Information Technology Risk Management

By Jeffrey D. Streif, CPA, CFE, CISA, QSA

Is your information technology risk management (ITRM) program integrated into your overall enterprise risk management (ERM) strategy? IT risk management programs seem to have their own little island and language, which is why so often they are separated from the rest of the ERM initiative. Information technology (IT) assets affect most business processes either directly or indirectly in today's business operations. It is imperative that IT risks be integrated into the business risks.

Risks can be classified into many different categories such as environmental, process, financial, operational, information technology, strategic, treasury, legal and compliance. Even though IT typically has its own category of risk, it is important to note that IT can affect multiple categories as the threats identified can trigger risks in other categories. For example, an identified IT threat of unauthorized access can be related to other risk categories such as reputation, legal and compliance risk. A recent data breach at a company has led to multiple risks being realized through a chain of unfortunate events. Companies should as part of their ERM program try to identify such events and the response to those events to limit the damages. When multiple risk categories are involved in an event, there are multiple types of damage involved such as financial, legal, reputational and compliance.

Risk management is not an easy task to undertake as there are typically a lot of obstacles in the way. Some of the most common obstacles are company culture, costs, knowledge, lack of documentation and poor communication. IT risk management control objectives involve security, compliance, confidentiality, integrity and availability. An effective ITRM program involves the following high-level steps:

1. Obtain board and senior management approval and involvement;
2. Select a leader to run the program;
3. Perform initial IT risk assessment (which is integrated into overall ERM assessment);
4. Develop a preliminary action plan and responses;
5. Understand risks and appetite of company;
6. Develop a reporting and communication process;
7. Develop a monitoring process; and
8. Perform steps three through seven again.

It's important to remember that IT risks change daily. Therefore, the monitoring and communication steps are critical and ongoing. In today's business environment, new technological trends are popping up with increasing frequency. Some of the popular ones are consumerization of technology, cloud computing and cybercrime. Companies are being hit with numerous requests to utilize new versions of devices like smartphones and tablets. Cloud computing often entails outsourcing technology resources to third parties. Cybercrime makes the news almost daily with headlines like, "ATM Thieves Steal $45 Million in Massive Cyber Attack."

As part of the risk assessment and integration process, company policies and procedures need to be updated to take advantage of the new technology. This new technology can possibly lead to improved communication, more efficient business processes and cost savings. However, with any new technology, there comes new risks associated with using it. As part of the IT risk assessment step, the company should identify the risks associated with the use of the new technology to verify that the benefits exceed the risk and that the return on investment is acceptable. Utilizing cloud services can possibly save on licensing and infrastructure costs, but the company needs to be aware of where the data is and how it is being secured. Introduction of personal devices into the business environment can increase risks of data leakage or unauthorized access if the device's security cannot be managed properly.

There are numerous categories of IT risk to consider when developing and managing your ITRM program, which include but are not limited to:

- Third party suppliers and outsourcing;
- Security of mobile devices;
- Data security;
- Compliance, legal and regulatory;
- Applications and related databases;
- Staff (training and awareness);
- Operations and communication; and
- Strategic alignment with business objectives.

Overall, your information technology risk management program should be integrated into the business enterprise risk management program as IT risks can affect every aspect of the business operations. The program needs to monitor not only internal risks but external risks as companies try to find a competitive advantage through adoption and use of new technology.

Jeff Streif is a principal with UHY Advisors in St. Louis and leads their Technology Assurance and Advisory Services Practice. He chairs the MSCPA Information Management and Technology Assurance Committee and is the treasurer of the St. Louis Chapter of ISACA. Jeff can be reached at jstreif@uhy-us.com.