# RECORD, Volume 29, No. 3*

October Annual Meeting
October 26–29, 2003


## Session 89OF
## Risk Management Framework in a Life Insurance Company

**Track:** Financial Reporting


**Moderator:** MAX J. RUDOLPH
**Panelists:** MAX J. RUDOLPH
ELLEN COOPER
JAMES P. GREATON



*Summary: This session introduces attendees to the growing area of enterprise risk management (ERM). It provides an overview of an ERM framework as well as issues and challenges of implementation. Regulatory and rating agency reactions are discussed in depth. Attendees will have an enhanced understanding of what is meant by ERM in concept and application, various undertakings within the United States and Canada, issues and challenges to implementation, and regulatory and rating agency reactions.*


**MR. MAX RUDOLPH:** Welcome to Session 89. I'm going to introduce our three speakers and then we'll get right into the program.

I'm a vice president and actuary with Mutual of Omaha. I graduated from Michigan Technological University. My focus is primarily on asset/liability management (ALM) and other balance sheet risks, such as liquidity and capital. I am a past Investment Section chair and one of the founding members of the Risk Management Task Force. Ellen Cooper, a graduate of Temple, is a senior manager with Ernst & Young in Philadelphia, focusing exclusively in the risk and value optimization consulting area. Her expertise includes corporate risk and corporate investment reviews, stochastic modeling, variable annuity analysis and stochastic generators. Jim Greaton is a graduate of Purdue. He is currently Vice President, Annuities Actuarial

at Sun Life. Prior to that he was Vice President, Risk Management in charge of Sun Life's Risk Management function for its U.S. Operations. He has served on the Academy's Committee on Life Insurance Financial Reporting (CLIFR). He was also a member of the Society's Financial Reporting Section Council and served on the Academy's Equity-Indexed Annuities (EIA) Task Force.

I will focus on the basics on enterprise risk management to set the stage for our other speakers. A lot of what I'm talking about today is based on a book that came out in summer 2003 called "Enterprise Risk Management: From Incentives to Controls." James Lam is the author. I recommend it. James is one of the board members for the Professional Risk Managers' International Association (PRMIA), so he's very involved in risk management. James has spoken at previous SOA seminars.

Not everything that I'm going to say is from Dr. Lam's book, because he's focusing on how to do enterprise risk management across a wide variety of industries. There are a few things that I've tried to expand on, so if you don't agree with something, it's likely something that I have added.

What is risk management? It's an integrated approach to managing a portfolio of risks, as opposed to a silo approach. It's a framework. It's a process. It's a tool. It's not an end-all.

While risk mitigation is important, it's only part of the story. Enterprise risk management can be used to optimize returns relative to risk for your product line or your personal financial situation. It helps you get to the efficient frontier. We should be using enterprise risk management as a profit center, to suggest solutions where we can take more risk, make the company more profitable and increase shareholder value. How can we do things better? We must be aware of the appropriate risks to measure and manage. Enterprise risk management is driven by the control cycle. You look at where you are, formulate a plan to make it better and then monitor the results. You iteratively make it better. It's not going to be a one-time fix.

You should not always control or reduce risk. Sometimes it makes more sense to increase risk. If you are ahead of the curve on enterprise risk management, you will have a competitive advantage in the industry. The key is culture. You need a common language. You need people talking a common language across different business units, including the investment department. You need a champion who walks the walk. If the champion says, "Yes, we need to do enterprise risk management. But, of course, it doesn't apply to me; it only applies to people below me," that's not going to work. Employees pick up on those actions. A lot of it is common sense. The models are important, but you still need to make sure that they make sense. If an arbitrage-free scenario tells you that the value of a bond that's going to mature in two days at $1,000 is only worth 2 cents, you should challenge the model.

The alternative to thinking ahead about risk management is crisis management. You can either wait for the problem to arrive, or you can try to anticipate what the problem is going to be. Analysis using risk silos is a start, but you need to go beyond that and look at the interrelationships and correlations between different risks.

What are the practical reasons for ERM? It's a big part of management's job. If management doesn't think they're responsible for managing the risks of their business, perhaps saying that's the actuary's job, there's a problem. Many consultants suggest pursuing enterprise risk management because it can reduce earnings volatility. I'm a firm believer that that's only part of the picture. We get paid, as insurers, to take volatility from individuals. When somebody buys a life insurance policy from us, that person is reducing his or her volatility and increasing ours. With the law of large numbers this works out for us. Bottom line, our job is to buy volatility and get paid for it.

Theoretically, an academic might tell you that an investor can diversify. They would say that management's job is not to manage all their risks, or to limit some of those risks, because an individual can always invest in something that has a negative correlation to that company. That's true to a point. But you have a lot of other stakeholders besides the investor. You have all your employees. You have your policyholders. It's management's job to manage all of a company's risks.

