Feature

Risk-based Approach to IT Systems Life Cycle and Change Control

Loic Jegousse, CISA, CISM, is the director of IT standards, compliance and internal controls with MDS Inc., a global life sciences organization. Jegousse has spent his 11-year career in technology risk consulting and audit in global industries such as financial services, life sciences and professional services. His specializations include IT controls, regulatory compliance, information security, IT governance, IT outsourcing and process improvement.

> *"If one is forever cautious, can one remain a human being?"*
> *—Aleksander Solzhenitsyn*

The human brain is inadequately trained to manage risk effectively: Countless people continue to smoke tobacco, drive without a seatbelt and engage in other hazardous behaviors. Individuals may accept unreasonable risk (e.g., get a loan while already indebted to invest on a speculative investment) if it can yield a higher payoff.

Running against human nature, regulatory and governance pressures—e.g., the US Sarbanes-Oxley Act, Basel II, International Organization for Standardization (ISO) standards—are prompting management to systematically identify significant risks and mitigate their impact. In risk management literature, risk is seen as a function of the probability of occurrence and impact. These are difficult to assess with precision. In real life, humans tend to underestimate ("accept") risks that have a low or remote probability of occurrence (even those that could have a catastrophic impact) for reasons including scarcity of resources (especially time) and tendency to focus on short-term objectives. In the business and technology world, managers struggle to implement sustainable and cost-effective means to balance risks and operational constraints.

BALANCING EXERCISE

This article explores the concepts of a risk management model in the context of change management to IT systems, and their ramifications with respect to system life cycle controls. However, the model and its concepts could be applied to other business risk areas. **Figure 1** illustrates a practical, risk-based approach to IT systems that proposes a balance between two extreme models (noncompliant vs. highly compliance-focused). This approach is aiming to deliver:

- Documentation and system validation efforts commensurate with the risk
- A repeatable, measurable and scalable IT risk assessment process over IT systems
- Sustained compliance with regulatory requirements

The main critique of the highly compliance-focused approach is that it is resource-consuming and difficult to apply consistently. In real life, an illustration of such an approach applied to the airline industry would be that all components of the aircraft, as well as passengers and staff, would be thoroughly and consistently checked for structural damage, identity of passengers would be checked, inspection of luggage would be conducted, etc. All possible scenarios that could compromise safety (e.g., liquids, hidden explosives, collusion with staff) would be examined, ranked and managed accordingly in a series of standard procedures and checklists. Such conservative approaches, while robust on paper, are not necessarily sustainable in the long term, as large costs would be involved.

At the other end of the spectrum, a noncompliant approach would involve a highly judgmental, undocumented and subjective assessment of risks. In the airline analogy, the unstructured control would be left to airline crew screening sample passengers via an informal procedure, e.g., using observation and simple inquiry only. Such an approach would cause unreasonable acceptance of risk to passengers' safety and would understandably cause public concerns.

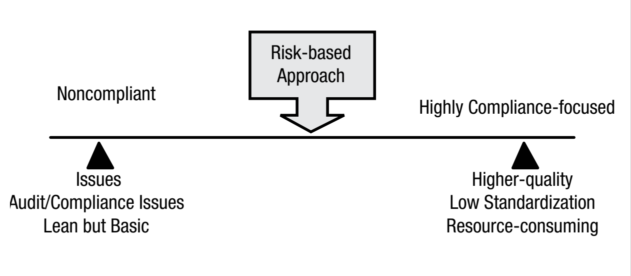
REDEFINING RISK

When it comes to IT systems life cycle and change control, there is often some confusion as to how to comply with certain regulatory requirements relating to computerized systems, without producing massive amounts of documentation for a simple change or a large implementation project. For instance, publicly traded

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Figure 1—Balance Between Noncompliant and Highly Compliance-focused Approaches



organizations encountered an excessive paperwork burden during the first years of enforcement of the US Sarbanes-Oxley Act requirements for systems that were remotely related to financial reporting. Other examples are the "good practices" from the US Food and Drug Administration (FDA), which require computerized systems to be maintained in a validated state.

Taking, as an example, a complex business application, such as an enterprise resource planning (ERP) system, for which code changes or extensions occur frequently, some areas of the application system, such as payroll, cash management or general ledger, are subject to a higher level of data integrity and system security. When a particular change is made to an application system or its supporting hardware components, how can management ensure that it will not have any unforeseen negative impact on certain functionalities or data? On the one hand, IT could take a hands-off approach and hold the business users accountable for data integrity. Such a noncompliant approach could rapidly cause soaring audit costs, regulatory issues and lack of trust toward the systems. On the other hand, performing extensive validation, regression testing and documentation for the entire system every time a change is made to ensure that everything works as expected can be expensive and would not be sustainable in the long term. There needs to be a compromise between these two models. The solution is to use a risk assessment framework that will assist in simplifying the degree of system life cycle controls relative to perceived risks.

