NORGES INTERNE REVISORERS FORENING

INTERNREVISOREN

Nr. 1 • SOMMER 2006 • 14. årgang

HELHETLIG RISIKOSTYRING

Professor Larry Rittenberg, COSO styreformann på talerstolen i Bergen

Uken Bergen var COSO-hovedstaden

- Risikostyring stat
- Risikostyring finans
- Risikostyring og IT
- Riksrevisjonen

INTERNREVISJONSkonferanse

BERGEN
21. – 23. mai
2006
HOTEL NORGE

Week 21, 2006: COSO Headquartered in Norway

Dr. Larry Rittenberg, Chair of COSO talks to Frank Alvern, CSO of IIA Norway

For a good week in May 2006, the COSO Headquarters was located in Norway. Dr. Larry Rittenberg, Ernst & Young Professor of Accounting, University of Wisconsin headlined IIA Norway's annual conference which was arranged in Bergen for the first time. Internrevisoren jumped at the opportunity to talk with the 2005 recipient of our profession's most prestigious award - the IIA's Bradford Cadmus Memorial Award, as a historic visit came to close.

Thank you for taking the time to talk to us towards the end of your stay in Norway. First of all, all of us who met you in Bergen want an update on your trip to the Northwest where your wife Kathleen's family originated from. How did that go?

It was wonderful and another testament to the greatness of the IIA family that truly believes in sharing. Thanks to the help of Frank Alvern and Per Olav Nilsen, we were able to identify my wife's grandparent's home towns (a few houses, not really a town). We stayed with a wonderful couple that Per had identified; we met many of Kathleen's cousins. More importantly, we were able to see where her grandfather lived, and even more exciting, we had coffee and cakes with a second cousin who lives in the house her grandmother lived in prior to coming to America. What a dream – to sit in the same house; to walk in the footsteps of her grandparents; and to see the wonderful land of Norway. It was one of the highlights of our lives. On top of that, one of her cousins invited us to have dinner on his boat as we cruised the fjord. It was just wonderful.

You have been a member of the COSO board for several years, but assumed the position of the Chairman in January of last year. How would you describe these 17 months?

IIA Norway's Annual Internal Audit Conference

- The current model of 2 1/2 days (Sunday – Tuesday) was introduced in 1992.
- Number of participants at the first conference was 50, and it has slowly risen to last year's attendance of 139.
- The final number for the 2006 conference was 278 participants.
- In comparison, IIA Norway's membership has grown from 232 to 650 in the same period.
- 40 % were women, 60 % men
- Excluding guests and exhibitors, representatives from more than 80 different organisations were present in Bergen.
- Almost without exception, IIA Norway has been able to headline one key IIA / ECIIA representative in all these years. The list of representatives includes chairmen, presidents and board members.
- The 2006 conference brought together two Bradford Cadmus Memorial Award winners. The 2005 recipient, Dr Larry Rittenberg met up with the 1998 recipient Knut Løken. Knut Løken, who is now retired, followed in the footsteps of Odd Hunsbedt who became the first Norwegian to win this prestigious award.
- The Bergen conference also had two Leon R. Radde Award winners addressing the record number of participants. Dr. Rittenberg, who won the award in 1998 was followed by the 2002 recipient Dr. Flemming Ruud on the podium. It should be no surprise that both these IIA Educators of Year received very high evaluations.

COSO

- Established in 1985 as The Committee of Sponsoring Organizations of the Treadway Commission
- COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.
- The following five organisations makes up COSO: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants).
- Dr. Larry E. Rittenberg is the current chairman, and President Dave A. Richards is IIA's representative on the Board.
- Published the landmark I*nternal Control – Integrated Framework* in 1992. Known as COSO 1, the concepts in this framework have been incorporated into legislation in numerous countries around the world.
- In September 2004, COSO released *Enterprise Risk Management – Integrated Framework* as a principles-based framework for managements and boards to comprehensively manage risks to objectives.
- COSO is scheduled to release a new document called *Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting* in July 2006. The objective is to provide guidance related to Section 404 efforts of the Sarbanes-Oxley Act.

The last 17 months have been very hectic and, sometimes frustrating, as it has taken longer to develop small business guidance than I had expected. COSO has developed excellent frameworks on internal control and enterprise risk management. However, with the advent of Sarbanes-Oxley in the US; coupled with cost concerns, there has been a great deal of pressure for more guidance in implementing the framework in a cost-effective manner. We were able to identify fundamental principles on which the COSO Internal Control, Integrated Framework was developed. We have articulated those principles, as well as provided examples of how to accomplish those principles.
I personally think that this upcoming guidance, although intended for smaller businesses, brings the COSO framework into sharper focus and will help all companies. We hope you will take a look at it. We plan to have it on our website around July 15 of this year.