I remember a consultant coming through a couple of years ago and showing us how great it was going to be if we could reduce earnings volatility by doing something that they were suggesting. The consultant never mentioned the offsetting cost. You don't want earnings management. That was really what they were selling at the time, and a lot of companies have gotten in trouble since the public realized that's what they were doing. Hedging is good, but reserve manipulation is bad. At GE, as noted in the Jack Welch books, they could reduce a 15 percent return that exceeded guidance to 12 percent by increasing their research budget. I don't think that's good. You lose transparency.

Efforts to maximize shareholder value are driven by culture. If you can build risk management concepts into your culture, opportunities will be easier to see. People are going to be more aware of opportunities. Someone may read in the paper that there's a company that looks undervalued. Maybe they should look at it. Maybe it goes through and you end up doing a deal that provides an internal hedge. It provides a disciplined approach and consistency. That's a good thing. It forces you to look at risk-adjusted returns. It builds skills internally. If I have a lot of skills in the corporate area for managing risk, but I don't have any in the product lines, the company is not better off. We need to have a culture that is aware of risk, where we are doing the cost-benefit analysis to make sure that we get paid for the risks that we're taking.

Let's talk about job and financial security. Senior managers who practice risk management are less susceptible to external volatility for interest rates or for a big spike in mortality. Senior managers generally have stock options and invest in their own companies. If their company goes under, those stock options aren't worth much. So there is a benefit to risk management for senior managers as well. It's in their best interest. Hopefully, they'll recognize that and do it.

There have been several recent risk management issues for actuaries. I'm sure I am not telling you anything you don't already know. It's important for us not to do single-scenario, expected value pricing where, if I look 20 years out, it looks great, but I went bankrupt in the fifth year. If I'm in great health 20 years from now, but I died five years out, who cares? I'm still dead. It just doesn't work. The guaranteed minimum death benefit (GMDB) product feature is covered by other sessions at this conference. You need to keep track of what's going on, if you're a U.S. actuary, with the American Academy of Actuaries' RBC C-3 Phase II project. It's expected to move forward soon. Then it will be up to us, the people in this room, to implement it. There will be a lot going on next year with that.

When we first started writing long-term care, who knew that product was lapse supported? Hopefully, nobody who was pricing it. There are also bank annuity-type products, primarily deferred annuities, where we've given out options but haven't charged the right price for them. One of my mantras is "Never assume the policyholder is stupid." Even if they act that way today, they may not act that way tomorrow. We're seeing some experience in our deferred annuity block right now where it's in their best interest to stay due to the low interest rate environment. We had a floor in our lapse curve, and we're going to take it off. It's no longer appropriate. They figured it out. The same thing happened with mortgage-backed securities. I occasionally give talks to our financial staff, like the accountants and investment folks. I'll ask who has refinanced their home mortgage in the last couple of years? As the ALM guy at an insurance company, I hate those people— almost everyone with a home mortgage. That's the risk. Think about how easy it is to get the information that it is in our best interest to refinance. It's in USA Today. It's even on the front page of the local weekly paper of villages with 5,000 people. It's everywhere.

I want to focus on what James Lam was talking about. He discusses seven basics of enterprise risk management for senior managers. I think he did a pretty good job of coming up with them.

1. You want to know the business that you're in.

2. Make sure there are checks and balances.

3. You want limits and boundaries—when should you stop writing variable annuity business with GMDB dollar for dollar?

4. Keep your eye on the cash. (Lam included this quote, "Cash is king. Accounting is opinion." I love it.)

5. ERM provides a yardstick. As we view it more and get better at it, we'll understand which pieces of risk management are leading indicators and which ones are lagging indicators.

6. We want to incent the desired performance; we must put incentives in place that encourage people to make the right decisions. I know, as actuaries, we struggle with that a lot. One of the things I liked best about this book is that, although I didn't learn a lot by reading it, it gave me lots of quotes that I could go and say, "See, it's not just me. Here, look at this guy. He wrote a book, they published it and it's saying the same thing." That's very powerful with some senior managers. They don't want to hear it from their actuary, but they will listen if somebody has been published.

7. Finally, there is the distinction between hard and soft risk management. Soft risk management includes enablers. What types of things enable you to do risk management? They are things like infrastructure, independent risk functions, oversight committees, audits and risk assessments, procedures and policies, systems and models, with reports ready to go on a regular basis. My staff doesn't like it when I say this, but we need to get to the point where we can push a button to produce our reports. Push a button and it will give us the output overnight. Then we can spend our time analyzing it. There are some companies that are at that point. It's very impressive. They're able to spend their time on the analysis. If we can spend our time on the analysis instead of on the data collection, think what we could accomplish. It improves our timeliness. It improves our effectiveness. Enablers also allow you to limit the exception process. Say we're only going to sell life policies up to age 80, except for friends of the chairman. You can't allow that and have it work.

