# RECORD, Volume 31, No. 1*

2005 New Orleans Life Spring Meeting
May 22-24, 2005

## Session 83 OF
## Risk Management Governance

**Track:** Risk Management

**Moderator:** Francis P. Sabatini

**Panelists:** Craig R. Raymond
Kenneth Swenson†

*Summary: One of the most important elements of the risk management process is the process itself. Risk governance is an important part of any risk management process, yet the insurance industry has not implemented the procedures and controls as extensively as banking. This session looks at the elements of risk governance and discusses their importance to the risk management process. Specific emphasis is placed on risk management organizational structures and how different organizational structures may facilitate effective risk management processes. Insurance and banking practices are contrasted.*

**MR. FRANCIS P. SABATINI:** Risk management governance is an extremely important topic. We, as actuaries, have not spent a lot of time worrying and thinking about it, but it's at the core of every risk management process. The Risk Management Section has some articles coming out, and one of the articles is recent interviews with some chief risk officers (CROs). Craig Raymond is one of the people whom we interviewed. As you read through those articles, they'll talk about the importance of the governance process and what it means to what they're doing around risk management. It's a cornerstone of any risk management process that's put in place. Some of the companies that have good risk management processes may not be good modelers and they may not be good at a lot of other things, but



† Mr, Kenneth Swenson, not a member of the sponsoring organizations, is senior manager of global financial services at Ernst & Young in .

they're good at the process part, and the process part provides the discipline and the infrastructure to make some very good, sound decisions around managing risk.

I think this is an extremely important topic, and we have two speakers who are going to come at it from slightly different angles. Speaking first will be Ken Swenson. He's an associate with me at Ernst & Young. Ken is a senior manager with our financial services advisory practice, which means he works primarily in the banking environment, where risk governance has been ingrained for some time. One of the hopes here is that we can take some of the best in the banking world and adopt that for our environment. Craig Raymond is chief risk officer for all of Hartford—that means the life company, the property-and-casualty (P&C) company, their investment company and any other company that the Hartford owns. He has one of the more significant senior risk management positions in the insurance industry. He's going to talk from his perspective about one aspect of the governance process at the Hartford.

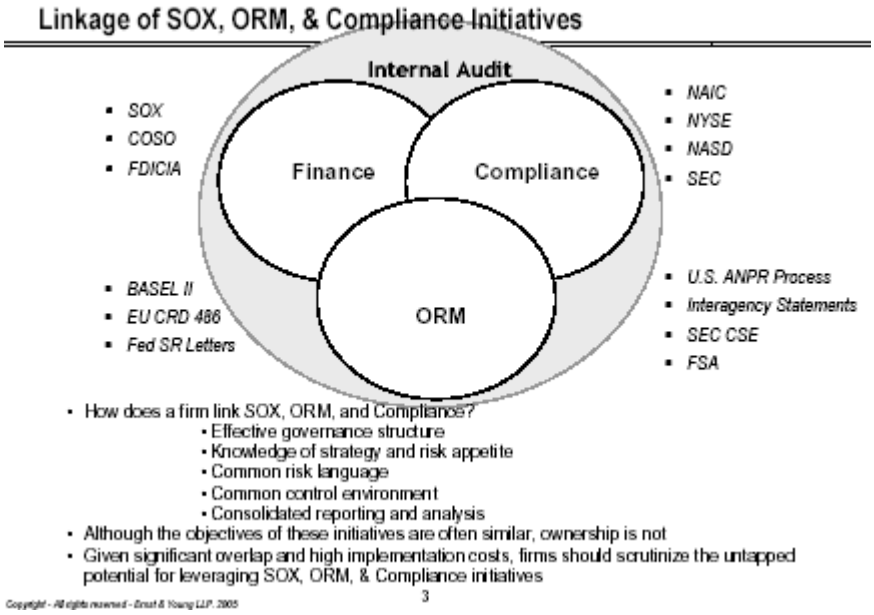
**MR. KENNETH SWENSON:** In light of Frank's comments, I would say that governance is certainly an important topic these days in financial institutions. I've had the opportunity to be involved with a lot of the Basel II implementation process in the commercial banks. It's interesting because you see some of the Basel II risk management practices for risk management and risk measurement trickling into the investment banks, not the least of which are also insurance companies. As a matter of fact, at some of the recent operational risk conferences, the insurance companies are now starting to speak at these conferences as well. They're starting to embrace governance, data collection, quantification and risk information reporting. We're going to hit on most of those topics, with the exception of quantification, but from a banking industry perspective. Craig will bring in the insurance company perspective.

We'll be talking about governance structure and the business hierarchy. How do you manage your business? How does that roll up to the board of directors? Also, a lot of companies are talking about performing, for data collection, a risk and control self-assessment (RSCA). You think about the inherent risk. What could go wrong? How bad could it be? What controls do I have around that inherent risk? What's the residual risk? You might want to think about testing your controls to see if there are gaps. If you have gaps, you put in an action plan and monitor the remediation. We're going to talk more about that. Risk information reporting is important. You need a governance structure, you need to collect some of your data and then you need to report that data. You need to report it, not only at the business-line level, but at the corporate level. So debt aggregation is an important topic. The appendix that we're going to talk about, assuming we get to it, is about the Basel II rulemaking process for commercial banks and some of the supervisory standards that apply that regulators are using to monitor commercial banks in their implementation of risk management and measurement structures. One other piece of data would be loss collection. We're not going to touch upon that very much, but the two ways to think about data collection are risk control self-assessment and

loss tracking (sometimes key risk indicators as well). For today's purposes, we're going to talk about RCSA for data.

Chart 1 lays the groundwork here.

Chart 1




It's kind of the, as I think Frank was saying earlier, "risk du jour." You take your pick. Is it the NAIC? Is it the New York Stock Exchange? This plethora of rules and regulations was great when I was a regulator, but I'm not so sure when you're on the other side of the house that it's great. The idea is, do you want one process to take care of what's going to come around the pike this quarter, the next quarter, next year or five years from now, or would you rather have a hit team assembled where you get all your best people, put them together for two months, solve that, then it disassembles, and then you have the next thing that comes along? Sarbanes-Oxley (SOX) is certainly an example of that. There was a bit of a retooling last week of some of the Sarbanes-Oxley. So, again, do you want a one-solution kind of a framework that can respond, identify, assess, monitor, control and mitigate risk, or would you rather just have a kind of S.W.A.T. team that takes your best resources away from other competing initiatives?

