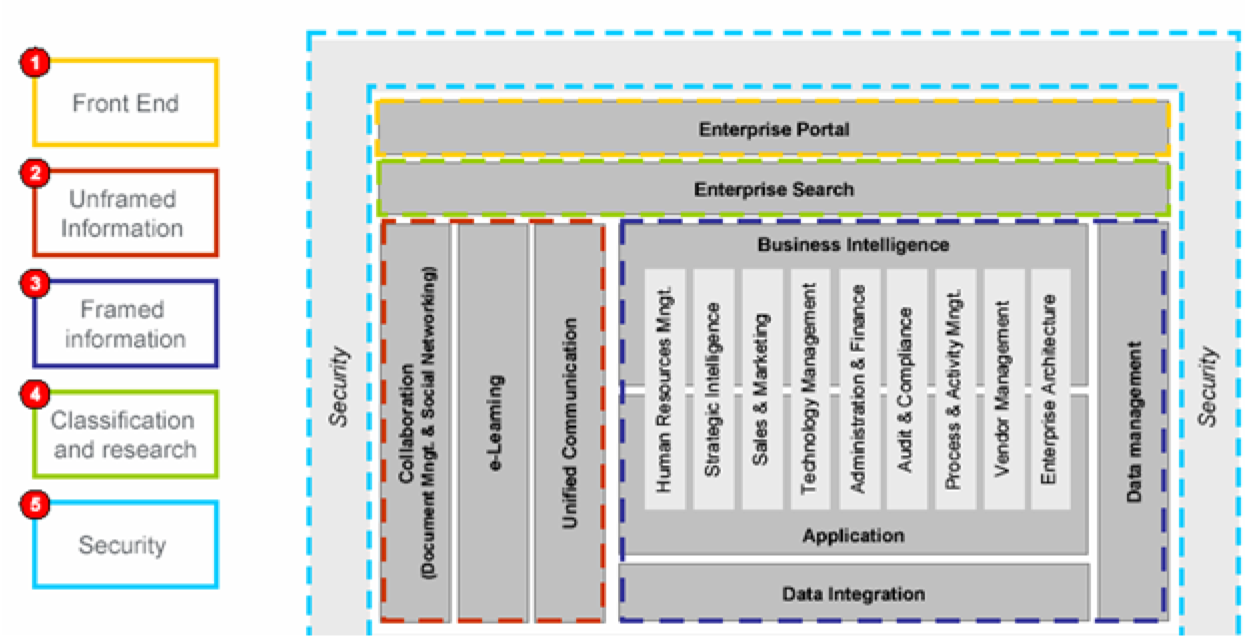

Figure 5: An EIM system

The functional schema of the IT compliance system embedded in the EIM systems is shown in Fig. 6. the system is composed by three layers.

- The presentation layer includes modules to support the navigation into the system and to access to information.
- The business logic layer execute the compliance tasks, that is:
  - it runs the rule based engine, to apply the controls to the in scope data processing;
  - it report about the non compliance operations and alerts about unauthorised accesses, mistakes in accounting and so on;
  - it controls the changes to the in scope applications;
  - it manage the logs and the traceability of each in scope operation.
- The repository layer manage the knowledge base; it includes several databases:
  - The compliance requirements contains all the laws, rules and regulations to be complied;
  - The compliance environment describes infrastructures and system configurations ;
  - The compliance documents repository contains all the policies, compliance documents and activities descriptions;
  - Compliance related events records all the logs and reports issued by the system;
  - Processes risks and cross references contains the list of all the reasonably anticipated risks and then related control objectives.