Then you have your drivers, the hard form of risk management. You need a champion, and it needs to be somebody at the senior level. You need that person to recruit other champions. You need champions throughout the company. You need the commitment, because that is what's going to drive enterprise risk management. Culture and values are important. Common sense is core. Design incentives so that it drives that same common sense process.

You want to facilitate open communication. One question that I hear a lot in the industry is, to whom does the chief risk officer (CRO) report? The chief risk officer might report to the chief financial officer or the chief operating officer. The CRO really needs to report to the board, or report to the CEO and have direct access to the board. If you see something bad happening, you need to be able, with impunity, to go to the board and tell them that there are concerns. One of the drivers, and I know I am preaching to the choir, is learning. Be open to continuing education. The ERM field is changing quickly. Emerging issues include fair value

reporting, C-3 Phase II, stochastic morbidity and stochastic mortality. Five years from now, today's skill sets won't be good enough, even for the people who are here. We have to continue to learn, including the people who are experts today. We'll have to continue to expand. Again, we want to reinforce it all with incentives.

This is a quote from the Lam book that summarizes the benefits of risk management. "Companies that understand the risk/return economics of the business can take more of the profitable risks that make sense for the company and less of the ones that don't." The part I add, "…and know which are which," is important too.

What would I suggest that you take away from this? If you consider yourself a risk professional, put together a list of what keeps you up at night. It's interesting that the rating agencies have picked up on that. I always get to go last, not surprisingly. I discuss ALM-type issues. Often they're late for a flight, they've been running long and they need me to go very quickly. So they'll stop and say, "We don't have time to go through your talk, but what keeps you up at night?" If you have a "top 10" list, a risk scorecard or something that talks about emerging issues, things that you're reading about in the industry and affects your company, that's all very useful. There's a lot of value to that.

Don't wait for modeling perfection. That's always been the case, going back to before cash flow testing came around. You can work on your models trying to recreate your day-by-day cash flows, but you're never going to get there. Do the best you can today, and then figure out ways to iteratively improve as you go along, whether it's next quarter, next year or whenever. There's always room for improvement.

**MS. ELLEN COOPER:** I'm going to talk about risk management in the context of the life insurer. You'll see that some of the themes I'll be discussing are going to overlap with some of the ideas presented by Max and Jim. When we think about attempting to solve the problem of measuring and managing risk, many of the processes and conceptual ideas about it are really quite similar. It's in some of the details where we get bogged down.

The first thing that we need is a mission statement. What are we trying to achieve when we talk about risk management? What are our goals? By a show of hands, how many of you within your organizations have some kind of an enterprise risk management framework or process on a regular basis? Good. I'd say that's probably about half of you. For those of you that do, and also for those of you striving to have some kind of a framework, I recommend thinking about what the goal is. What is our mission? What is it that we want to achieve? While you're defining the mission, you want to think about having consistency across the organization. What is my preferred measure of risk, and is it consistent with the people in the U.K.? Is it consistent between the life and annuity lines?

I want to make sure to aggregate my exposures across lines consistently, so that I can appropriately assess my diversification and concentration. Finally, I want to be able to define my global risk tolerance framework across the organization. I need a consistent definition, so that when I look across the organization globally and enterprise-wide, or by line of business, it's in a consistent framework.

When deciding on my mission, I also need to decide what kinds of information senior management and my unit need from me. What will it enable them to do? If I just print some glossy report on a quarterly basis, give it to somebody and nothing ever happens with it, then it's not adding much value. In this particular framework, we have the ability to add a lot of value if we're able to provide the right information, if it's explainable and accessible.

In addition to having a mission and understanding what our long-term objectives are, we need to know our definition of risk. As an organization, we need to be consistent about what risk is. Is risk looking at tail scenarios? Is it the 1 percent probability of going insolvent? Or is it the 10 percent chance of negative internal rate of return (IRR) under a new product? Is it what happens if my earnings are floating around too much? Or is it something else? Understand as an organization what its risk definition is. I can't manage it if I don't know what it is.

I have to look at all the different risks that we need to be managing in our enterprise. This includes all types of insurance risk, credit risk, investment risk, business risk and operational risk. We need to do it all simultaneously.

Once I've defined my mission and my risk definition, and I've identified what all my risks are across my organization, simultaneously, I also need to define what my organizational structure is going to be. We need to have clear roles. Max talked about that. We need to have good people. We need to have strong leadership. We need to understand our decision process regarding taking new risks. How are we going to examine risk issues? What is the process? How is our analysis going to drive management actions?

We need somebody to be the champion, as Max said. We need a CRO, a head of ALM—somebody who can be the overall enterprise risk management leader. By a show of hands, how many in your organizations today have somebody who is either performing the role of CRO or some kind of ALM leadership position? About a third of you. That is consistent with other analysis that we've seen.

I'm going to walk through an organizational structure. It's intended to be one example. It's an example of how you can put things together. The CRO should be responsible for leadership, and then should be able to delegate execution to the operating divisions. Somebody should be in charge of designing investment strategy and product pricing, and for execution of modeling, measuring and monitoring the risks.

