

# COMMENTARY

## The Evolution of ERM in US financial services

by David Zach

Philadelphia, September 2011

*Why should you implement an ERM program now?*

The US financial services industry is under high scrutiny after the recent federal bailout, and rightly so. The US Government spent \$700 billion of taxpayer money in the Troubled Asset Relief Program. Many analysts forecast the true cost of the bailout to be in excess of \$4 trillion. This has led to an industry-wide focus on Enterprise Risk Management (ERM) and what can be done to stop this kind of catastrophe from happening again – or at least alleviate the threat. One of the compelling debates in the GRC world is whether companies could have avoided their recent troubles by having a true ERM program in place.

But we've been down this road before. I thought it would be interesting to review what has transpired in the financial services industry over the past few decades, how ERM as we know it today came into existence in the US and to discuss where it is heading.

### **Then: COSO and SOX**

Financial services, and more specifically the banking industry, have employed risk management programs for a long time. However, prior to the 1980s there was very little identification of risks as we know them today. The word "risks" was used in the banking industry but these were managed more as "business activities" than as the actual risks we currently identify. The savings and loan crisis of the 1980s and 1990s changed everything. By looking at a brief history of this episode we can better understand where ERM has its roots in banking and its evolution to the format we recognize today.



## COMMENTARY

The US savings and loan crisis of the 1980s saw the failure of almost 25% of the savings and loan associations. While several pieces of legislation were passed during that time to better regulate the industry<sup>1</sup>, the Treadway Commission had the most resounding effect on ERM.

The Treadway Commission was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting. The Commission studied the financial information reporting system for two years and issued the *Report of the National Commission on Fraudulent Financial Reporting* in 1987. As a result of this report, the Committee of Sponsoring Organizations (COSO) was formed. In 1992, COSO released the *Internal Control-Integrated Framework* report which became the foundation for ERM as we know it.

From 1992 to 2002, financial institutions relied mainly on COSO to implement their internal controls and frameworks. The first Basel Accord passed in 1988, focused mainly on credit risk and capital reserves. It was adopted by the G-10 countries in 1992, coinciding with the COSO report. This marked the beginning of the accepted process of having a specific business risk mitigated by internal controls as opposed to risk being identified as a “business activity”. In 2002, Congress passed the Sarbanes-Oxley Act (SOX) in response to the major fraudulent scandals involving Enron, WorldCom, TYCO International, and Adelphia. SOX can be most easily broken down into the two sections that had the largest impact on accelerated filers over \$75 million in market cap: Sections 302 and 404.

Section 302 mandates that signing officers certify they are “responsible for establishing and maintaining internal controls” and that the internal controls have been designed to make sure “material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities”. The officers also have to evaluate these internal controls within a 90-day period prior to the report. Section 404 mandates that management and the external auditor report on the “Internal Control over Financial Reporting” (ICFR). Management is required to produce an “Internal Control Report” which confirms that an appropriate internal control structure is in place with proper procedures for financial reporting. The report must also include an assessment as to the effectiveness of the controls.



## COMMENTARY

SOX also created the Public Company Accounting Oversight Board (PCAOB) and handed down guidance about how to accomplish these tasks in 2004: Auditing Standard 2 (AS/2) and again in 2007: Auditing Standard 5 (AS/5). AS/2 was more of a bottom-up approach while AS/5 is a top-down, risk-based approach. The combination of the COSO framework and AS/5 created the most commonly used framework for SOX and, on a broader scale, ERM in the US today.

### **Now: Dodd-Frank and the risk committee**

In response to the financial crisis of the late 2000s, July 2010 saw the US Government pass the Dodd-Frank Act. Dodd-Frank is yet another regulatory effort to avoid future problems, with one crucial difference: it was the first legislation to include a provision for a “risk committee”.

Under Dodd-Frank, all public non-bank financial companies supervised by the Federal Reserve and public bank holding companies with assets of \$10 billion or more must establish a risk committee. The risk committee must also include one “risk management expert”, intended to mitigate the potential for another financial crisis by improving ERM practices across the industry. The change also attempts to balance executive compensation with the amount of risk-taking at the institution. Risk managers should report to the risk committee chairperson, addressing concern that a career may be in jeopardy for having an independent voice about risk-taking.

### **What does this mean?**

What about institutions outside these parameters: should you start to implement an ERM program? From what I have seen and heard over the past year, I believe the answer is: “Absolutely.” I hear regulators are asking for “an appropriate risk management process given the risk profile for your organisation”. It’s not hard to read between the lines; what I actually understand is: “Implement an appropriate risk management process (like ERM) before we need to pass more legislation under Dodd-Frank to force the issue.”



## COMMENTARY

Presently I think the industry agrees with me as financial institutions large and small are trying to pull their various risk assessments together to form what we now call ERM. We have evolved from “business activities” being considered a risk to monitoring enterprise risk on a company-wide basis in another attempt not to repeat the mistakes of the past. Risk management has also evolved from being strictly financial in nature to being more holistic. Instead of just having categories such as ‘credit risk’ and ‘fraud risk’, companies are trying to moderate areas like ‘reputational risk’. ISO 31000, introduced in 2009, was developed to provide best practices and guidance for all companies implementing risk management and is now widely being adopted in conjunction with COSO.

### **The future**

I believe the adoption of ERM in the financial services industry will be akin to the implementation of Internal Controls over Financial Reporting (SOX) for publicly held companies but voluntary. Over the next two to three years, regulators will make sure that the industry is sound and that we do not fall into the next financial crisis. As with SOX, larger companies will initially be scrutinized but, unlike the repeal of auditor attestation for non-accelerated filers under Dodd-Frank, smaller financial institutions will have to have in place “an appropriate risk management process given the risk profile for your organisation”. Given the history of the industry outlined above, the easiest and most generally accepted way for an institution to comply will be an ERM program using the COSO framework or ISO 31000.

As for the answer to whether having an ERM program in place would have shielded us from the recent financial crisis, I believe the debate will continue until we see how the current ERM programs respond to the next one. If we never see another catastrophe, the point is moot.

### **Not just financial services**

But what about companies in industries outside financial services? What types of company should be implementing ERM now? There have been rumours that rating agencies such as Standard & Poor’s will start to include – and even require – an institution to have an ERM program as part of their analysis for credit worthiness. At the moment, this is nothing more



## COMMENTARY

than speculation but I am seeing an influx of enquiries in several other industries, including the retail, energy, higher education and government sectors.

ERM benefits any institution and every company performs some form of risk management on a daily basis. It comes down to the risk appetite of management and how severe the impact will be on the company given the probability the risk will occur. At the very least, in a larger organization, I should be able to identify and categorize my top 10 enterprise risks. If the impact of a majority of those risks is “catastrophic” and the probability of them occurring is “highly likely”, I not only want to know this, I must also take steps to avoid them or soften the blow. In short, I need an ERM program and, the chances are, so do you.

David Zach is Methodware’s Director of Sales, North America, based in Pennsylvania. For more information, David can be contacted at [david.zach@methodware.com](mailto:david.zach@methodware.com) or by calling +1 484 924 9911.

---

<sup>i</sup> The Foreign Corrupt Practices Act of 1977 (FCPA), the Depository Institutions Deregulation and Monetary Control Act (DIDMCA) of 1980, the Economic Recovery Tax Act of 1981 (ERTA), the Garn-St Germain Depository Institutions Act of 1982, the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) and the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) to name a few.