REGULATORY CHIEF TALKS ABOUT ENTERPRISE AND TECHNOLOGY RISK MANAGEMENT

MATTHEW J. PUTVINSKI, CPA, CISA, CISSP

Recently, the Comptroller of the Currency made some very interesting remarks in regards to IT governance at community banks. In his address at the Bank Information Technology Training Conference in Atlanta on October 2, 2012, Thomas J. Curry, stressed that "as smart phones, tablets, and wireless Internet become ubiquitous, they are changing the business model of modern banking." Gone are the days of investing heavily into physical branches. Now is the time to shift those investments into channels that a growing number of your customers want. A community bank still needs a strong physical presence to show your commitment to the community but perhaps the dial needs to be turned a little to make sure future investments ensure your customers are satisfied with their banking experience.

The meaning in his message was very clear. There are major components of IT that you need to be managing well and that the examiners will be checking. Let's review his key points and compare them to what we see really happening.

KEY POINT #1 – A STRONG ENTERPRISE RISK MANAGEMENT PROGRAM IS INSTRUMENTAL TO THE SAFETY AND SOUNDNESS OF THE INSTITUTION

Mr. Curry remarked, "but regardless of size, the safety and soundness of these entities depends on the quality of their enterprise risk management, and in this information-driven marketplace, that includes ensuring the security of the technology and data that, today, are as vital as any aspect of the business."

Over the last few years, we have seen a number of examiners tossing around the term "enterprise risk management" but have yet to truly define what that means. If we can all agree that it will help mitigate bad things from happening, how do we know when we have achieved a strong program? One of the biggest hurdles that institutions face is the traditional nature of risk assessments where each department still continues to do them in their own silos. The primary reason for this is that technologies were not available to build a true ERM program. That is quickly changing.

A good program not only identifies all the people, processes and technologies within the institution, but also makes sure that everything is linked. How would you know the true risk of a vendor, without knowing the risk of the technology the vendor is providing? How does a good customer information privacy program work without know what controls are present for systems handling customer information?

Here are some red flags that, if present, could derail an effective ERM program:

1. Lack of Executive Sponsorship – Senior Management feels it's merely a regulatory cost and does not provide any business value.

2. Lack of an ERM committee – Departments are not getting together to talk about risk.

3. Lack of proper audit planning – Your internal audit and compliance programs are not driven by risk assessments.

4. The ERM does not align with the business strategies – Your individual risk management processes are not a component of a more holistic enterprise-wide Risk Management process.

5. No one in the institution understands your ERM strategy – A senior manager or executive cannot explain the overall strategy of the banks ERM philosophy.

6. The Board doesn't get it – The Board finds it difficult to accurately measure your risk exposure.

7. You have not defined your risk appetite – Senior management is unsure what risks they really want to take.

8. ERM is not involved in new products – You roll out new deposit products and do not feel the ERM program is necessary.

Recognize any? If so, it may be a good time to revisit or revamp the program.

KEY POINT #2 – SECURITY THREATS ARE GROWING AND, MORE IMPORTANTLY, CONSTANTLY CHANGING

Another point that the Comptroller presented very clearly was that while smartphones and other technology initiatives are flooding the market, "… we must not forget that the same gadgets and supporting networks that make our lives easier also carry enormous operational, reputational, and other risks for banks and thrifts."

A component of your ERM program is making sure you have a flexible and robust information security program that can handle the latest threats. The good news is that new threats rarely cause significant diversions or changes to your program. They usually just need to be evaluated and made sure you are addressing them. The bad

news is that it becomes increasingly difficult to keep up with them.

How do you keep up with the threats? Here are some suggestions:

1. Social media can be a great source of news. The problem is that it also can be a ton of unnecessary noise. If you are using sites like Twitter or LinkedIn, setup lists or access groups of folks that are committed to only sharing the news relevant to you. If you follow the right people, you can be adequately informed of what's truly going on in the information security world.

2. Join associations such as ISACA (www.isaca.org) and ISSA (www.issa.org). These associations are dedicated to educating you on maintaining security, confidentiality and integrity of your information systems.