In this organizational structure, we have included a board of directors. They give the responsibility of day-to-day risk management to senior management. We've seen examples in organizations where they have a senior executive committee focused on risk management. They appoint a CRO, or some champion, who is head of the organization. They also make sure that the risk management infrastructure is in place. It's the CRO's job to make sure that the process is in place. I'll talk later about how that means having a written policy on risk management, understanding how to set controls and how to have appropriate tools and processes around them.

The CRO needs to make sure that there is a consistent framework across the organization, including measures and assumptions. The CRO needs to understand where models are different, why, and where it's material. They need to know how to aggregate. If I have a PTS model in one part of my organization, a MoSes model somewhere else and an old Excel spreadsheet that somebody wrote 14 years ago somewhere else, I have to figure out how to aggregate all that and understand where the differences and inconsistencies are. If I'm doing stochastic modeling, I have to make sure that the generation of economic scenarios is consistent or, if it's not, I need to understand what the differences are. Are my interest rates parlayed with equity risk? The CRO is responsible for setting those policies in place upfront.

The CRO is also responsible for assessing risk exposure relative to risk tolerances, monitoring them on a regular basis and then developing a routine process to evaluate and control.

As I said before, the operating divisions are then responsible for the execution. They make sure that the real work is actually happening on a day-to-day basis, and happening efficiently.

We talked about defining risks and we talked about looking at all our various types of risk. We also need to create an inventory of the risks. We need to make sure that we have included everything. One way to do this is to qualitatively rank the risks. Categorize them and prioritize them, one through 10 or one through five. What are the most important risks? What are the things that keep me up at night? What are the things that I worry about most and that I need to manage most carefully?

Then I have to figure out which ones are easy to quantify. We have solved how we can quantify interest rate and equity risk, but others are more difficult, like terrorism, operational risk, credit risk for longer than a one-year time horizon, and trends in mortality. I can put those off on the side and deal with them as more difficult, long-term situations. In the meantime, I can make sure that, for those that I can solve, I begin now. Using my prioritization, I start to fix the problems that are high on my list, monitoring and measuring them now.

So far, I have identified my risks and decided which ones I'm going to quantify now, later, or never. Now I need to understand what I want to do with the risk. Do I want to take it and actively manage it? Do I not want to take it, and by not taking

it, do I want to make an active choice not to take it? I might want to make an active choice, for example, to avoid any living benefits on my books or not to sell GMDBs anymore. Or do I want to take it and transfer the risk? Do I want to have some kind of a hedging strategy, some kind of reinsurance or other mitigation strategy?

Then finally, there has to be some kind of process to re-evaluate the initial decisions on a periodic basis. Do they still hold? Do I still want to hedge? Is it too expensive for me to hedge? Do I want to get out of the business? Do I want to accept the risks?

As we said before, the CRO is responsible for a written policy and developing standardized reports. It's very important to make sure that the information being communicated is understandable and readable to management. Investment guidelines and strategy could be done by a CRO or by the chief investment officer, depending on the organizational structure. The CRO would also be responsible for processes around controls.

In terms of measurement, I need to make sure that I have good models. Again, the CRO is responsible for making sure that models are consistent across the organization and to be aware of any differences. I'm going to perform risk measurement, and I'm going to do it over multiple time horizons. I'm going to look at things like interest rate, equity, credit, foreign currency (if I have it), mortality, morbidity, and policyholder behavior. I'll make sure to do appropriate stress tests, sensitivity tests, and back tests so that I really understand the risks.

I also need to decide what kind of metrics I want to use in my risk measurement. Is this going to be an embedded value (EV) framework? Embedded value-at-risk (EvaR)? Risk-adjusted return on capital (RAROC)? I'm going to make sure that I report on a regular basis and that I review my exposures and tolerances on a regular basis.

I want to make sure that I have appropriate controls. This is not intended to be a plug for consultants, but there should be an independent review of our models. There should be some other person outside of the regular day-to-day function, whether it's somebody else in the organization or an external consultant, who reviews the models, critiques the process from time to time and gives insight into places where there is room for improvement. There will always be room for improvement. I need to make sure that my models are validated. If I have something in my model that doesn't make sense, obviously I want to make sure that I fix it before I start doing all my risk analysis.

Finally, I want to make sure that my policies and guidelines are clear and that people can understand them. Somebody other than the person who has written them is going to read and interpret them. If they're not extremely clear, they could be misunderstood or gamed. I want to make sure to have exposure targets around

asset classes, credit quality, duration and convexity mismatch, and so forth. This way, when I'm measuring my exposures and tolerances, I know when I'm out of balance and need to take some kind of action.

I want to make sure that reporting is timely, automated and accurate. I can develop routine reports that are not ad hoc. It's enough that we have these big complicated models that can take 24 days to run. Once I'm done with that, I then need to put everything into some kind of report. That process should be automated and standardized to the extent possible.

