Examiner®

Volume 42
Number 1
Spring 2017

Official Publication of the Society of Financial Examiners®

Examiner®

Volume 42 | Number 1 | Spring 2017

ISSN 0190-2733

Official Publication of the
Society of Financial Examiners®

Publisher
Society of Financial Examiners®
7044 S 13th St.
Oak Creek, WI, 53154
Tel: 414.908.4930
Fax: 414.768.8001

IN THIS ISSUE

CRE READING PROGRAM INSTRUCTIONS

The Society of Financial Examiners has a Reading Program for Earning Continuing Regulator Education Credit by Reading the Articles in *The Examiner*.

You can earn **2 CRE credits** for each of the 4 quarterly issues by taking a simple, online test after reading each issue. There will be a total of 9-20 questions depending on the number of articles in the issue. The passing grade is 66%. To take the test, read all of the articles in the issue. Go to the Members section of the SOFE website to locate the online test. This is a password-protected area of the website, and you will need your username and password to access it. If you experience any difficulty logging into the Members section, please contact **sofe@sofe.org**.

NOTE: The Reading Program Test from this issue and future issues of *The Examiner* will be taken online. You will no longer print out the test and send it in for scoring. Each new test will be available online as soon as possible within a week of the publication release. The Reading Program online tests are free. Scoring is immediate upon submission of the online test. Retain a copy of your online test score in the event you are audited or you need the documentation for any other organization's CE requirements. Each test will remain active for one year or until there is a fifth test ready to be made available. In other words, there will only be tests available for credit for four quarters at any given time.

Earn Continuing Regulatory Education Credits by Reading The Examiner!

The questions are on the following page. Good luck!

Earn Continuing Regulatory Education Credits by Reading *The Examiner!*

CRE READING PROGRAM QUESTIONS

All quizzes MUST be taken online

"How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency"

Multiple Choice Questions — Submit Answers Online

1. Q: Which of these are among the five key principles that an effective ERM program should include?
   a. Risk culture and governance
   b. Risk identification and prioritization
   c. Risk appetite, risk tolerance, and risk limits
   d. All of the above

2. Question: What is meant by Risk Profile?
   a. A composite picture of the risks an organization carries by virtue of what business it is in, its business model, strategy, and objectives.
   b. The maximum amount of risk a company is able to absorb in the pursuit of its strategy and business objectives while remaining viable.
   c. The amount of risk an organization is willing to take to achieve its strategy and objectives.
   d. These tools put specific directives or limits on the amount of variation that will be tolerated.

3. Question: What is Risk Appetite?
   a. A composite picture of the risks an organization carries by virtue of what business it is in, its business model, strategy, and objectives.
   b. The maximum amount of risk a company is able to absorb in the pursuit of its strategy and business objectives while remaining viable.
   c. The amount of risk an organization is willing to take to achieve its strategy and objectives.
   d. These tools put specific directives or limits on the amount of variation that will be tolerated.

4. Question: What is Risk Tolerance?
   a. A composite picture of the risks an organization carries by virtue of what business it is in, its business model, strategy, and objectives.
   b. The maximum amount of risk a company is able to absorb in the pursuit of its strategy and business objectives while remaining viable.
   c. The amount of risk an organization is willing to take to achieve its strategy and objectives.
   d. These tools put specific directives or limits on the amount of variation that will be tolerated.

CRE READING PROGRAM QUESTIONS

All quizzes MUST be taken online

5. Question: What is Risk Capacity?
   a. A composite picture of the risks an organization carries by virtue of what business it is in, its business model, strategy, and objectives.
   b. The maximum amount of risk a company is able to absorb in the pursuit of its strategy and business objectives while remaining viable.
   c. The amount of risk an organization is willing to take to achieve its strategy and objectives.
   d. These tools put specific directives or limits on the amount of variation that will be tolerated.

"The Value of ERM Interview"

True or False Questions — Submit Answers Online

1. Enterprise Risk Management does not need to pervade the entire organization.
2. Risk based interviews are the only source of information that can be used to gain an understanding of an entity's risks.
3. Among an organization's various units, risk based interviews promote a broader perspective and base of thinking about an entire organization's risks.
4. Effective risk interviews are considered to be less effective when open-ended questions are asked.
5. The various amounts of information that is gathered from risk based interviews is limited in its use for the organization.