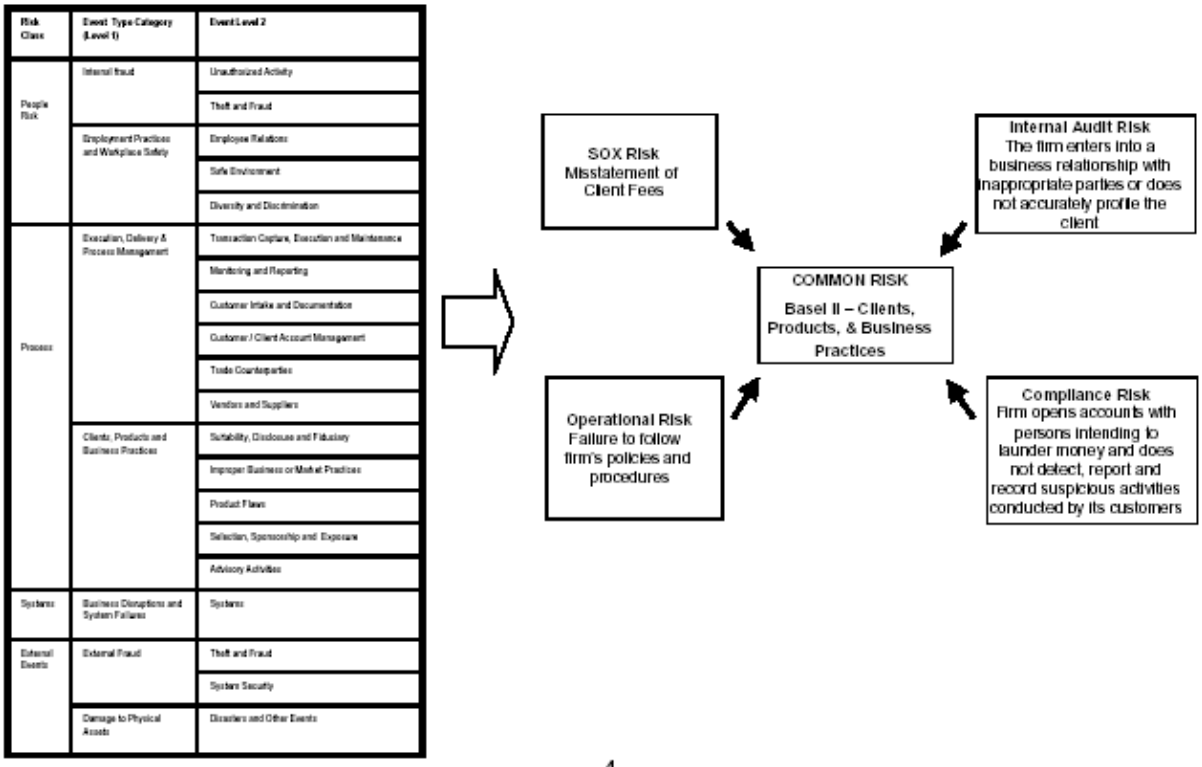
The way that you can do that is by putting in place an effective governance structure, a type of strategy, a risk appetite, a risk language and a common environment. Then you want to report that. You want to think about analysis of the reporting and using it to make decisions. Many firms collect data; not too many use it to make decisions. It's probably an iterative process, and eventually we'll get there, but we're not there yet. I think about the overlap between these different

initiatives and how you put a framework in place. What's driving this is this confluence of framework structures. If you want to think about a common risk language, again, we can think about inherent risk (the risk before considering controls), your controls around that inherent risk and then your residual risk.

You need to think about a taxonomy for risk management. One is shown on Chart 2.

Chart 2

## Illustration: Implementing a Common Risk Language that is Flexible & "Aggregatable"



| Risk Class | Event Type Category (Level 1) | Event Level 2 |
|---|---|---|
| People Risk | Internal fraud | Unauthorized Activity |
| | | Theft and Fraud |
| | Employment Practices and Workplace Safety | Employee Relations |
| | | Safe Environment |
| | | Diversity and Discrimination |
| Process | Execution, Delivery & Process Management | Transaction Capture, Execution and Maintenance |
| | | Monitoring and Reporting |
| | | Customer Intake and Documentation |
| | | Customer / Client Account Management |
| | | Trade Counterparties |
| | | Vendors and Suppliers |
| | Clients, Products and Business Practices | Suitability, Disclosure and Fiduciary |
| | | Improper Business or Market Practices |
| | | Product Flaws |
| | | Selection, Sponsorship and Exposure |
| | | Advisory Activities |
| Systems | Business Disruptions and System Failures | Systems |
| External Events | External Fraud | Theft and Fraud |
| | | System Security |
| | Damage to Physical Assets | Disasters and Other Events |

SOX Risk
Misstatement of Client Fees

Internal Audit Risk
The firm enters into a business relationship with inappropriate parties or does not accurately profile the client

COMMON RISK
Basel II – Clients, Products, & Business Practices

Operational Risk
Failure to follow firm's policies and procedures

Compliance Risk
Firm opens accounts with persons intending to launder money and does not detect, report and record suspicious activities conducted by its customers



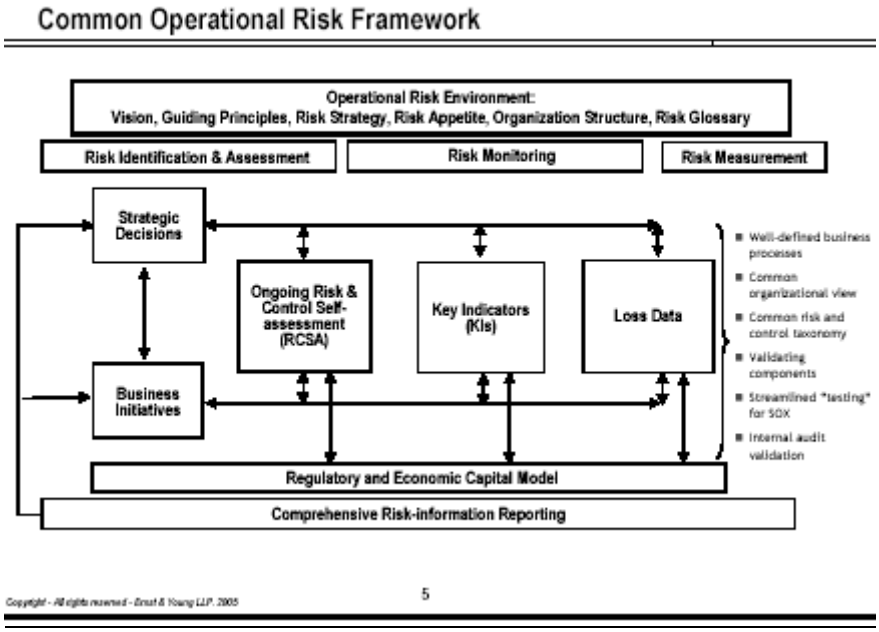
4

This is straight from Basel II. They basically have seven loss event types. They also think about operational risk. Is the risk of loss due to people, process, system or external events when those are inadequate or failed? You can group the seven loss event types into those four areas. Internal fraud and external fraud are two of the seven loss event types. Clients' business practices are a big one. But the point here is that it's one single taxonomy—this one has seven different areas that roll up to four—to think about risk. Some institutions, before they get to this point, might have 25,000 different risks. That probably sounds somewhat unwieldy and probably does not lend to aggregation very well. On the right side of the chart you see SOX and misstatement of client fees, and then someone else may talk about the client fees being inappropriate. They're talking about the same thing sometimes, and if

you think about a taxonomy and roll it into that, you can use it to make decisions and report and aggregate.