**MR. JAMES GREATON:** I currently work in the U.S. Annuities Division at Sun Life. Before that, I was vice president of Risk Management. I'm going to look at how Sun Life is trying to implement some of the ideas that Max and Ellen were talking about.

I'll give a brief background on Sun Life. It's a Canadian insurer. Therefore, it's subject to regulation by the Office of the Superintendent of Financial Institutions (OSFI), the regulatory body in Canada. We have three different types of entities that we have to worry about in the United States. We have a U.S. branch of a Canadian company. We have a U.S. subsidiary of that company. We have two other subsidiaries—Keyport, which is a life insurance company, and IFMG, which is a marketing organization—that were recently purchased by Sun Life.

It's different up north of the border. OSFI is a federal regulatory body that regulates all financial institutions, not just insurers but also banks, brokerage firms and the like. Their exams include an assessment of the risk management capabilities of the organization. They look at the inherent risks and the risk mitigants that the insurer has put in place. They're currently in the process of implementing a risk management rating system, so they're going to rate each financial institution, not just insurers, as to how they manage risk. So there's a real imperative for us to have a risk management process up and running. It's something the regulator has mandated that we're going to do, and OSFI is going to rate us on how well we're doing it.

As Ellen described, it's important to have a framework. It's what our approach to risk management is going to be and, more importantly, who is going to be responsible for what and how that is going to be delegated down into the organization. I want to stress that this is how Sun Life has done it; it's not the only way. You could come up with a different framework and you could come up with different responsibilities. The key is that you have a framework and assign responsibilities to individuals.

We have written policy statements that we call "consolidated risk management policies" (CRMPs). The board approves them, and the board gives specific authority to management to implement policy statements and risk categorizations within the written policies. Once the board has promulgated a risk management policy, the central risk office will then try to slate it into different risk categorizations and come

up with policy statements. We have a grid that we put together that uses red, yellow and green lights. Red are those risks that we want to avoid. Green are those risks that are okay to take. Yellow are the risks that you need senior management approval to accept. Then we've put together a process.

The policy statements will state what kinds of risk we take. What kind of risk is it, and does it fit smoothly into the current categories that we have? What's our tolerance level for it? Are we going to accept it or not, and how much will we take? It also defines a maximum tolerable loss in terms of volatility of annual earnings. How much pain are we willing to take in any one year for having the risk on board?

I'll step through what our high-level categories of risks are under our consolidated risk management policies. There's capital adequacy risk. Do we have sufficient capital to absorb expected fluctuations in the business? We have asset risks, such as credit or liquidity. We have liability side risks, such as mortality, morbidity, lapse, and expense. We have asset/liability risk. Do we invest properly to match the cash flows of the liabilities? Then we have operational risks, such as fraud, market conduct, legal liability, terrorism, disaster, HR concerns and strategic concerns.

I thought I'd take a moment to review so you can get a feel for the framework and how it's designed to operate. Let's take credit risk. We have a consolidated risk management policy about investment risk. In it, there will be a maxim, or statement, that we take on investment risk in order to minimize the costs of our liabilities. In order to maximize our return on investments, we need to invest in obligations of corporate companies. They have credit risk associated with them. Then we'll assign responsibility to a particular position, not to an individual, in this case the chief investment officer, to investigate credit risk and generate maximum allowables for it. Then there's a policy process in which the chief investment officer will come up with, for credit risk, tolerances within certain investment portfolios for how many names are allowed or what exposure to particular names is allowed. There are very specific limits defined. Then there's a process to monitor whether we're complying with the limits. It's a top-down approach. At the top, authorization is given to an individual to set the risk parameters. Then the parameters are defined, followed by a process to see if we're complying with the parameters.

In a general risk management framework, the first thing you need to do is to figure out what risks you have. You then need to select a risk management strategy. You need to implement that strategy, report on it and monitor it. Then you start the cycle again. You then have to re-identify or reassess the risks, select the strategy and go around again.

I want to stress what Ellen said, that identifying the risk is not a risk management function. Risk management is the leadership in the organization that puts the process in place. It has a public presence to enforce the culture that you're trying to impose on the organization. But it's the organization itself that has to take ownership for the risk management process. It's not a risk management function to

identify the risks. You're providing a framework. You make sure that the risks are identified and tracked. It's the other folks on the front lines that know the business, see the stuff coming, and go with it.

The real intent is to have a strategic business unit (SBU) own the risk, not the risk management area. If risk management owns it, then no one is managing it. Other areas can help us identify our risks in addition to the strategic business unit. That could be audit, compliance or controllers. Investment folks or sales folks can also contribute ideas.

We have several different processes in place at Sun Life that help us identify risks. One is a "top 10" process. Annually, each strategic business unit and each corporate line function, such as the finance area, the compliance area or the audit area, will identify what they think the top 10 risks are that their organization faces.