One thing we emphasize in the new guidance is that the COSO framework must focus on accomplishing objectives; particularly the objective of achieving reliable financial reporting.
The 5 components all contribute to accomplishing that objective. However, the choice of controls to be implemented to accomplish the objective is a management decision based on characteristics such as efficiency, cost effectiveness, and relevance to the risk addressed. There is not one unique answer that applies to all companies; rather each company must make choices.

As you know, IIA Norway was instrumental in translating the first COSO framework on Internal Controls into Norwegian some 10 years ago. The framework has influenced our way of looking at the whole concept of internal control here, and has worked itself into the methodology employed by internal auditors, controllers / line management and regulators alike. But looking from the outside, it seems like it took the major corporate scandals and the Sarbanes-Oxley Act to make the US aware of the framework. Why do you think that is?

I think most companies in the US were using the COSO framework, but had not paid as much attention to internal controls as we would have liked. Controls were generally pretty good over transactions, but there was a problem at the higher level of the organization dealing with adjustments, contract modifications, closing entries, off-balance sheet transactions, and so forth.

I find it interesting that most of the recommendations that COSO made in the Treadway Commission in 1987 regarding financial reporting pretty much parallel the legislation enacted in the Sarbanes-Oxley Act of 2002. We had a situation where management domination and management compensation simply got out of hand in the US. Further, there was a problem of what was acceptable behaviour, i.e. if it is perceived by most CFO's that pushing accounting principles (or rules) to accomplish earnings reporting objectives is acceptable, then more companies engage in financial engineering.

Most of the big control failures were at the top of the organization. It was fundamentally a problem with the ethical climate and lack of independent oversight by the Board. They had to be reminded to do their job. But, it also meant that we were not very good in recognizing the risks to reliable financial reporting posed by dysfunctional compensation schemes and how those risks needed to be controlled. In my speeches, I often say that if you do not understand an organization's compensation schemes and the risks that they portend, you have not fully implemented the COSO Framework.

With the most frantic SOX work behind them, do you think that US corporations are open to expanding their focus from internal controls over the financial reporting process to an enterprise-wide risk management focus? And what is the strategy from COSO to encourage such a transition?

I hope the answer is yes, but that answer is probably a bit premature. Not all the hectic work is behind the companies. In my view, organizations need to switch from a compliance focus on controls to one where they view Sarbanes-Oxley as an opportunity to reengineer and really improve their processes. When they do that, they will realize real substantive cost and efficiency benefits.

Europe does seem to be ahead of the US in applying the ERM framework. In my opinion, it is a very robust framework because the objectives are broader and the components focus on accomplishment of the organization's objectives. However, one problem that many companies have is determining where to start, and how to integrate or develop a comprehensive ERM. From our point of view, it is most important to simply get started. We do think that internal auditors are often a key in leading the way within many organizations.

In the end, we feel that ERM works best when it becomes ingrained in the culture of the organization. As I noted in my talk at the Bergen conference, I believe it is very important that organizations understand that they need to take risk. There are too many instances of very successful companies that focus on improving a great product; but fail to innovate. That is a huge risk and often leads to the demise of a great company. ERM does not discourage taking risk; rather it encourages organizations to understand the need to take risk; to understand the risk; and to manage those risks within the risk appetite set by the board and implemented by management.

As for strategy, we will continue to promote the ERM framework as a common language and approach to help organizations accomplish their objectives. Too often, there is a tendency to view control and risk management as overhead. We have seen many conferences that demonstrate quite the opposite; control and risk management lead to more effective organizations and greater success. We will participate where we can to promote this understanding. In the future, I would like to see us sponsor more research on successful implementations of ERM.

We see from the www.coso.org that the list of the ERM Executive Summary in different languages is constantly expanding. I think that there are about 10 different language versions out now. Who is translating into these languages – is it again the internal auditing profession or are other bodies involved? How pleased is COSO with the reception of the ERM model, in the US as well as internationally?

We are finding that the lead is most often taken by the internal audit community. I stopped by Stockholm after the Bergen Conference and met with some of the leaders of IIA-Sweden. We just approved a Swedish translation which will be led by the IIA-Sweden. We had a similar effort by IIA-Italy and I was fortunate enough to have the time to join them in their conference celebrating the translation.

Why is the leadership coming primarily from the IIA? I think it is closely related to the very definition of internal audit developed by the IIA that defines internal auditing's objective to improve the governance, risk management, and control practices of organizations. I am finding that individual IIA members are taking that responsibility seriously and are very much the leaders in integrating these three concepts across the organization.

Personally, I like this leadership as I have been active in the IIA throughout my career. I do see a potential risk to the internal auditors in the US that they may see themselves more defined by Sarbanes-Oxley. If that should happen, I think the value proposition for internal auditing decreases. Thus, I encourage you to continue to provide leadership in integrating the three objectives of governance, risk, and control across your organizations.

In Norway, we see that our translation of the COSO ERM framework finds itself into the required readings of our business schools. How has the reception been at US colleges and universities?

