

Information Systems: At Risk ?

>> A fresh start...

Now is the time of season's greetings. The majority of our contacts in France have replied to us saying that 2010 will be the year of South Africa !

They probably refer to the World Cup ? This reminds me of how France got qualified, and it was one of the most shameful sport memories of 2009. That and the disastrous rendering of Nkosi Sikelel' iAfrika by the rasta man at Stade de France.

These instances are memories we would rather forget as a new year starts...!

So let's create good memories in 2010 ! In sport, and more to the point in finance ! (which is, let's not forget, the subject of this newsletter).

To start the year we have decided to focus on a broader subject that is applicable to all, "Information Systems Risks".

Take a step back and look at the organisation as a whole, and not only on the risks that are under constant scrutiny.

Our world has been rocked, and the aftermath is always a good time to reflect on those unassuming risks that creep in.

Until next time, ...

Nelly Willemse

>> Managing Information Systems Risks: a Holistic View

While risk management is not a new activity for most companies, many still confine the development of Information Systems (IS) 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 IS, and the exposure of critical activities to IS risks has led more and more companies to adopt a holistic approach, allowing business optimisation regarding their risk appetite.

> 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 to tackle strategic issues.

IS Risk Assessment

Between activity-related risks and technology-related risks, the potential for failure is high, and the scope of IS 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 the company's various entities. The evaluation of these risks, compared with the cost of associated protection measures, ensures the optimisation of the resources devoted to security.

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

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

IS Risk Management

IS risks are not limited within the company's perimeter. With the complexity and increasing openness of IS, a third party's failure can lead to dramatic consequences for the company's IS, and its management can be held legally responsible for these security lapses, even if they were introduced by the third party. Furthermore, IS 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 IS risk management strategy must be aligned with general risk management, and must conform to the company's accepted tolerance level.

Continued on page 2...

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

The principle behind this holistic approach is that the whole is not equal to the sum of its parts. This results from the collation of intelligence and operational organisation that always exceeds the sum of its parts. IS risk management fits this principle. The consistent and transverse management of all of the company's activities, along with the coordinated and active participation of all involved parties, will in effect lead to the minimisation of overall risk.

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 includes network and IS security, exchange authentication, access and authorisation management, governance, protection of economic intelligence, data classification, managing information as an asset, the continuity of activity, training and the awareness of all resources involved.

Technology on its own cannot solve all security problems. The solution rests on a complementary approach that is organisational as well as technical. Risk management makes it possible to assign a rational justification to strategic choices. The convergence between traditional risk management methods and IS risk management, by setting better priorities in remediation efforts, produces benefits inherent to good risk assessment, strong decision-making, and generates financial profits. In addition, appropriate risk management, based on recognised standards, increases customers' confidence in the company.

Software developers have clearly 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 the 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 proportionate to the risks.

Frames of Reference and Best Practices

The implementation of an IS 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 recognised good practices (ISO 2700X Standard, EBIOS, Mehari, 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 organised, functional, 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 that defines the framework, objectives and scope, and also validates the risk

assessment in agreement with the 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 stage of business stakes analysis that classifies the resources dedicated to the 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 IS' four layers: business, functional, applicative and technical.

- > In the vulnerability diagnosis stage, the possible threats that could occur (potentiality level 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, legal department...).

- > 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 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 the company's strategic objectives, and to review the risk analysis. A new iteration of the various preceding stages will refine this risk management model.

No organisation can maintain its activity and eliminate all risks. On the contrary, taking risks creates value as long as the management of these risks is optimised and leaves space for risk identification and assessment. The point is not to deter but rather to facilitate risk-taking and risk / performance arbitrage.

From the company's vantage point, optimal risk management 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. It also contributes to the optimisation of the allocation of its own capital in its various activities.

In that sense, the consistent assessment of risk is crucial to the development of an organisation as a whole. By adopting this overall vision, the company can capitalise on its diversified business offerings and thus can 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 the organisation. The initial implementation investment is quickly compensated by the induced optimisation of risk management activities.