Our product design process is also a place to identify risks. It's where we price a product and design it, but part of that process is to identify the risks associated with a new product. Our compliance area also identifies risks. They notice a lot of the risks because someone else in the industry has messed up. Generally there is a regulatory body that is either put in place to monitor that risk exposure or regulations have been put in place to avoid it. So compliance is a useful function for identifying risks and having them appear on the radar screen.

We've also instituted a series of regular reports that helps us identify when risks get out of kilter, and that can spur identification of risks. We produce maximum risk tolerance limit (MRTL) reports, earnings at risk (EaR) reports, and an annual dynamic capital adequacy test (DCAT), which is disaster scenario testing.

In Canada, they also have something called the SSBFPs, the Sound Standards of Business and Financial Practices. It's a questionnaire put out by OSFI that identifies if you have various management practices in place. That can be a good process to identify risks. Either there's not a management practice in place to handle something on OSFI's list, or a company response says that the process was in place but failed in the last year because something else popped up.

We also do an annual assessment of embedded options in our organization, where we look at the liability side of the balance sheet and assess each product for its embedded option features. Once you've identified a risk, management has certain options. Ellen went through these as well. You can avoid the risk, manage the risk with a mitigation strategy, transfer the risk, accept it, or try to eliminate it all together. You can eliminate it by fully transferring it or avoiding it.

You can't have risk management without a management action plan. Within our consolidated risk management policies, there is authorization for management to deal with risks. The risk management policies call for specific action plans, with clear lines of accountability for each risk. In other words, if the risk is identified in a

"top 10" process, through an audit or an SSBFP, we need to identify the risk and have a written paper trail of what the action plan is. Are we going to avoid the risk? Are we going to transfer the risk? Who is responsible for implementing the action plan? It is no good unless it's executed, so these action plans are usually put on people's performance objectives.

Part of the process is to have regular reporting. We have a series of committees within Sun Life that meet regularly and receive regular reports. There's a senior leadership team as well as risk management committees. Ultimately it all rolls up into a report that is given to the board once a quarter.

Part of the process is actual incidents, things that have arisen during the quarter. There are current assessments. Each actionable item will be assessed as to whether anything has been done on it. The person who is held accountable reports to the risk management committees on that item. Of course, there are status updates on the action plans.

I said there are risk management committees; we have more than one. We have a U.S. Risk Management Committee. We have a Central Risk Steering Committee, which is made up of the risk management officer in each one of the national offices, along with the chief risk officer for the company. We have an Executive Risk Committee, which is comprised of the chairman, president and chief financial officer of the organization. The chief risk officer reports to the Executive Risk Committee once a quarter. The Audit Committee of the U.S. boards gets a report once a quarter, as does the Risk Review Committee of the parent board. Of course, Internal Audit also does periodic reviews. Part of their review process is to review the "top 10" process, but they will also identify separate initiatives each year, most of which have some risk piece to them.

All this corporate governance does not come at zero cost. There's a staff. We have a corporate staff that sets policies within the consolidated risk management policies. There is a vice president in charge of risk for each of the national operations in the United States, Canada, U.K., and Asia. They monitor compliance within the national organizations.

Can't we avoid all risk? No. As Ellen and Max have alluded to, acceptance of risk is an essential part of our corporate strategy. The goal is to earn a competitive return at acceptable risk levels. Effective risk management protects and enhances our value. It helps us meet that return goal within acceptable risk levels.

There are some practical pitfalls that should be avoided. One is if there is a risk identified, but it's not "owned" by someone in the business unit. If it is a corporate-identified risk, nothing will get done until the business takes ownership of the risk. In order for risk management to be effective, it has to be embedded in the culture of the organization. It has to be something that is bought into by the organization and by the strategic business units. They have to see that it adds value to the

organization.

Management at the senior-most level must support risk management. They must look for the reports, read them, and give you feedback. They have to make sure that if a risk is identified, a strategy is identified and accountability assigned, that there are incentives for the individuals in the organization to follow through on those plans. If there aren't incentives, it won't be done.

The framework must be understood. There have been times when portions of our framework have been confusing or contradictory. That doesn't help actuaries, in particular, when you're trying to come up with a product development process and you have to comply with two different standards, which don't jive with each other internally.

As actuaries, we tend to think of risk in terms of things that can be quantified. We like to manage asset-side risk because we can come up with distributions of investment returns or interest rates or credit losses. A lot of risks in organizations reside outside of typical actuarial issues that we tend to study and develop probability distributions for. The operational-side risks, the risks of a sales organization, and the risk from competition invading your particular market niche are all types of risks that you need to have on your radar screen and that need to be part of this process. Don't be afraid of a risk because you can't quantify it. You can probably quantify it within big boundaries, such as it's less probable than a tornado. That's fine. Put it on the list and assign responsibility for someone to be thinking about it. Have an action plan in case it comes to fruition, or be thinking about how you can avoid it. That's a real helpful thing to have in your organization.