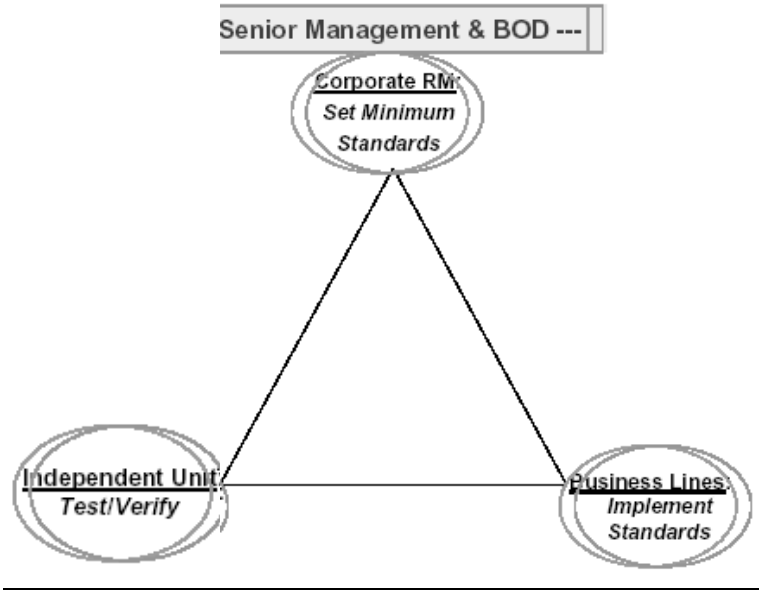
As shown in Chart 3, the board of directors would be on the top of the house thinking about risk strategy, appetite profile, the risk control self-assessment process and also your tactical decision-making, your business initiatives and your strategic decisions, but these can all feed back and forth. Your other data collection could involve key indicators for risk and loss data. But really what informs is, what is the risk appetite? Are we in compliance with that risk appetite? Where are we today, and where would we want to be tomorrow? That's really thinking about how you can derive value from a governance structure.

Chart 3




I want to draw your attention to the equilateral triangle in Chart 4. If there's nothing else that's a takeaway from my presentation, I think this is a good one. You can think about the senior management and board of directors at the top of the house. Within the equilateral triangle, each one has roles and responsibility. There's corporate risk management, the business lines and an independent function, which is typically internal audit. There are roles and responsibilities that each one should have, and corporate should set the minimum standards. The business lines should implement those standards in a business-line context, that is, how it works for them but complying with those minimum standards. With regard to internal audit, the main point is that someone other than corporate risk management and the business lines needs to validate that (1) the business lines are complying with the standards and (2) that the standards are appropriate in the first place.

Chart 4




I think business-line compliance is pretty straightforward, but what do I mean by "appropriate" standards? From a banking perspective, we could talk about reconciliations. Many banks think that if an item is unreconciled for 30 days, you have to sign off on 90-days of charge-off. If that's the corporate standard, that's one thing. If the corporate standard was 300/900, the good news is that the business lines would all comply with that. The bad news is that it would be a terrible standard, and that bank might not be open for too long. That's the idea of the equilateral triangle.

I want to talk about some of the challenges of implementing governance structure. The board of directors wants to set a risk appetite. It can be a quantitative number, or it can be more of a type of qualitative reporting, such as risk control self-assessment. Quantitative reporting would be more of loss tracking and/or capital allocation, which could be fed through the RCSA, as well as loss tracking and indicators. You need to have aggregated risk-information reporting, and also think about a gap analysis. What's your current state? What's your future desired state? As a proxy, you could use the supervisory standards that I'm going to talk about at the end of this presentation. Perform a gap analysis and see where you are. Where are your gaps? Prioritize what you want to close, and move forward to a more cohesive and rigorous risk management structure.

In terms of operational risk management, some of the implementation and challenges are the roles and responsibilities. How do you report it, and how do you link it to Sarbanes-Oxley and other initiatives? If it's one cohesive framework that fits all those needs, I think that's better than having a one size fits all answer for everything that's difficult to aggregate. You need to put together some policies and procedures.

Many firms spend about 80 percent of their time collecting data and 20 percent, at best, analyzing the data. If you think about it, it probably should be the flip of that. Again, it's probably an iterative process, so maybe it will happen across time. Speaking to that, the challenge for the business lines is harmonizing risk management framework implementation. You might have four business lines. One is doing a great job and one is doing a terrible job, and the other two are doing okay. But if you don't have a harmonized implementation, it's not going to be a cohesive apples-to-apples framework across the firm.

With regard to independent testing and verification, Frank and I talk to a lot of institutions that say, "Well, there's nothing for me to audit. What can I audit? The framework is brand new. It hasn't been implemented, and the ink isn't dry yet." Again, if you've done a gap analysis, you have an implementation plan with milestones that are measurable. Audit can play a role there. Once you move along down that line, you can think about the corporate standards. Are they being implemented by the business lines? Are they appropriate?

It would seem pretty simple. You have minimum standards, implementation of the standards and validation of the standards. That sounds very straightforward. What's the problem here? This is what typically happens. Often you will have, for example, internal audit executing the RCSA process, and you say, "Well, don't the business lines own the risk?" Those are usually the same institutions that slam their fists and say, "The business line owns the risk, knows the risk and eats the risk." You ask, "Who really does the assessment of the risk?" They say, "Oh, that's audit." You can play around with this. If you have it configured the right way, this is the way you can drive the framework through.

So, again, it's pretty straightforward. What's the problem? The next thing that comes into play is the business-line risk management. The way I like to think about this is that you have corporate operational risk management responsible for the corporate function, but, by the way, you have the business-line executives, you have internal audit (we've talked about that) and you also have risk managers that should reside within the business line. Then the question becomes, where do they report? Do they report to corporate? Do they report to the business lines? Is it double-dotted? There's a lot of work still being done. Some of the biggest institutions in North America are moving to solid corporate and some are moving to solid business lines. What does that really mean at the end of the day? This is probably where the most work is being done currently.

Now we want to think about the risk appetite. How does that work? What's the governance structure? When you think about insurance companies, maybe underwriting, sales, back office and what you have could be your three or four business lines. They think about reporting to a consolidated risk management corporate committee that thinks about how to identify, assess, monitor, control and mitigate risk as part of an overall approach to risk management. That should flow

up to the board. The board could set a risk appetite and approve limits that they can set by reviewing the risk information reporting. There should also be cascading risk information reporting, so there's more information that goes to the business lines, an exception basis that goes to the risk management committee, and then what you really need to know at the end of the day that goes up to the board.

There are some implementation challenges in risk control self-assessment. I've seen certain firms that are quite large and quite complex that have a risk control self-assessment process. They show this excellent heat map for the different risk classes and the different business lines. It's red, yellow or green. Green is good, red is bad and yellow is kind of indifferent. Then you ask how they arrived at this. They have five generic questions that they ask across the firm. So it's kind of hard to figure out how they heat map the firm. One could probably heat map any firm. The question is data integrity. That's kind of a closed end, where you have five generic questions across the firm.

There's another way to think about it. More of an open-end risk control self-assessment would be thinking about a facilitated session with the business lines and with the business-line risk management as well. What are my key risks across the taxonomy? Populate that. What are the controls around those risks? Think about testing that risk. That's the way you can surface gaps and tighten up the risk management of the firm.

Typically RCSA is separate from internal auditing risk assessment; this is a self-assessment of the business line by the business line. As firms rely on risk control self-assessment, the experience is that it usually takes about two to three iterations for business lines to successfully implement such a process. The first time is kind of tough.