In all honesty, I have to say it is not as good. I personally use it in my graduate class and it is very well received. I supplement the reading with a "hands-on" experiential learning exercise. The last one we did included a complete risk analysis for JC Penney, in cooperation with their CAE. It worked great.

There are pockets where risk management is taught as a separate course with a great deal of case studies. The demand for students with that kind of training is high. The demand will drive more courses in the area. As an example, Miami University in Ohio has just developed an Enterprise Risk Management Center that will be funded for upwards of $5 million to teach and research in risk management. One of our COSO Board members, Mark Beasley has developed a similar center at North Carolina State University. It has been met with great success –both for students and for interaction with practice. They have monthly breakfast meetings with companies to share their experiences with ERM. They have great attendance. More will follow.

In your second presentation in Bergen you mentioned that the new COSO initiative to provide guidance for smaller businesses on using COSO for PCAOB Standard 2 compliance will be published this summer after the period for commenting on the draft has now ended. This particular guidance is still an unknown quantity in Norway, but in your opinion it contains material that is of value well outside of US companies needing to comply with current requirements?

PCAOB

- Public Company Accounting Oversight Board (PCAOB) was created by the Sarbanes-Oxley Act of 2002.
- The mission is to oversee the auditors of private companies protecting the interests of investors and furthering the public interest in the preparation of informative, fair, and independence of audit reports.
- All accounting firms must be registrered with PCAOB to prepare or issue audit reports on U.S. public companies and participating in such audits.
- Have published four auditing standards to date. No 2 – *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, which was published on 9 March, 2004 included a specific reference to / recommendation of COSO's Internal Control Framework and made COSO a household name in the U.S.
- More information can be obtained at www.pcaobus.org

Yes, I think the new guidance will have significant value outside of smaller businesses and outside of the US. I would be very happy if the IIA-Norway also took the lead in translating the guidance. I believe the primary value in the new guidance is the specific articulation of fundamental principles underlying the 1992 framework. We identify principles, attributes of those principles, and provide examples of how smaller businesses might implement policies, procedures, or other actions to accomplish those principles.

We also do a couple of other things:

1. we emphasize the importance of the "monitoring" component of the COSO framework and make the case that most companies need to seriously look at the monitoring component as one approach to achieve greater efficiency in their control processes.
2. we focus on "achieving the objective" of reliable financial reporting. Sometimes the objective gets lost in assessing whether all of the components are present and working. However, the end judgment has to be whether the components, as they all work together, achieve the objective.
3. we emphasize that management judgment is needed in determining the optimal set of control and governance policies for each organization. While we do provide a questionnaire, the answer is not in "checking the boxes", but in determining how everything comes together to achieve objectives.

You responded to questions from the audience about COSO's relationship with or maybe lack thereof, other international standard setting bodies and agencies. ISO and the Basel Committee were forwarded, and you mentioned a few others in you response. Could you share your thoughts with our readers on this important aspect of harmonizing global (ERM) guidance?

Yes, I believe it is very important. There is not a great deal of differences between many of the frameworks. Some are more detailed; others less detailed. Some believe the objectives ought only to be set by management, e.g. Turnbull, while others, including COSO, recognize that there may be external influences on the definition of objectives (most notably the criteria for effective internal control over financial reporting). However, they essentially embody the same concepts.

The real value of harmonizing frameworks is that we move to a common language and a common understanding of framework components. We are truly a global economy. We need to move to a common framework to help our organizations consistently implement risk management, control, and governance. The work done by the Basel Committee is very consistent with COSO. They combine their principles with more guidance.

Professor Rittenberg (left) with Frank Alvern in Bergen.

If we have a common framework, we can move forward in providing greater common guidance.

I would like to see COSO take a lead in working towards this harmonization. I also think that we should become more inclusive and international in our membership, i.e. we should have a risk management organization as part of COSO; we should have international membership; and we should be broader than just the accounting profession. One of the things I like about the ISO organization is that they have standing working groups that can be called upon to provide guidance related to the broader standards. As an example, I would like to see a working group composed of members of ISACA, the IIA, the AICPA, a security organization, and so forth, work together to provide one set of guidance to deal with Information Technology control and security issues. A multiplicity of frameworks does not necessarily improve market acceptance or implementation. We need to get over the "not invented here" syndrome and find ways to work together.

Thanks again for taking the time to talk with us. We now have a face to go along with the acronym, and that is an inspiration to us going forward with COSO in Norway! Any last thoughts or ideas you would like to share?

Thank you for inviting me to participate in your conference. I really saw the "Progress Through Sharing" theme present at the conference. I also sensed a strong commitment to professionalism within the IIA members at the conference. You have a beautifully country; but more importantly as I stated in response to your first question; you have friendly people who care about each other. Your people and your leadership will build a stronger internal audit profession in Norway and the Nordic Region. I would be happy to work with the IIA-Norway in the future.