**MR. SHELDON LAVEMAN:** How much should an insurance organization spend or budget to build one of these frameworks? How much might we spend on an ongoing basis? I think that Sun Life is a good example, because it's multijurisdiction and multiline. How long might it take until you have this framework in production? As much as there was a comment that we shouldn't be fearful of something we can't measure, how can you actually measure whether this thing is working? Is there any research that demonstrates it's actually effective at all?

**MR. RUDOLPH:** I'll answer the last one first. I think there are plenty of examples where if you don't have it, bad things have happened. Enron was thrown out as the example of a company with a chief risk officer. It comes back to the culture and the champion. Did anybody listen to the chief risk officer?

**MR. GREATON:** How much do you want to spend? You probably already have a lot of the quantitative tools in place. You probably already have tools that manage and look at ALM risk, credit risk, or underwriting risk. It's not that expensive of a function to put in place. You do need some staff. You do need a chief risk officer. If you're involved in multiple jurisdictions, you probably need a person in each one. But that person's primary job, at least to get off the ground, is merely to collect the

information that's probably already embedded in the organization and to surface that information to the top. It takes some time to put that framework together. Some work has already been done in books like the one Max mentioned. There's time spent studying, putting together some documents, running it by senior management, and getting the board to approve it. It's not going to happen overnight. It's going to take you a year or two. Your first cut at it is going to be wrong. You're going to redo it. But it's doable.

**MS. COOPER:** I'll add that if you have nothing in place, the best way to start is by tackling one line of business and deal with some of the process-type questions. I think if you did it in the right way and it was a proactive effort, you could have something up and running in several months for one line and also have a first attempt at a policy. Within probably three months, you could be looking at stochastic modeling results to measure things like interest rate and equity risk for one line of business. Then you add from there. It also allows the company, your organization, to buy in to what's happening. Once they realize the power of what you're doing, they will want to see it across the whole organization. They will be hungry for more once they see what's happening.

As a follow-up to Max's comment, I think if you don't measure it, you can't manage it. Without being able to know what the number is, we have no way to know whether or not it's good, bad, or indifferent.

**MR. RUDOLPH:** You want to leverage off of the models you already have. If you're doing cash flow testing already, a lot of your financial models have already been created. Where the struggle comes in is how to do the operational risk and how to correlate that back to the financial risk. In terms of cost, we have to convince our senior management that it's not really a cost because the return is going to be greater than the cost to the unit.

**MR. LAVEMAN:** Can one of you give an example of a framework in place that led to the successful avoidance of a risk and therefore, you did achieve a benefit that exceeded the cost?

**MR. RUDOLPH:** Several years ago, when Long-Term Capital Management was going down and interest rates were dropping, we looked at whether we should buy some floors to back our deferred annuities. We said the volatility cost was too high right then and we would be better off going naked on that. So we did. We saved quite a bit of money by not doing that.

**MR. GREATON:** We did the opposite. We bought a series of hedges to hedge our GMDB costs on the variable annuities because it violated our maximum risk tolerance limits for earnings. They're currently in the money. We haven't sold them yet.

**MS. COOPER:** Companies often use stochastic modeling to do things like manage

interest rate risk. We help companies on a quarterly basis look at things like the duration and convexity of their portfolios. They actually make decisions about investment strategy, new products, and interest rate crediting strategies based on being able to duration match. That's part of the risk management process. On the equity side, how much equity risk exposure do I want compared to my interest rate risk? We do a lot of that kind of work. We help companies figure out what percentage of risk they actually want to take, which is really an active decision.

**MR. RUDOLPH:** There is a term that we haven't used today. "Risk appetite" is a concept that is becoming very popular. It means choosing the level of risk that you want to have, as opposed to letting it choose you.

**MR. STUART WASON:** Could the panelists give their reflections on whether it's better to have a separation between the role of chief actuary and the role of the CRO?

**MR. GREATON:** Certainly at Sun Life, I think it's been beneficial to have someone who is primarily focused on risk as opposed to the role of the chief actuary. The chief actuary has enough on his plate dealing with valuation standards across multiple countries, as well as looking at pricing standards and the like. There are many areas of risk that are not in the traditional actuarial domain. You don't need an actuary to be a chief risk officer. However, it's a good opportunity for an actuary to step out of a traditional role and broaden his or her experience. That's been a good thing for the person that has stepped into that role. So I think it's a positive thing, and these two people certainly have enough on their plates to keep them occupied.

**MR. RUDOLPH:** I personally think that in an insurance company, the chief actuary is a very good candidate for chief risk officer because of the skill set that we have. So much of the dollar risk is financial, and the actuary likely has a better feel for that than the accountant or even the investment officer. But I don't think it should always go to an actuary.