I have some industry observations. There's linking this process to Sarbanes-Oxley, which we talked about. Also, there's mapping to the auditable entities, which is kind of interesting. You might have four business lines, or maybe you have 40 business lines. Well, how do your self-assessment entities map against the auditable entities? After all, audit is charged with validating the process to the extent that they map against the auditable entities. If it's one to one, that's great. But if at least they can map, that's still feasible. What's your risk class universe? Is it credit market optional? Is it reputational? Is it strategic? Again, what is your taxonomy for risk class universe? What are your standards? What's your rating methodology for high, moderate and low? Is it objective or subjective? A key thing is testing. You can look at RCSA processes, and they can often be pretty sophisticated and pretty complex, depending on the business line in which it's engaged. A good way to look at how rigorous the process is that if you have a 10-page RCSA that has no gaps, my guess is that no one did any testing. If there's no testing, you'd lose a lot of the value, if not all of it.

Chart 5 is an example of risk control self-assessment. What's the business unit? What's the inherent risk? Is it people, process, system or external event? If you want to think about lending to quantification, you might want to think about the frequency of that event happening and the severity of it happening—how often and how bad? What are the controls around that? Again, it's critical to know if you tested or not. Is there a gap? Was there an action plan? What's the milestone or remediation?

Chart 5

**Data: Risk & Control Self-assessment:** *Template Matrix*
*-- For Illustrative Purposes Only --*

| Business Unit: Level 1 & 2 | Inherent Risk (People, Process, System, External Event) & Average Transaction $ Amount | Inherent Risk Rating (Include Frequency/ Severity) | Control | Control Rating (Indicate Preventative/ Detective/Compensating | Tested (Y/N) & Gap Noted (Y/N) | Gap Description | Action Plan (Y/N) & Comments (As Necessary) | Implementation Milestone Date & Comments (As Necessary) |
|---|---|---|---|---|---|---|---|---|
| Underwriting | | | | | | | | |
| Claims | | | | | | | | |
| Sales | | | | | | | | |
| *Aggregate* | | *Moderate* | | *Acceptable* | | | | |



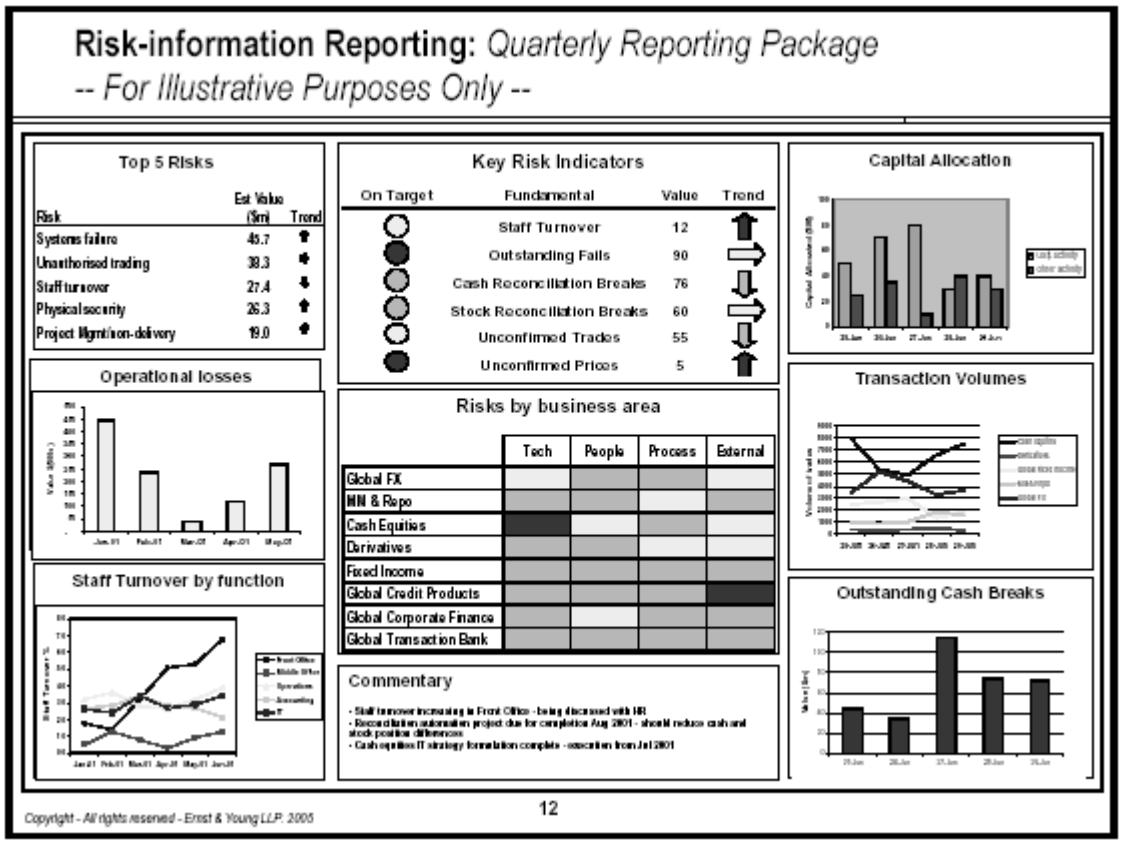

Let's talk about risk-information reporting. Some firms have business-line reporting. Fewer firms have firm-wide board awareness and reporting and aggregation. Typically if you ask what information goes to their board, especially in terms of operational risk, maybe some sporadic losses and some audit findings go to the board, but probably not solid risk-information reporting, which would include loss tracking, key risk indicators and risk control self-assessment. Again, is it used to make decisions or is it just some paper that goes somewhere and disappears? That's the data collection versus data analysis issue.

Firms are striving to get meaningful data aggregation to use it to make decisions and to better inform the firm. Another idea is that once you start collecting this information, you start with point-in-time. That doesn't tell you quite as much as a trend across time. An example is, why are IT exceptions high? Because it's IT. You know that a lot better when you have the trend across time as opposed to the point in time. The best and most rigorous is to use it to make a risk response. Think about "acceptable, transfer, mitigate." You might want to accept the risk. You might want to use risk transfer, i.e., assurance, or you might want to avoid and get out of that business line.

Here are some ideas in terms of observation of the industry. You need to aggregate the data, report it, monitor it and use risk resolution. Also, is it timely, relevant, accurate and complete? Absent any of those elements, it tends to lose some of its usefulness. Is it transparent? Can you understand what it's trying to say? Good risk information moves from qualitative (subjective) to quantitative (objective).

Chart 6 is a generic example of risk information reporting. I don't want to draw too much from it, but this could be one reporting template that could go to your risk management committee and possibly the board. It gives you a lot of information. It's just one example, but the takeaway here is that you should have consistent risk reporting across time so it can be comparable and can be viewed to see what happens from one quarter to the next quarter.

Chart 6




I will quickly talk about the Appendix now. Again, Basel II is a global rulemaking process for capital measurement and management. Within the United States, we have a Basel II rulemaking process, which is the Advance Notice of Proposed Rulemaking (ANPR). There are 33 standards in there that apply to institutions that want to implement sophisticated risk management. I want to highlight a couple of those standards to demonstrate how an institution can think about what it wants to implement and what standards. What could be its desired state in performing a gap analysis? Some standards are straightforward. Some are not. We're going to talk about the governance structure first. Then we're going to talk about data, and then we're going to talk about risk information reporting, which has been the theme of this presentation.

Some of the standards that apply to governance structure talk about oversight, the framework, corporate risk management, business lines and independent unit. I think the oversight standards numbers S 2 and S 3 say that the board should oversee the development of the operational risk framework and changes to that framework, and establish accountability. One way to do it is the equilateral triangle. Another thing is, has the framework been approved, if not by the board, at least by a committee of the board? That would lend to board awareness. Are there appropriate resources allocated to support the framework? This is a good question.