"Fraud Risks in 2017"

True or False Questions — Submit Answers Online

1. Identity theft fraudsters use stolen personal information, e.g. name and Social Security Number, etc., to set up a shell company, usually an LLC because it is the easiest to create.
2. With the newest technology in online banking, double-cashed fraud schemes have been declining.
3. According to the FBI report, the CEO E-mail fraud had cost U.S. businesses in excess of 2.3 billion dollars in 2015 alone.
4. According to the 2016 Cost of Data Breach Study: Global Analysis Benchmark research sponsored by IBM, The average cost to the victim of a data breach in 2015 was $4 million.
5. The U.S. Department of Justice stated there are approximately 4,000 ransomware attacks by cybercriminals daily in the U.S.

Fraud Risks in 2017

By **Robert Minniti**

As we progress through 2017 it is a good idea to consider some of the newer fraud risks facing organizations in a digital world. The Association of Certified Fraud Examiners estimates businesses lose around five percent of their revenue to fraud, so it is important that we identify the fraud risks so proper internal controls can be put in place to help prevent and detect these risks to the organization. Here are some frauds that were trending in 2016 and should be considered risks in 2017.

Criminal Identity Theft

There is a modern version of criminal identity theft. The typical pattern for this newer type of criminal identity theft is for the criminal to misappropriate your Social Security Number, driver's license number, passport number and other personal information. There are various ways for the criminal to do this including data breaches, mail fraud, phishing, vishing, etc. They can also get personal information from social networking sites or by purchasing information on the darknet. Once they have your personal information, they use your name and Social Security Number to set up a shell company, usually an LLC because it is the easiest to create. The paper work for the shell company will be filed with the state, but there are no operations, nor is there any real business being conducted. After the criminals have the shell company approved by the state they open a bank account, with you as the owner, again using your Social Security Number, as the sole proprietor of the LLC. The address will for the shell company will usually be a box at a mailbox store which was rented in your name and usually paid for with cash in advance.

Once the shell company and bank accounts are set up, the fraudsters get to work cashing stolen checks and processing transactions from stolen credit cards in the shell company's bank accounts. Once the funds are available in the accounts, the criminals immediately wire the money out of the accounts, usually on the very same day the funds were released. The funds are usually sent to overseas bank accounts to make it more difficult to trace. The money is then laundered and put back into the criminal's pockets. In a case from Houston, Texas, the fraudster was able to cash over $5 million in stolen checks using this fraud scheme. In another case from California, two defendants pleaded guilty for fraud after cashing stolen U.S. Government checks using bank accounts that were opened using stolen identities. When law enforcement starts to investigate, the identity theft victim is usually the first one brought in for questioning.

Double Cashed Checks

In 2016, there was a growing trend in double-cashed fraud schemes. This particular scheme takes advantage of some of the newest technology in online banking. When a payee receives a check, the payee uses their cell phone to deposit the check into their bank account. The check clears and

Fraud Risks in 2017

(continued)

the victim reconciles their bank account without any issues. Up to this point everything is legal and no fraud has occurred. The fraudster then sits on the check for five or six months and then takes the original check to a checking cashing outlet and cashes the check by presenting the original signed check. If the victim is properly reconciling their bank account, they will notice that this check cleared a second time. If the victim is lucky, and using positive pay, then their bank may refuse to pay the check a second time. Herein comes the legal issue. Unless the victim can prove the check cashing store knew the check had been previously deposited, the check cashing store will usually prevail in litigation to get paid for the check since it has an original check with a valid signature.

Once the victim has paid the check cashing store, his or her only recourse is to sue the payee who cashed the check twice. It would be especially difficult to convince a prosecutor to file criminal charges against the payee unless the victim could show a history of double cashing checks because the payee is going to claim it was a mistake, and they forgot they previously cashed the check. The payee will often offer a payment plan of a minimal amount per month with no interest to repay the money. Because of the claim that this was an error and an offer for restitution, it could be all but impossible for the prosecutor to establish mens rea or intent for the crime.

CEO Spoofing

CEO spoofing is another fraud that took off in 2016. On April 4, 2016, the FBI reported the CEO E-mail fraud had cost U.S. businesses in excess of 2.3 billion dollars. CEO spoofing occurs when the criminal creates a fake email that appears as if it was the CEO's legitimate email. The criminals use the spoofed email to send an invoice or instructions for payment to an accounts payable clerk with instructions that a payment be made that day by check or ACH. The spoofed email will often contain a fraudulent invoice with an "Approved" stamp and the CEO's signature, which was copied from documents on the internet. Once the payment is sent the thieves transfer the funds out of the United States making recovery difficult.