3. Develop relationships with risk professionals. Some community banks are just too small to be able to afford full time Risk professionals. Find yourself a guide on the outside that can help you with your ERM initiatives.

The key is preparing for the "Unknown". You don't know how the next breach will happen but you should feel comfortable that you did your due diligence to try to prevent it.

KEY POINT #3 -BUSINESS CONTINUITY PLANS NEED TO BE MORE ROBUST

While most Business Continuity Plans we see typically include most of the areas required by the FFIEC, one big component still remains a challenge. A good ERM program means that you truly have an idea of how each business unit can deal with either a technology outage or a horrific environmental disaster. As the Comptroller says, "To consider ourselves prepared for the worst, it is essential that our banks and savings associations can remain operable in the event of a terrorist attack or natural disaster, and that they all have robust business continuity plans in place."

Most likely, if you have a plan that merely gets refreshed every year with employee names and phone numbers, it is most likely not going to be very helpful when a disaster occurs. Business Continuity planning means not only making sure you have the correct names, forms and phone numbers , but it also that you understand the different business lines in the institution and set a score on the likelihood and impact a disaster can have on them. This information can be used to develop metrics such as the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to clearly illustrate expectations with the business lines on when they will be back and running. Lastly, make sure you have a robust testing plan that will evaluate all the critical areas of the institution. Testing a backup tape or

short roundtable discussions with your senior manager is just not sufficient anymore.

KEY POINT #4 –REGULATIONS ARE GOING TO REQUIRE MORE INVESTMENTS IN YOUR TECHNOLOGY INFRASTRUCTURE

In particular, the Comptroller mentioned how Dodd-Frank will have serious implications on the technology you use. As he says, "Congress intended the increased reporting and oversight requirements of the Dodd-Frank Act to enhance the stability of the U.S. financial system overall. But due to their scope and breadth, these requirements also present significant challenges to the technology systems of banks and thrifts."

The biggest issue we see is the data reporting requirements that you will be faced with. The government is going to be asking for more information that you most likely have, though cannot be easily obtained using your current technology.

Mr. Curry continued, "Taking advantage of these opportunities, however, will require major upgrades to IT infrastructures, and these changes, if not done the right way, have the potential to affect how these systems perform."

While it is still not exactly clear what will need to be done, it will be important for you to stay on top of the guidance that eventually comes from the regulation and make sure you understand how your technology vendors are going to deal with it.

KEY POINT #5 –THE IMPORTANCE OF VENDOR MANAGEMENT

"A danger for banks and thrifts lurks in the reliability—or lack thereof—of third parties hired to manage data and provide IT knowhow, or even Internet access."

We have all either seen or experienced an issue with a third party that was found negligent protecting their customer's data. Whether it's a lawyer who loses a laptop, statements sent to the wrong customers or an offsite storage provider that loses a box of files, your reputation and future is on the line. As the Comptroller mentions, "Banks and thrifts have repeatedly found themselves the victims of lax security by third parties."

Many of the vendor management programs we see focus solely on IT vendors. While it makes sense that these would be targeted first, its typically the smaller vendors you work with that will most likely give you the most headaches. They are more likely to not invest in the same level of security protection that you are. That doesn't mean you have to find a larger vendor but it does require that any vendor being provided with customer information needs to go through some level of scrutiny and contracts should clearly illustrate your expectations.

The Comptroller sums it up well to say, "Effective vendor management programs are not only a regulatory expectation; they are necessary components of effective enterprise risk management."

CONCLUSION

This was a nice reminder from the regulators as to what may be expected of you. The questions will now be how the individual examiners interpret the guidance. Those who address the idea of ERM are likely to have a much easier exam in this area than those who avoid it. We are seeing many of our clients not only embrace the idea of ERM, but also are finding value in their investment. When done correctly, good ERM programs not only mitigate regulatory criticism, but help keep you focused on the business of Banking.

MATTHEW J. PUTVINSKI
CPA, CISA, CISSP
MEMBER OF THE FIRM
617-428-5479
MPUTVINSKI@WOLFANDCO.COM

WOLFANDCO.COM