It took some of my colleagues a while to figure out how to actually implement this. How can you determine if you have enough resources? I think the answer is to perform a gap analysis. A gap analysis against the supervisory standards can drive your implementation timetable and milestones. That's a demonstrable way to say that, yes, you do have the appropriate resources or, no, you do not.

In terms of the framework, this is, again, back to the equilateral triangle. You need to have three independent functions: business lines, independent unit and corporate risk management. You should have policies and procedures that talk about identification, measuring, monitoring and controlling risk across the firm as part of an overall approach to risk management.

Corporate risk management is responsible for setting the policies and procedures throughout the institution. It should be applicable to all the business lines and implemented by all the business lines. Business lines own the risk. They have day-to-day responsibility for management of the risk and should ensure that their implementation is consistent with the corporate standard. Independent unit, again, is typically internal audit. Some firms, interestingly, talk about outsourcing this function, but I haven't seen it yet. So typically internal audit serves as a unit that's independent of corporate, as well as the business lines, and is responsible for testing the accuracy and appropriateness of the framework, as well as making sure that it's implemented.

The Advance Notice of Proposed Rulemaking talks about business environment internal control factors (BEICF), but you could think about that as, what's my inherent risk in the business environment and what are my controls? That would be your control factors. So a risk control self-assessment process would be one way to facilitate the business environment internal control factors. You have to have a system to identify and assess business environment internal control factors. If you ask a lot of firms if they have that, they'd probably say that they do: if someone makes a mistake, the person gets fired. I'm not sure if that's very proactive, so maybe a risk control self-assessment process would be a little more proactive.

You should periodically compare the results. You can think about back testing your loss tracking against your risk control self-assessment output. If you say that you have low risk, but you have all kinds of losses, there's some type of disconnect. This is one way of validation as well.

The last point is risk information reporting. You must ensure that risk exposures are reported not only across the business lines but to the board of directors and senior management. You must ensure that the data is aggregated in a timely fashion. You must address both the business-line exposure and the corporate firm-wide exposure and the loss experience, and you must have reports at least quarterly to the board. That's a quick drive-through of, once again, governance structure, risk information reporting and risk control self-assessment.

**MR. CRAIG RAYMOND:** I'm going to tell you what has gone on at The Hartford over the last year to give you a picture of the process that we've gone through to implement an enterprise risk management (ERM) structure, the thoughts that went into that and the issues with which we dealt. Hopefully, I will impart some of the wisdom that I've gained in going through this process.

The Hartford operates as three very independent operating companies. We have a property-and-casualty company, which is a fairly diversified operation. It's in personal lines and commercial lines and is a fairly large player in most of the markets that it's in. We also have a life company, which is a significant player in the variable annuity market, individual life market and group disability, as well as having a mutual fund operation. In addition to that, we have an investment management company, which we operate as a separate entity within the organization, whose role is to provide investment management services to the life and the P&C companies, as well as to manage third-party investments. The Hartford is a very diversified organization.

Operations of this organization have been very decentralized. We really do operate them as independent operations. The holding company, Hartford Financial Services, has traditionally been a fairly small organization where we've had very high-level staff that has operated very much as a fairly "hands-off" holding company. Over the past few years we've been going through the process of looking at where we need to get more involved as a holding company. Where do centralized operations make more sense? Where can we take advantage of doing things across the organization? Another point that's important is that with that decentralization, we are very proud of the entrepreneurial spirit we have within the organization. Despite the fact that we are a very large, diversified company, within the operations (even within each of these three businesses) we run very small business units that operate very independently and generate a significant amount of entrepreneurial spirit. They like to be left alone, which is a great part of our culture but, as we start talking about looking at how we manage things corporately, that becomes one of the issues with which we have to deal.

What goes along with this is that each of these operations has a very strongly ingrained risk management culture within it. The Hartford has been proud of that point for a long time. We are very financially disciplined, and risk management is ingrained throughout the organization. As a matter of fact, when we first started talking about the idea of an enterprise risk management structure and an enterprise risk management function, the immediate feedback we got from most of the business managers was, "Well, risk management is my job. How can you create somebody else whose job it is to be the risk manager, because you're taking something away from me?" For example, I was the chief actuary of the life company. When we looked at the life company, I viewed my job as the chief actuary as being responsible for managing the risks and overseeing the risk management of the life company. At the same time, the CFO, when she was asked, said that her job was to be the risk manager for the life company. We had a few

other people that felt that way, too. That's a good thing, but it doesn't give you that structure where you can pull things together. However, the starting point that everybody's job is to manage risk is very important and ingrained in the culture.

If everybody is already managing risk, why do you need an ERM function? Although everybody was managing their own risks, we lacked an overall framework to ensure consistency across the enterprise. Very often we'll hear words like "common risk language" and "an ability to aggregate." They're very important concepts and very important things to manage risk of the enterprise as a whole. As a matter of fact, when we interviewed management throughout the organization, we received one consistent piece of feedback from everybody. Everybody was very confident that the risks within their piece of the organization were very well managed and very conservatively managed, and they were worried about what "they" were doing over "there." That was a very common message throughout the organization, which, again, was very good. It's a very strong part of the culture. Everybody was very focused on their piece of the operation and that risk management attitude was very much ingrained.

As we looked at this, though, we clearly saw that our businesses were so diverse that without a centralized ERM function, we could not ensure that we had everybody on the same standards and that everybody was being held to the same standards. Again, the feeling that we got from the businesses that they were comfortable with what they were doing but that it was difficult for them to feel that everybody else was being managed to the same standards led to a cohesion around the idea that we *do* need a function. We do need some ability to be able to compare across the enterprise.

Our objective was to create a common enterprise, a common understanding of risk appetite and tolerances. Another objective was to understand and report on significant risk exposures across the enterprise. We had a great deal of reporting on individual risks and risks within each line. The ability to pull things up on a consistent basis and look at risks across the enterprise, particularly where we had similar risks, was something that was a strong, driving force for us. Interest rates affect everybody. Equity risks affect a lot of our businesses. Terrorism was a focal point for us over the last few years. We wanted the ability to wrap that up, roll it up across the whole company and say what our exposure is to a single site across the whole company. As we did this, the ability to develop and share risk mitigation and transfer methodologies across the company were very significant objectives. The end result was to build a framework that enables business leaders to make appropriate and consistent risk return decisions and that facilitates management of overall enterprise risk profile and capital. Consistency and aggregation are very important.

One of my favorite comments when I talk about risk management is "No surprises." Our objective here is to ensure that there are no surprises. "No surprises" doesn't mean that nothing bad will ever happen. What "no surprises" means is that we will

take intelligent risks, and we will never be surprised by the implications of the risks we've taken. People will be fully informed and will understand that these were possibilities, so that when something bad does happen, we can explain that that was a risk we took and why we took it. It's an objective. That's a lofty objective, and we will continue to strive for that.

There were key design principles that we arrived at as we looked at translating these objectives into structure. Risk needs to be owned by the business units. They already had that ownership, and we wanted to clarify that they own the risk. They needed to understand that the ERM function doesn't take that ownership away from them. Actually, the ERM function should not own any risk at all. ERM should be responsible for the framework, for evaluating, understanding and reporting on risk. The business people own the risks. We just make sure that we look at things consistently, report on it and evaluate it appropriately.