RISK ASSESSMENT FRAMEWORK

The proposed risk-based approach to IT systems is based on classes of risk (hereafter referred to as risk factors). The value of the risk factors relates to a situation that has a combined probability and impact value, which can be expressed as a monetary value (e.g., net present value) or in a qualitative manner. Risk factors are to be defined based on the potential damage to the organization, as well as the existence of predetermined methods that can be used to reduce the damage. As an example, this article further details a two-dimensional model that involves the following risk factors:

- **Business**—A situation that may result in loss of productivity, financial loss, liability or reputation damage, if it is not managed effectively. An example of a risk mitigation method to reduce business risk would be to increase management oversight of the activities.
- **Regulatory**—A situation that may modify the configuration of key automated controls that support compliance with regulatory requirements (e.g., controls over financial reporting or other key business processes such as privacy, drug or medical device safety). An example of a risk mitigation method to reduce regulatory risk resulting from data integrity issues would be to increase the depth and breadth of system life cycle artifacts.

To operate such a process, management needs to develop explicit criteria to define what the low, medium or high risk ratings mean. For instance, in the context of regulatory risk, high risk criteria are defined per an explicit list of systems controls that are subject to regulatory requirements. Low risk criteria include instances with a very remote likelihood to modify the integrity, availability or confidentiality of records or sensitive data. Each risk factor is assessed for a low, medium or high value. The results are then plotted on the risk level chart, which returns the resulting risk level (e.g., 1 to 4), as shown in **figure 2**.

RISK MITIGATION STRATEGIES

The risk levels are defined in a manner to provide a higher level of management oversight as the business risk factors increase. As an illustration, the risk levels may be defined as shown in **figure 3**.

In addition, the resulting risk levels involve an increasing amount of system life cycle controls, as the regulatory risk factors increase. This would include increased effort with respect to system documentation, testing and code review. **Figure 4** is an illustration of the relationship between the risk levels and the typical documentation deliverables required for various stages of the process/life cycle (e.g., design, testing, promotion, validation).

Figure 2—Risk Level Chart

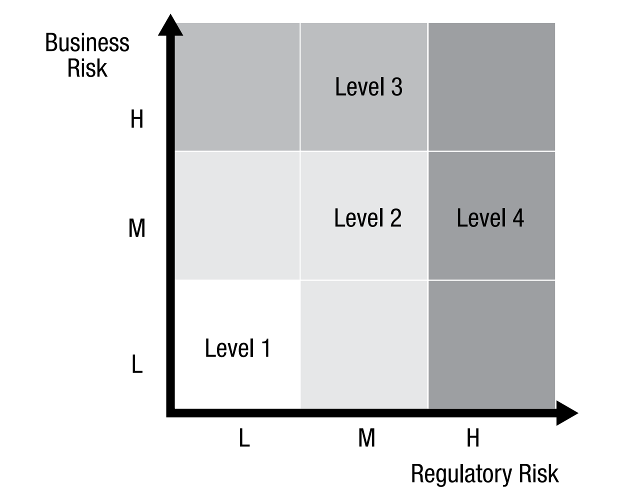


Figure 3—Risk Levels for High Business Risk Factors

Risk Level	Management Oversight
Level 4	All members of the IT leadership team plus one member of quality assurance/compliance/audit, etc., function
Level 3	All members of IT leadership team
Level 2	One member of IT leadership team
Level 1	One manager of IT

Figure 4—Risk Mitigation for High Business Risk Factors

Risk Level	Stage A (e.g., formal specs)	Stage B (e.g., formal testing)	Stage C (e.g., change control form)	Stage D (e.g., validation report)
Level 4	Required	Required	Required	Required
Level 3	Required	Required	Required	Discretionary
Level 2	Discretionary	Required	Required	Discretionary
Level 1	Discretionary	Discretionary	Required	Discretionary

CRITICAL SUCCESS FACTORS

The risk-based approach should be supported by standard operating procedures (SOPs) to provide instructions and training to the affected personnel. Frameworks such as COBIT, IT Infrastructure Library (ITIL) and Good Automated Manufacturing Practices (GAMP) provide high-level requirements for the design of IT processes over the system life cycle, application management, access control and change control.

When designing a risk-based approach, it is important not to underestimate the effort required in performing an accurate inventory of automated systems functions or situations that are linked to high risk factors. This inventory is the backbone of the risk-based procedure, and its accuracy and simplicity will enable an effective process. A key success factor is the adequate involvement and support of the various quality assurance, privacy, legal, audit, regulatory affairs or compliance teams in high regulatory risk situations. Some IT system changes may, based on risk ratings, require sign-off from key stakeholders before proceeding.

CONCLUSION

Organizations that have successfully implemented risk-based approaches have observed cost savings, cycle time and customer satisfaction improvements. Management can appreciate that lower risk change requests can be processed swiftly, while still demonstrating the rigorous analysis that was performed to justify a low risk level. In addition, key stakeholders (even outside of IT) are now systematically consulted before approving system changes that are deemed as higher risk. Such an approach can also deliver increased governance over those particular risks that are not tolerated within the organization.

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.