Data Breaches

Data breaches not only inconvenience the victim companies and the individuals whose information has been compromised, but they also place a significant cost on the victim. Because an organization is considered to be negligent in its duties to safeguard the information provided to it by employees, customers, and others there is a significant cost to being a victim of a data breach. According to the 2016 Cost of Data Breach Study: Global Analysis Benchmark research sponsored by IBM and independently conducted by the Ponemon Institute, LLC , the average cost to the victim of

[1] http://www-03.ibm.com/security/data-breach/

Fraud Risks in 2017

(continued)

a data breach in 2015 was $4 million. Smaller organizations fared better than larger ones. The average cost of a smaller data breach where less than 10,000 records were compromised was $2.1 million; whereas the average cost of a larger data breach where 50,000 or more records were compromised was $6.7 million. The average cost of a data breach in 2015 was up 29% over the average cost in 2013. On average it cost the victim approximately $158 per record compromised.

Ransomware

Ransomware is a type of malware that is placed on a computer which then encrypts all of the files on the computer. The criminals then require that the victim pay a ransom in order to obtain the decryption key and have access to their files. The most well known example of ransomware is CryptoLocker. Cryptowall 2.0 is a newer version of ransomware being used by cybercriminals. The FBI estimates that ransomware is a $1 billion a year fraud. A new type of ransomware, called Reveton, installs itself onto the computer without the user's knowledge. Then, the computer freezes. A bogus message from the FBI pops up on the screen saying the user violated federal law. To unlock their computer, the user must pay a fine .

For a single computer, the cybercriminals will initially request a ransom ranging from $300 to $500. Larger ransoms are demanded when more computers are infected with the ransomware. Once the deadline for the payment has passed the criminals up the ransom demand to around $1000 per infected computer .

Typical ransomware software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key .

On August 9, 2016, the FBI changed its position on paying the Bitcoin ransom to the cyber criminals. Supervisory special agent for the FBI's Cyber Division, Will Bales, said that businesses or individuals targeted by ransomware should refuse to pay the ransom. The U.S. Department of Justice stated there are approximately 4,000 ransomware attacks daily in the U.S.

Credit Card Fraud Attacks on the new EMV Chips

While many people believe the security of their credit and debit cards has increased because the banks and card issuers added EMV (Europay MasterCard and VISA) chips to the cards, this may not in fact be true. Although the EMV chips make it more difficult for criminals to skim the information on the card and create a duplicate card, the criminals have

[2] https://www.fbi.gov/audio-repository/news-podcasts-thisweek-reveton-ransomware/view

[3] https://www.knowbe4.com/

[4] https://www.knowbe4.com/

Fraud Risks in 2017 (continued)

developed a new fraud scheme to take advantage of the vulnerabilities of the EMV chips. These chips are radio frequency identification chips (RFID), and you can pay for a transaction by waving the EMV chip card over a point-of-sale transaction device designed to capture the RFID information. What most consumers don't know is that the chips in a smart card can be read at distances up to three feet away.

The criminals are aware of the new chip card's vulnerability, and they use portable, battery-operated, point-of-sale devices to capture the information broadcast by the smart cards and process card present transactions. The criminals go to crowded areas such as malls, sports venues, subways, busses, and other public places carrying these portable devices and have them automatically process a card present transaction for under $50, which is the federal legal limit for a fraudulent transaction that is the responsibility of the consumer. For fraudulent transactions over $50 the card issuer is responsible for the transaction. When consumers attempt to dispute these transactions, some card issuers will argue that since the card was present, and you still have possession of the card, it must be a legitimate transaction. They may even imply you just forgot about making the purchase.

As CPAs we need to be aware of these trending fraud schemes and ensure that our clients or employers have considered these fraud risks and developed appropriate internal controls to help prevent or detect these fraud schemes. The Arizona Society of CPAs offers numerous continuing professional education courses on fraud and internal controls throughout the year to keep us informed of the latest fraud schemes.