Clarity of accountability in responsibilities is critical. Often, "everybody is responsible" translates into "nobody is accountable," and that's not acceptable. Central oversight has to be part of this process, but we need to do it cost efficiently. Enterprise risk management is part of the team and must be integrally involved with the businesses. We need to be a key piece of the operation as a "thought partner." We want risk management to be ingrained in what's done. We want the people that make up the risk management team to be integrally involved in the decision process so that we're not the cops from the outside. We're part of the process. We're helping make decisions and helping move things forward.

One of our objectives was to build on that strong risk culture, leverage the resources that we had and not be duplicative. We have tremendous strength in risk management throughout the organization. We don't want to reproduce that and I don't want to take that away from the rest of the company, so we need to find a structure that will let this happen. Visible risk management excellence is clearly an objective, for me at least. Most importantly, we want to add value, not just bureaucracy. Again, we don't want to be just the cops. We want to enhance our ability to take risk, not just limit risk. That's what effective risk managers should be doing. Effective risk managers are making sure by intelligently understanding the risks they're taking that they can intelligently take more risk and create new opportunities.

How do we structure something that accomplishes this? What you typically hear first about organizational structures is centralized versus decentralized. I always get confused when we talk about centralized versus decentralized, but that's why I like to start from the extremes. The extreme of a centralized process would be where you have a CRO, and the CRO has a very large corporate staff that essentially performs all the ERM functions. The extreme of a decentralized process would be one where you don't even have a chief risk officer. Instead, you have a risk committee. Representatives from various business units work as a team as a

risk committee and manage the ERM function as a committee in a very decentralized fashion.

When we first started talking about this structure last year in creating an ERM function, my bias was toward the decentralized side. I very strongly felt that that was my preference versus a very centralized function, because I didn't want to lose that ownership and the amount of risk management that was ingrained in the business, as well as the connection to the business that the risk manager, being part of the team of the businesses, brings to the table. Most ERM functions, however, are something in between these two extremes. I like to talk about them as hybrid structures. I've talked to a lot of people that effectively operate in hybrid structures, and, depending on their perspective, they'll call it either centralized or decentralized. I've seen people get into fairly heated arguments about whether this is centralized or decentralized; I like to think of it as a hybrid. What we do here is we have a chief risk officer. The chief risk officer has a small staff of functions that need to be at the corporate level and support that needs to be at the corporate level. The CRO also chairs a risk committee, which has responsibility for overseeing the activities of unit-based CROs. Then you have the unit-based CROs that have that chief risk officer responsibility within their units. This structure allows focusing commitment of a CRO and the small corporate staff, which is necessary to build the cohesive framework that's necessary for an effective ERM function, while also leveraging the staff that's in the businesses and keeping that connection to the businesses, which is important for creating a level of understanding and ownership of risk throughout the organization.

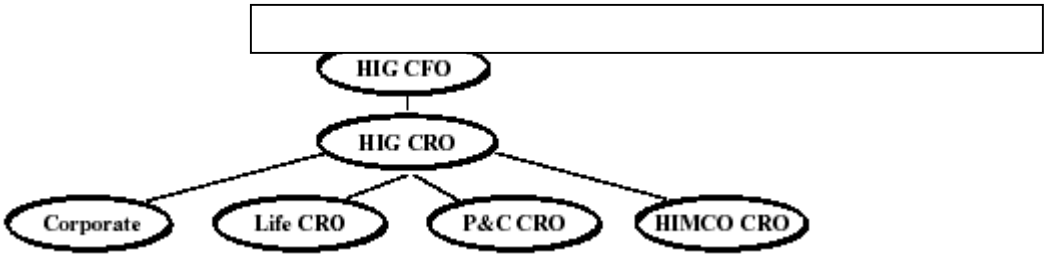
What we at The Hartford settled on was essentially an iteration of that hybrid structure. We started working on this last summer. The drive to create the ERM function came from looking back at all the issues that had occurred over the last few years, starting from September 11, and driving us toward the question, how do we manage the company as a whole? After September 11, our company went through a series of difficult periods that we came through very strongly, but one of the things we learned was that our risks were very strongly correlated across the organization. We had always felt that life and P&C could be operated independently. We discovered over the last few years that when bad things happen to one company, they could very well happen throughout the organization. Terrorism risk, coupled with equity and interest rates, caused us to feel that we had that correlation of risks across the company. We needed to have a corporate function to manage this. We started looking at this very seriously last summer, and we brought in some consulting help to help us look at organizational structure, which helped us settle on this.

I was involved in the process of answering the question, what should this look like? As we went through that process of defining, if we were going to have a CRO, what the job would look like, I was also convinced to take the job, which was not an easy decision. The world has changed very quickly in the last year, and the chief risk officer position has become very visible, but that's a fairly new thing. I think we're

all trying to figure out this role. This is how we implemented this role. I am the chief risk officer. In our company, I report to the CFO. That's one of the organizational issues for a lot of companies. Where should the chief risk officer report? Should it be to the CFO? Should it be to the chairman? Should it be to the president? I report to the CFO, but I have very strong reporting responsibilities directly to the board. I am on the board's agenda at least every other month. We have a package that we provide to the board on a monthly basis for reporting, which we will continue to expand. That's an important part of the function. We established chief risk officer positions within each of the entities. We named a life chief risk officer, property-and-casualty chief risk officer and a Hartford Investment Management Company (HIMCO) chief risk officer. It was very important to us when we established these roles that these were individuals that had significant responsibilities within the operations, that they were tied to the business and that they were respected within the companies, so that they would have a lot of weight and a lot of involvement in what they were doing.

Let's talk about reporting relationships here. Ken mentioned dotted line and solid line. We had a lot of discussion about dotted line and solid line. As shown in Chart 7, these positions have dual solid lines. We define this very clearly. They have dual solid lines with primary reporting responsibility directly into the line. Within our culture that works very well.

Chart 7




It's important that they be part of the business, but it's also important that they have accountability to me and that they have the ability to separate themselves from the business and think about things from a corporate perspective. For example, the life CRO is the new life chief actuary, and he operates as the chief actuary as well as the CRO. There's a lot of overlap in responsibilities. All three of these individuals have other jobs. When I deal with their other supervisor, there's a lot of overlap in what they want them to do in their existing jobs. What they want to do in their existing job has a lot of overlap with what I expect from them as risk officers. It really is a team effort, and there's a lot of overlap in these responsibilities. They're accountable to both their line manager and me.

We're leveraging the expertise that we have in the organization. A very important part of this structure was to not only keep these people on the lines, but also to have access to the staff and the expertise they have. One of the ways we're doing

this is that I work together with this group as a team. We get together on a regular basis. We meet once a week, along with the chief actuaries of the two organizations and the three CROs, to make sure we're on the same page, to make sure we're going in the same direction, to coordinate activities and to open up communication. One of the things that we've done as part of that, to help them to use the expertise but also help them step out of what they're doing, is to make them risk champions on specific issues. For example, the P&C CRO is the risk champion for terrorism risk. Within his organization is where we have the most expertise in analyzing terrorism risk and in evaluating terrorism risk. We've leveraged that throughout the organization by giving him the responsibility throughout the company for our management of terrorism risk. Even though he sits in the P&C company, he coordinates with the life company. He has that responsibility. The life CRO has responsibility for equity risk, not just within the life company but throughout the organization. The HIMCO CRO has responsibility for interest rate risk, and, again, that's throughout the organization. I also chair a senior-level risk committee, which has responsibility for the establishment of our risk tolerances and our risk policies. It includes our chairman, all of his direct reports, as well as the risk officers and the CFOs of the organizations.