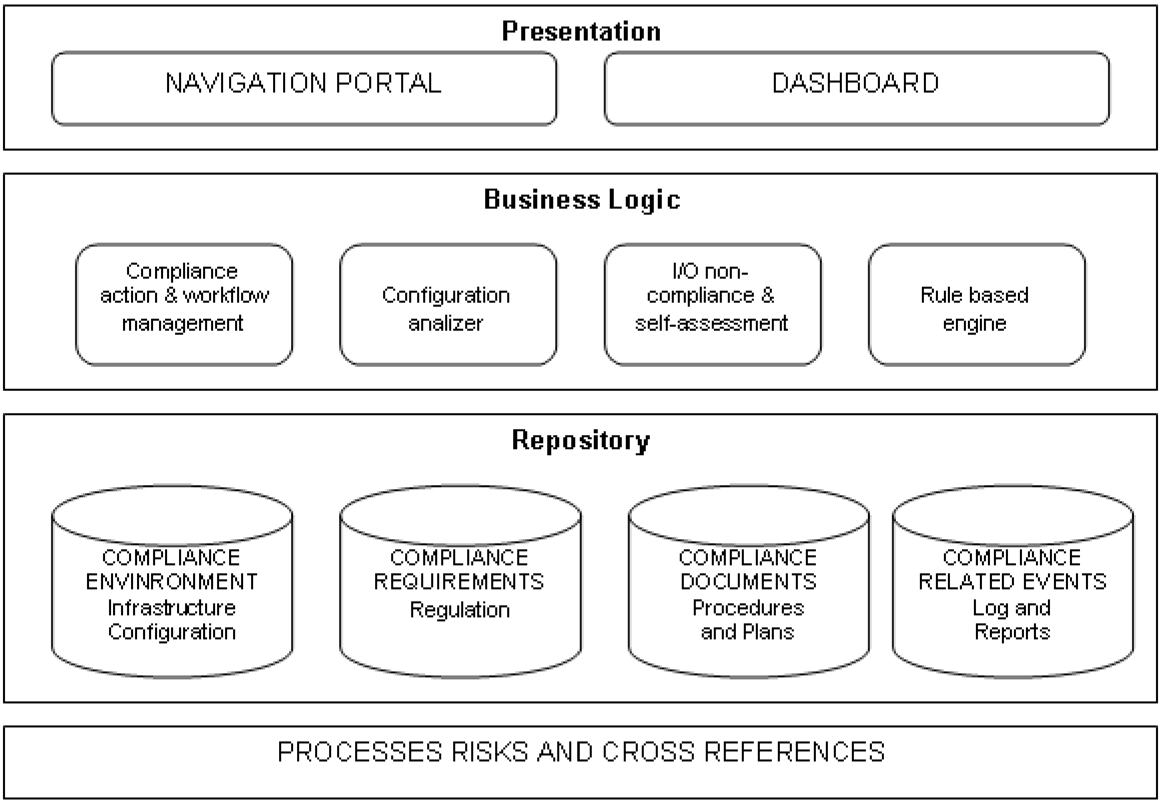
Presentation
NAVIGATION PORTAL
DASHBOARD
Business Logic
Compliance action & workflow management
Configuration analizer
I/O non-compliance & self-assessment
Rule based engine
Repository
COMPLIANCE ENVINRONMENT Infrastructure Configuration
COMPLIANCE REQUIREMENTS Regulation
COMPLIANCE DOCUMENTS Procedures and Plans
COMPLIANCE RELATED EVENTS Log and Reports
PROCESSES RISKS AND CROSS REFERENCES

Figure 6: The EIM compliance module functional schema

7. Conclusions

IT compliance is a veritable challenge for large companies, both for the high costs of IT auditing and for implementation difficulties. Such a huge effort in money and work needs to return better results, than to simply accomplish financial rules. To obtain the best return from IT compliance activity, company could act in two opposite directions:

- to reduce the cost of IT compliance activities;
- to enhance the return of IT compliance.

To gain efficiency and reduce cost, companies could use an automated IT auditing system; the best solutions are GRC systems, that is, integrated IT systems able to assure in the meantime organization, control and protection for accounting information systems. The initial investments in GRC systems produce important savings in the lifecycle of IT compliance.

To enhance the return from IT compliance, companies could use the GRC system also to create an Enterprise Management Information System, that is, to integrate all the financial information about the company and to put them at disposal of all the interested workers all over the organization.

To reach these goals, companies should carefully analyse both the structure of their information systems and databases and their IT governance framework; it means that, indirectly, the implementation of GRC and EIM systems produces also an improvement of the architecture of Information Systems and of the effectiveness of IT governance.

References

COSO (2005), Internal Control – Integrated Framework

COSO (2006), Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting

Dameri R.P. (2006), “IT governance e creazione di valore nei sistemi aziendali complessi”, impresaprogetto n° 1(2008), Governance, Risk and Compliance Management Suite. A software selection for implementing an integrated compliance framework in listed companies, Genova, 2 April

Dameri R.P., Garelli R. (2007), “A model for IT governance in business groups”, 13th European Conference on Information Technology Evaluation, Genova September

Damianides M. (2005), “Sarbanes-Oxley and IT governance: new guidance on IT control and compliance”, Information Systems Management, Winter 2005

Giustiniano L. (2007), Strategie, organizzazione e sistemi informativi: dall’IT alignment all’IT governance, Franco Angeli Milano

ITGI (Information Technology Governance Institute) (2004), IT Control Objectives for Sarbanes-Oxley

ITGI (Information Technology Governance Institute) (2005), The Val IT Initiative

ITGI (Information Technology Governance Institute) (2005), CobiT 4.0. Control Objectives for Information and Related Technology

PCAOB (Public Company Accounting Overside Board) (2005), PCAOB Audit Standard n° 2. Control Objectives for Information and Related Technology

Rappaport A. (1986), Creating Shareholders’s Value: the New Standard for Business Performance, The Free Press

Remenyi D., Money A., Sherwood-Smith M. (2000), The effecftive measurement and management of IT costs and benefits, Butterworth-Heinemann, Oxford

Schwartz A., Hirschheim R. (2003), “An extended platform logic perspective of IT governance: managing perspections and activities of IT“, The Journal of Strategic Information Systems, Vol. 12

Turner L., Weickgenannt A. (2008), Accounting Information Systems, Wiley-Blackwell London

Van Grembergen W. (editor) (2003), Strategies for Information Technology Governance, IGI Global

Ventrakaman N., Henderson J. (1996), “Aligning business and IT strategies”, in J. Luftman (Editor), Competing in the Information Age: Practical Applications of the Strategic Alignment Model, Oxford University Press, New York

Weill P., Broadbent M. (1998), Leveraging the New Infrastructure, Harvard Business School Press, Boston MA

Weill P., Ross J. (2004), IT Governance. How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, Boston MA