About the Author

Dr. Robert Minniti
President and Owner
Minniti CPA, LLC

Dr. Minniti DBA, CPA, CFE, Cr.FA, CVA, CFF, MAFF, CGMA, PI is the President and Owner of Minniti CPA, LLC. Dr. Minniti is a Certified Public Accountant, Certified Forensic Accountant, Certified Fraud Examiner, Certified Valuation Analyst, Certified in Financial Forensics, Master Analyst in Financial Forensics, Chartered Global Management Accountant, and is a licensed private investigator in the state of Arizona. Dr. Minniti received his doctoral degree in business administration from Walden University, received his MBA degree and Graduate Certificate in Accounting from DeVry University's Keller Graduate School of Management, and received his Bachelor of Science in Business Administration degree from the University of Phoenix. Dr. Minniti teaches graduate and undergraduate courses in accounting, fraud examination, fraud criminology, ethics, forensic accounting, external

Fraud Risks in 2017

(continued)

audit, and internal audit, at DeVry University, Grand Canyon University, Northwestern University, and the University of Phoenix. He designed graduate and undergraduate courses for Grand Canyon University, Northwestern University, and Anthem College. He is a writer and public speaker. He has experience in forensic accounting, fraud examinations, financial audits, internal audits, compliance audits, real estate valuations, business valuations, internal control development, business continuation planning, risk management, financial forecasting, and Sarbanes-Oxley compliance work. Dr. Minniti is an instructor teaching continuing professional education classes for the American Institute of Certified Public Accountants, ComplianceOnline, CPE Link. AccountingEd, Clear Law Institute and various state CPA Societies.

The Value of Risk Interview As Part of Enterprise Risk Management Strategy

By **Neil Amato**

Enterprise risk management (ERM) demands an entity-wide strategy—one that comes from the top and encompasses the entire organization. For executives, even those whose main job is to oversee risk management, it can be difficult to have a full view of the risk landscape, especially in larger organizations with far-flung divisions.

To better understand the risks a company faces, experts recommend risk interviews that, when done correctly, improve the ERM process one answer at a time.

The process is fairly straightforward: Facilitators interview employees across the organization to glean valuable insight that can help uncover major risks or developments surrounding known risks.

Once risk interviews are completed, organizations can use the information to better educate employees, executives, and board members; can revamp strategy based on risks identified in interviews; and can better integrate risk discussion into other company functions, such as budget approval and internal audit.

"I've been amazed over the years at how candid people are about what they feel about risk," said David Hughes, CPA, assistant vice president of ERM and business continuity planning at HCA Holdings, a Nashville, Tenn.-based operator of health care facilities.

Hughes oversees one-on-one risk conversations for the company, which has more than 230,000 employees and records $40 billion in annual revenue from hospitals, surgery centers, and other medical facilities it owns and operates in 20 U.S. states and in England.

Initially, HCA's risk interviews were part of the internal audit function; there wasn't a formal ERM program until 15 years ago. The number of interviews conducted was small at first. The talks were limited to about 15 members of the executive team.

Last year, the ERM program included more than 100 interviews, either face to face or by phone—a process that takes a couple of months to complete. Another month is spent analyzing the interviews for information that will influence the company's ERM strategy and preparing a report to share with executives and the company's board of directors.

With a broader number of voices, Hughes said, there is better perspective, and there are more early warning signs about emerging risks.

Why the Risk Interview?

There are plenty of other ways for an organization to quickly seek information from numerous employees. But solutions such as suggestion boxes and

The Value of Risk Interview As Part of Enterprise Risk Management Strategy

(continued)

hotlines rely on employees to volunteer information, and anonymity can be a barrier to getting to the root of the problem. Online surveys, another tactic, can also be tricky. Not everyone reads every email, and not everyone who reads the email completes the survey.

While some surveys can be used effectively—and they are at HCA, according to Hughes—they also have limitations and should not be the company's exclusive source of information. HCA uses information from the risk interviews in addition to data from hundreds of employees who take an annual online survey, to get a more accurate, multilevel picture of company risks. Follow-up questions in surveys are difficult, and it can be hard for someone reading a typed answer to get a full sense of the respondent's tone.

The in-person interview solves these problems. Facilitators have the advantage of being able to read nonverbal cues and body language. Interviewees are more likely to open up in a conversation, especially when they are assured that their names will not be attached to their comments.

"You're getting a sense of materiality or concern about the risk or the topic, more than you would get reading the text of a survey," said James Rose, CPA, payer sector compliance practice leader for consulting firm Navigant's health care practice. "You can type out, 'That's a risk.' Or you can say, 'Wow! That's a risk!' The facilitator's ears are going to perk up, and they're going to ask for more on why. You get a better sense of what the concern is."

What are the Questions?