I also work very closely with audit and compliance. I see our ERM as filling the holes left after audit and compliance do their jobs. Again, that's one of the places when you create this role that you get sensitivity from a lot of people about what's their job and what's your job.

I spent a lot of time over the last six to nine months talking to people in our audit area and in our compliance area, basically explaining to them that my objective is not to reproduce anything they do or to limit anything they do but to leverage what they do. If there are processes in place that are effectively controlling, managing and reporting on risk, I don't want to take those over. I don't want to replace them. I want to use them and leverage them. My staff and I will look at the processes that are in place, look for where there's holes, look for where we don't feel that we have effective risk controls in place and find ways to either fill those holes or to make sure that there are others in the organization that do have that role. So, again, we work very closely—it really is a very complementary process—with both audit and compliance so that they can do what they do and we can do what we do.

I have learned a few lessons through this process. First of all, commitment from the top is critical. I've talked to a lot of people that have gone through creating risk management functions, and I cannot overemphasize this point. Having the message clearly delivered throughout the organization that the company takes this seriously, that the senior management takes this seriously, that there is going to be reporting to the board, that this is going to happen and that that management team is going to be looking at this is critical to making this work effectively, because you're asking people to change. You're asking people to do some things a little differently, and if they don't get that strong message from the top that they're behind this change and they're behind doing it differently, then it's not going to happen.

There's a second lesson that is also important to me. As an actuary, I like to solve problems. I like to do things. I like to get stuff done. Process to me always felt like it got in the way of doing stuff. An important thing that takes me a bit to get used to is that overlaying good process and structure doesn't get in the way of doing things. It helps do it. You can implement process and structure appropriately without creating bureaucracy. Very often, process and structure aren't done appropriately, and they create bureaucracy. If you do it right, you can create process and structure without creating bureaucracy. Establishing that process, establishing information flow, establishing accountability and establishing reporting structures enhance decision-making. It doesn't get in the way of it. That has been an important lesson for me to learn, but, again, it's very important. But you've got to learn how to do that the right way so that it does help the businesses and not slow them down or hurt them. It's a little bit painful sometimes to get there because, again, you've got to make people change, and you have to put processes in place that don't necessarily fit with what people are used to.

That brings us to communication. Communication is the key to making this work. There's huge value in sharing knowledge across the organization. One of my major accomplishments in the last eight months has been getting people talking to each other. The wonder of an entrepreneurial, decentralized culture is that people operate within their business units and operate very focused within that, but very often that means that they're not learning from other people around them and they're not taking advantage of the immense amount of skill and knowledge that we have, being a very diversified company. One of the things I'm most proud of is that I have our life and property-and-casualty actuaries talking to each other, and they like it. Once we opened them up and got them talking, they're actually seeking each other out and realizing that there are things that they can learn from each other. I always thought there was something that we could learn from each other, but there are a lot of differences in language and a lot of differences in approach, and it takes some work to break down barriers. We have found that it's well worth the effort of getting people communicating and working together.

My last point is that dictating standards and process doesn't change behavior. I've seen a number of people enter into roles like this who have been very frustrated. They have come in and established process and established standards, and they get the reporting they want, but they don't change behavior. You don't want to just change the way people present information to you. You need to change their behavior, and behavior changes occur when you get people to understand and buy into the objectives that you have and why you're doing them. Again, that goes back to communication. You have to get people to understand why we're doing things and not just tell them that they have to do them. That is probably the overarching key to making this work effectively and not just turn into that piece of bureaucracy but turn into something that can add value to the organization.

**MS. BEVERLY E. STEINHOFF:** Craig, one of the key aspects of data collection for operational risk is incident reporting. I'm curious how The Hartford has changed to

an environment where you actually want to encourage incident reporting instead of having people be afraid to speak up.

**MR. RAYMOND:** Within each of the operating lines we've had fairly strict standards from an operational incident reporting basis. That for us has not been much of a challenge to change the culture because it's one that has been ingrained in the customer service structure that we've had for a number of years. I would expect that the challenge was there at some time in the past, and I'll admit that we've had some very talented people that have worked on managing our operations that have gotten over a lot of those issues. I, unfortunately, can't tell you how they got there, but what I know is that we do have a very strong structure of reporting and sharing of information there.

**MR. SWENSON:** It's partially a cultural thing to get away from the feeling that it's bad to raise your hand and say you had a big loss. Maybe it's good to report it, track information and aggregate that information. You can have a carrot-and-stick approach as well, where you can incent it with capital relief. If you have losses declining across time, a stick would be that internal audit could review it and ensure that there's compliance with the corporate standards. If you're not compliant, that might be a bad audit. If you are compliant, that might be a positive audit. I think there are other ways to reinforce it as well. It's also a cultural change from reporting losses as bad to reporting losses as good. Some people say that if you don't measure it, you can't manage it. One institution talks about as soon as they started measuring it, losses went down about 20 percent over a couple of years. There's your value proposition in and of itself.

**MR. RAYMOND:** Very often you find in organizations a bias away from giving credibility to reporting by always having some reason why that report is bad. Even if you have data, there's a reason why you shouldn't be looking at that. One of the things that we have found—I've seen this in other organizations, too—is that cultural change that says, "Look, these are issues that we're going to report on." That sends the message from the top down that you have things, we're going to report on them, and if the data isn't good, then you're going to be accountable for bad data. It's not going to be an excuse that the data is not good. You're going to be accountable for that. That is also an important point to help push things through and get people to give you good data and get people to be accountable for whatever risk issues you're looking at.

**MR. DAVID FRANK TAUBER:** When you actually implement all these processes, going from running your business and managing your business and capital management and growing different product lines, you're obviously going to view those things differently. How have companies gone through that process and been able to change line-of-business management's view of being maybe the star growth line of business? From top down saying, "Well, we have too much of this risk. We need you to slow down." Have you had any pushback on how you're managing your businesses, either on the business side or with those kinds of experiences?

**MR. RAYMOND:** IAgain, it goes back to getting the issues on the table. Yes, part of the driver for seeing the importance of enterprise risk management goes back to some of those issues. As you build the businesses independently, how do the risks fit together? Are there benefits of aggregation? Are there benefits of diversification, or do things just continue to add up? What is the balance of the company? Getting to that point where we can pull things together and aggregate things has been an extremely important piece of that. It does facilitate discussion about what you want the company to look like. How do you want to manage your risks? Where do you want to grow? How do you want to change your businesses? The beauty of having this kind of structure in place is that you can have the information to have that discussion. Until you have a consistent view of risk across the businesses, it's very difficult to have that discussion about the balance between businesses. What's the balance of risk? How do they aggregate? Do I have too much of one or the other? When you don't have that basis of consistent discussion, it's not a productive discussion. The flip side of that is that it does force those discussions, but those are productive discussions.

**MR. SWENSON:** A lot of folks talk about the board setting the risk appetite. If you ask three or four firms how the board is setting the risk appetite, there are not too many ways. It's more qualitative than quantitative. The best you might hear is some form of capital allocation. Then you might ask how you allocate that capital. What's your methodology? They answer that it's gross income. That's not exactly overly risk sensitive.

