

Managing Information Systems Risks: A Holistic View

Christine LABARRE, Manager

While risk management is not a new activity for most companies, many still confine the development of Information Systems risk management to IT departments, due to the specificity and complexity of the decisions that need to be made.

However, growing regulatory compliance constraints, the increasingly strong correlation between business skills and Information Systems (IS), and the exposure of critical activities to IS risks has led more and more companies to adopt a holistic approach, allowing business optimization regarding to their risk appetite level.

Information Systems Vulnerability

Information is one of a company's major assets, on equal footing with other assets linked to production systems such as physical, human or financial assets. It acquires value when it helps business stakeholders tackle strategic issues.

IS Risk Assessment

Between activity-related risks and technology-related risks, the potential for failure is high and the scope of Information Systems risks is very wide. However, the management of these risks is still often separated into silos (operational risks, projects risks, IT security, compliance, governance...) and the absence of common and homogeneous measuring criteria leads to disparities in the identification and implementation of corrective measurement priorities.

The implementation of IT security management is a prerequisite to IS risk management. The main strategic security decisions should be based on business needs and challenges, which are defined by an analysis of the risks incurred by a company's various entities. The evaluation of these risks, compared with the cost of associated protection measures, ensures the optimization of the resources devoted to security.

But Information Systems risk management can only be beneficial in the long term if it addresses a business's expectations and is in line with a company's overall strategy.

Thus, it is important to hold managers accountable for identifying and implementing appropriate processes. This responsibility includes subjacent Information Systems; more precisely, with respect to data protection and information security. They must understand that there are real and quantifiable costs associated with various types of risks.

IS Risk Management

IS risks are not limited within a company's own perimeter. With the complexity and increasing openness of Information Systems, an external partner's failure can lead to dramatic consequences for a company's IS and its leaders can be held legally responsible for these security lapses, even if they were introduced by the external partner.

Furthermore, Information Systems are not limited to information processing: information arises in forms that vary greatly in terms of storage, representation and transmission. The risk of losing sensitive information (rendered more acute by the use of cell phones, laptops, USB flash drives, Web access...) can lead to tremendous loss of revenues.

The human dimension of security is key. Counterintuitive to what one might suppose, internal attacks within a company have the worst impact. Information security is thus a pervasive concern which must be supported by management at all levels of a company.

Reaching a 0% failure rate at a reasonable cost is impossible. That is why risk coverage must be planned accordingly. The Information Systems risk management strategy must be aligned with general risk management, and conform to the company's accepted tolerance level.

Expected Benefits of Implementing an Information Security Management System (ISMS)

The principle behind the holistic approach is that the whole is not equal to the sum of its parts. It results from a construction, an organization of intelligence that always exceeds the sum of its parts. Information Systems risk management fits this principle. The consistent and transverse management of all of a company's activities, along with the coordinated and active participation of all involved parties, will in effect lead to the minimization of overall risk. Information Systems risk must be integrated in to this approach at this step.

Information security can thus be defined as a general risk management device that guarantees a suitable level of protection and ensures the availability, integrity, confidentiality and traceability of this asset. It covers a vast field, including network and Information Systems security, exchange authentication, access and authorization management, governance, protection of economic intelligence, data classification, informational assets management, continuity of activity and the training and sensitizing of the actors involved.

Technology cannot solve all security problems on its own. The solution rests on a complementary approach that is as much organizational as technical. Risk management makes it possible to assign a rational justification to strategic choices. The convergence between traditional risk management methods and Information Systems risk management generates financial profits, which can be achieved by setting better priorities in remediation efforts and which produces benefits inherent to good risk assessment and strong decision-making. In addition, appropriate risk management, based on recognized standards, increases a customer's confidence factor for a company.

Software developers have well understood the importance of an overall process and their new GRC tools (Governance, Risk and Compliance) offer companies a framework for developing this. However, these tools can only be effective if a company's risk policy is clearly stated, well-conceived, controlled and constantly improved.

Information Security Management Systems then make it possible to produce results that are actual, enduring, measurable and proportioned with the risks.

Frames of Reference and Good Practices Referential

The implementation of an Information Systems risk management policy within a company requires the board's support. It fits into an iterative process of continuous improvement and can be based on recognized good practices (ISO 2700X Standard, EBIOS, Mehari methodology, COBIT...).

The ISMS model put forward by the ISO 27001 standard is based on an approach to risk management that defines a set of security measures. It makes it possible to ensure that information security is organized, in place and fits into a process of continuous improvement. It does so by applying Deming's "Plan Do Check Act" cycle, instantiated to IT security.

The risk analysis process breaks down into six main stages:

- A stage of upstream governance which defines a framework, objectives and perimeter, and that also validates the risk assessment in agreement with a company's policy. This stage aims to establish the foundations of a common risk management policy, to define a communications plan and to allow for the implementation of risk-driven management.
- A business stakes analysis stage that allows for the classification of resources dedicated to a company's key processes. The risk analysis should be centered on critical assets. This stage requires the participation of operational management and is based on the cartography of the Information Systems' four layers: business, functional, applicative and technical.
- In the vulnerability diagnosis stage, the possible threats that could occur (potentiality and impact) are identified, assessed, and the acceptable risks are differentiated from the unacceptable ones. This stage rests on an analysis of transverse processes and requires the participation of central departments (IT, HR, the legal division...).
- A risk treatment stage in which the risks can be reduced, transferred, avoided or accepted according to criteria defined beforehand.
- A stage of planning, managing and implementing adapted controlling processes that measure the effectiveness of the ISMS.
- The model's ultimate stage is of improvement. It is important to take into account on a regular basis the changing context of an organization, and to alter a policy, if necessary, based on a company's strategic objectives and to review the risk analysis. A new iteration of the various preceding stages will allow for the refinement of this risk management model.

No organization can maintain its activity and eliminate all risks. On the contrary, taking risks creates value as long as their management is optimized and allows for risk identification and assessment. A company can thus define, with full knowledge of the facts, new opportunities and offer new products with controlled risks and optimal tariffs, which leads to better positioning in the market. The point is not to deter but rather to facilitate risk-taking while arbitrating between risk and performance.

From a company's vantage point, optimal risk management on the one hand contributes to a reduction in the volatility of results, thanks to the creation of standards, which lead to a better appreciation of all dimensions of the risks taken. On the other hand, it also contributes to optimization of how its own capital is allocated in its various activities.

In that sense, the consistent assessment of risk is crucial to the development of an organization as a whole. That is why it is important to manage Information Systems risks on a company-wide level by complying with the rules of business management. By adopting this overall vision, a company can capitalize on its diversified business offerings and thus take more risks in certain activities with strong profitability.

The implementation of an ISMS makes it possible to adopt this holistic vision and to diffuse the risk culture at all levels of an organization. The initial deployment investment is quickly compensated by the induced optimization of risk management activity.