**MR. SEAMUS CREEDON:** I have a comment and perhaps a question for Jim. Our equivalent of OSFI in the U.K., our integrated regulator, is the Financial Services Authority (FSA). As an aside, they publish reports on insurer risk management practice that are worth reviewing from their Web site. They regularly draw contrasts between banking industry practice, which they generally like, and insurance industry practice, of which they're generally critical. They make the point that the best banks, particularly the investment banks, are ahead in terms of developing risk management frameworks, whereas the insurance industry generally is in a position of trying to guess what will satisfy the regulator. That's the comment leading up to the question. How much of Sun Life's approach was driven by OSFI versus Sun Life running ahead and creating good practice?

**MR. GREATON:** I think it's a combination of both. OSFI chastised Sun Life for its

risk management process a few years ago, and that spurred the process. They weren't too helpful in directing us as to where we ought to go, so it is an internally developed process that we came up with. It's something that they are a lot more satisfied with.

**MR. JOHN SCHREINER:** In discussions I've had with the rating agencies, the enterprise risk management processes that they've seen at insurance companies have underwhelmed them. What feedback have you gotten from the rating agencies?

**MR. GREATON:** They've been positive with what we've put in place. It may be something of a comparison to other insurers—we have something. They're impressed that we quarterly measure our maximum risk tolerance and earnings at risk. These are things that are not done typically in U.S. insurance companies. So we've gotten some positive strokes from them, but it may be just because we're a little ahead of the rest of the field.

**MR. RUDOLPH:** What we find is that we get some very nice comments in the rating agency write-ups. Over time, what we've tried to do is put together a consistent presentation so they see the same thing from year to year. Many of them are learning at the same time as we are. I'm finding that we're getting better questions every year. Also, because we show them things and ask them every time if there is something they'd like us to do, as they start going through and creating, for example, new capital tests this year, we've gotten on the list and gotten to see those ahead of time. We've had some comments on them and have been allowed to comment on them. We don't always get what we think makes sense, but they listen. If they don't agree with us, they seem to look for verifying opinions from an unbiased source. I think they're very open to companies that are doing this type of work, and I think it is reflected somewhat in the rating agency reports that we get.

**MR. MARK ABBOTT:** There has been a lot of volatility in the market, especially in the last several years. In your board discussions defining risk appetite, how do you actually communicate that, what do you think is the best way to communicate that, and what role would scenario analysis have in that process?

**MR. GREATON:** Once again, what we have done in our maximum risk tolerance is to communicate it purely in terms of how it's going to impact Canadian GAAP reported results. In other words, a certain shock to the equity markets or interest rate markets is going to impact your Canadian GAAP earnings by X million dollars. That's what has been communicated up directly to the board level. They've come back with directions that we should not allow it to vary more than X, and that's been translated into action.

**MR. RUDOLPH:** Sun Life is quite a bit ahead of where we are. We frequently struggle to get our message to the board. There's a book coming out called "Asset/Liability Management of Financial Institutions" by Leo Tilman at Bear Stearns

(available through Institutional Investor). A number of actuaries wrote chapters in it. I think it will be a good read. It's designed to go beyond insurance companies and talk about banks. I think it will be a good reference point for us to look at where we're at, relative to other financial institutions.

**MR. ABBOTT:** My personal view is that there needs to be a balance in risk management between the various competing risk management perspectives. I think the chief risk officer has to be someone who is very inclusive in their thinking, to encompass not only the various financial reporting needs, what the regulators want to see and what the rating agencies want to see, but, ultimately, what is going to make the company perform best in the long run. The CRO must have the long-run perspective in addition to the short-run perspective. There needs to be a balance of economic valuation perspectives and these accounting issues. I want to get your opinion about these two competing interests. How can you best mitigate the risk to the organization of doing something incorrect that will damage it in the long run, while balancing these competing interests in the short run?

**MS. COOPER:** That's part of the challenge, Mark, no question. Some of what we've helped clients with is looking at the risk under different frameworks. We're looking at short-term, long-term, GAAP versus stat versus economic value. Companies are struggling with the question, if I'm measuring economic value by calculating a fair value of my liabilities and I'm looking at market value of assets, can I manage to that? It's not really how the world works right now. I can't really manage to an economic value. I can manage to my GAAP income, but economic is more difficult at this point in time. I think it is part of the challenge and the balance. You're right—it's very complex. There are lots of different issues, lots of competing needs, short-term versus long-term, different accounting relevancies. Cash versus accounting is a whole other issue. Just having these frameworks in place, you can really look at all the different types of analysis.

**MR. GREATON:** Part of what makes the job fun is that you have the different frameworks. My old boss didn't like to have multiple models because he didn't want to have multiple answers. I think getting the multiple answers sometimes helps you understand the problem better, because you come at it from several different points of view, and that's helpful. That stimulates the discussion and helps you understand your business better. If you're going to narrow in on a single constraint, then you're going to miss a little bit of the richness of the analysis.