Maybe the way to set the stage is three words: governance, data and quantification. You need to have the governance structure, which is the triangle. For the data collection, you might have RCSA, indicators, metrics and loss tracking. Then that pulls in your quantification methodology. When you have those three things, you can talk about risk information reporting and going up to the board, which can set the desired risk appetite and the actual risk appetite and close the gaps to get where you want to be. I think the firm across the business lines is becoming more efficient. Maybe it's not a zero-sum game.

**MR. SABATINI:** I'd like to offer one additional comment. I've seen this now in a couple of instances. Once companies have implemented a more disciplined process around risk, what happens is that the lines of business now have to sort of run the gauntlet. What that means is that they eventually end up in front of the risk committee, particularly if it's a major initiative. Either they're going to grow the business, or they're going to introduce new products. In the two companies that I'm thinking about, in both instances they ended up sending people away and disapproving what was being proposed. That had an impact across the entire organization. That began the real culture change, because they realized they couldn't just go and do what they wanted to do. Both of the instances I'm thinking of were around new product introductions. They were asked questions addressing risk issues and addressing other issues. They didn't have the answers. They were

sent back and told not to come back unless they did have the answers. In one instance, I think, they never did introduce the product. Now it's interesting because you talk to the people that are on the risk committee, and they're looking for other opportunities to disapprove to establish their position, but everybody is off doing their homework now and getting it right. So if you put the good governance structure in place, it can change behavior, and it can change it pretty quick.

**MR. RAYMOND:** That's a great example of having the support from the top and of having a structure in place where you can actually have that influence and you can say no to something. That really empowers the process. My objective has always been to never say no but to make sure people understand the objective, so we can get to the point where I never have to say no. I've felt that way in my previous role as well as in this one, but occasionally you have to say no.

**MR. SABATINI:** I have a question for both Ken and Craig. Can you talk about risk policies, the role that those documents play and the importance of those documents?

**MR. SWENSON:** I think the corporate risk management policies are an important thing and probably where a lot of, if not the most, development has happened over the last five years. If you were to ask a lot of firms to see their risk management policy from a corporate standpoint, it might not be a very long policy, especially in the case of operational risk. I think a lot of banks now have pages and pages of policies that talk about roles and responsibilities. When we've actually worked with some of the firms, the governance data quantification is quite a useful technique and outline that's kind of comprehensive and not overlapping. If you think about the different elements of governance data quantification, you can hit on most of all the points that culminate in risk information reporting. In terms of that, it's nice to have some kind of corporate templates that say this is how it's going to be reported, this is the frequency it's going to be reported and this is to whom it's going. Then you roll it through the committee structure as well, which Craig hit on pretty well in his presentation. Roles and responsibilities are important things to talk about.

**MR. RAYMOND:** Policy falls into my "process can be good" area. I'll admit that when I became the chief risk officer, policy was identified as a very high priority for me, and it was not something that I felt all that strongly about as being important. I like to do stuff, and writing policy was not one of the things that I saw as a real priority. I'd say that I've gained an appreciation for the process and the importance of policy. We are spending a lot of time on getting policy in place so that we have a clearly delineated process for making decisions. It's clear through the policy what authority the board has delegated, to whom they've delegated that authority and how decisions can be made. One of the things we found when we first started pulling together some really good information was that when we got together to look at making decisions off of that information, it wasn't clear who had what authority to make some of these decisions, as well as exactly on what basis we

were going to make the decision. It was very telling to me the first time I sat down with a group of senior managers and we looked at an issue, about which everybody had very strong opinions, and the question that two of them asked was, what are we trying to accomplish? We know we have a risk and we want to do something about it, but what is the objective? What are we trying to accomplish? Having that clear policy gives everybody that clear direction. You understand what authority has been delegated, what level of authority has been delegated and the objectives. That is key to establishing that framework so that you can make appropriate decisions.

**MR. SWENSON:** The first thing is your definition. What are you trying to achieve? Until you figure that out and put it on paper, it's fairly ambiguous. Once you've done that, it becomes an auditable process, which is important because, after all, corporate risk management should be an auditable entity that's subject to audit, just like a business line. So, the first thing audit should do is say, "Where's your policy? Where's your procedure? By the way, are you in compliance with that?"

**MR. JAMIE P. BEAUCHAMP:** Craig, do you have any advice on how a junior-level associate can get involved in the enterprise risk management process? You identified the stages and the levels of people that are involved, and they're very senior-level management.

**MR. RAYMOND:** What I would say is that the function is very broad-based. A lot of what we do as actuaries feeds into the enterprise risk management process. The best preparation to getting involved is to make sure that you're getting a broad understanding of the risks of the business and getting broad exposure to the risks of the business, and not just understanding it from a purely technical basis but understanding how risk affects the business. The difficult step for many actuaries is stepping beyond just analyzing the risk to being able to look at the implications to the business. One of the things I find in people that are effective at the broader roles is communication skills. When I've talked to people and when I look at other structures, the key to being effective in enterprise risk management is not just having the technical, analytical skills but being able to explain what this means to people. Finding the opportunities to develop those skills is the best way to move your career in that direction.

**MR. SABATINI:** Speaking as the chairman of the Risk Management Section, one of the first things you should do is join the section if you're not currently a member. We'll provide you with plenty of educational opportunities. At the same time, you should look for opportunities to work on risk management-related activities within your organization. If there are parts of the organization that are focused on risk management, even if there's no formal ERM component of the organization, you should seek out those opportunities. Then work on building the skill set and getting as much exposure to the subject as you can. There's plenty of material that you can read that will open your eyes, because risk management is a lot more than stochastic modeling. That's part of why we've had some of the sessions that we've had during this meeting and others. Risk management is not just interest rate risk.

It's not just equity risk. Craig, of the five broad categories of operations risk, interest rate risk, equity risk, credit risk and governance risk, where do you spend most of your time, as you look across the past year?

**MR. RAYMOND:** That's easy. Governance is where I've spent most of my time. Frank has got a great point. There is a lot more to it than just the analysis that we're used to on the risks.

**MR. SABATINI:** That's not typically the stuff that is currently part of the exam syllabus. You need to go buy yourself a book on operational risk. You get a guy like Ken who lives and eats it every day, and he's talking about self-assessments, and I'm sitting here thinking, what the heck is he talking about? We work on projects together, so I actually do know what he means, but I didn't know it, and, since I don't like to read books, I hang out with people that know something and I learn that way. I would add that to your list.

**MR. RAYMOND:** Absolutely. One of my objectives over the next 12 months is to add somebody to my staff that has expertise on operational risk because it's not our initial focus. None of my experiences has prepared me for it.

**MR. SABATINI:** I think the operational risk issues are the ones that present the greatest risk to insurance organizations, not necessarily the financial ones, because we've gotten pretty good at managing those. We haven't been as disciplined on the operations risk side as, for example, the other financial institutions, such as the banks. Typically you need the governance process to drive all that.

**MR. SWENSON:** I'm an operations risk guy. From being on the interagency Basel II subcommittee, in credit risk they're probably all 55-year-old, gray-haired people. In operations risk, that wasn't the case. I would say also that there's capital risk management and corporate risk management. There are probably a lot of opportunities in business-line risk management. A corporate group sometimes is a small set of people, only four or five; it's not this monstrosity of hundreds of people. But there are a lot of opportunities within business-line risk management to think about process improvement.