The questions in a risk interview can be simple; they are designed to be conversation starters. The first one is generally along the lines of "What are the top risks?" At HCA, the risk interviews include three planned questions:

- What are the top three business risks, in priority order, the company faces over the next two years that could have a significant adverse effect on the company's ability to achieve its strategic and/or financial objectives?
- What are some of the things the company is doing to help manage or mitigate each of these three risks?
- In your opinion, are these risk mitigation strategies effective? And if not, what else should we be doing?

Who is Interviewed?

At HCA, 101 risk interviews were conducted in the fall of 2015 by Hughes; Joe Steakley, CPA, senior vice president of internal audit and enterprise risk services; and Phil Billington, CPA, vice president of internal audit. The company's 61 corporate executives were interviewed, along with 30 division executives and 10 of the company's board members.

The Value of Risk Interview As Part of Enterprise Risk Management Strategy

(continued)

Each year, Hughes circulates his interview list with corporate and division executives to see whether more people should be interviewed. If a new executive is hired or someone has been assigned to head up a new major initiative, that person's insight should be included. Each person is asked the same set of questions, but the answers are different based on their perspective. The chart "A Ranking of Top Risks" highlights the different perspectives as well as the alignment of management's views on the company's risks.

Surveys are also sent to officers of the individual hospitals. HCA owns about 170 hospitals, and the executives at approximately 50 hospitals receive a survey each year, meaning each executive is sent a survey every three or four years.

How are the Answers Used?

The interview and survey answers go into a database, and HCA uses a program to produce visualized reports. Since all risks are not equal, the company prioritizes them by assigning point totals to each respondent's risk ranking: 5 points for the top risk, 3 for the second, and 2 for the third. By the end of the calendar year, Hughes has all the data, and the information is presented to executives and to the board in January.

The compilation can show which risks may have bubbled to the top and can help influence strategic plans. These top risks are added to the agenda of the full board and board committees, and risk owners present updates on how risks are being managed and how they may affect the company's strategic objectives.

HCA also finds value in tracking the risk rankings over time and their relationship to one another. The chart "Risk Summary by Year" is an example of a report shown to the board. It also shows how certain external factors such as the economy or changes in the regulatory environment affect the risks.

The interviews themselves serve another purpose: They get different parts of an organization thinking more about risks outside their own. When people in operations start thinking about legal, financial, and regulatory risks, for example, they think more like a CEO and less like a division manager. "If communication is good up and down the ranks, the right risks get focused on before they become big problems," Hughes said.

The Value of Risk Interview As Part of Enterprise Risk Management Strategy

(continued)

The traits of an effective risk interview

Risk interviews involve more than going down a list of questions and recording answers. Here are four tips for an effective risk interview:

1. ***Prepare the interviewees.***

   Sending a calendar invitation with the title "Discussion about top risks" is not as valuable as providing light preparatory work in advance for those to be interviewed. Larry Baker, CPA, senior leader of ERM at Devon Energy in Oklahoma City, said risk interviews are more valuable when the interviewees are given a simple, one-page template to use for their preparatory notes and a high-level inventory of risk categories so that they think more holistically about an organization's risks. The following is one example of a preparatory statement: "We want to discuss with you the top three risks to the successful execution of your strategic plan."

2. ***Ask open-ended questions.***

   An interviewee is more likely to talk if an interview has fewer questions, and includes ones that are conversation starters, according to David Hughes, CPA, assistant vice president of ERM and business continuity planning at the health care organization HCA Holdings. If someone hears, "OK, here are 30 questions we're going to ask you," that person tends to make answers shorter so he or she can get through the interview faster. Interviews at HCA basically consist of three open-ended questions.

3. ***Ask appropriate follow-up questions.***

   Sometimes, this involves reading people, who may give nonverbal cues that they're holding information back. Other times, the follow-up question is as simple as "Why is that?" For example, if a division executive says a risk mitigation strategy is ineffective, it's worth asking why. That person likely knows more about the particular risk, and mitigation strategies, than the interviewer does. Simple questions can elicit valuable information.

4. ***Take good notes, and compare notes.***

   Hughes said two interviewers take part in each risk interview, and both take notes. After the interview is over, the interviewers compare notes to make sure information is not misinterpreted. Sometimes, they send the notes to those interviewed to make sure they accurately captured the person's thoughts. Baker also recommends having two interviewers, one to type answers in real time while the facilitator asks questions and listens for needed follow-ups.

The Value of Risk Interview As Part of Enterprise Risk Management Strategy

(continued)

About the Author

Neil Amato is a Journal of Accountancy senior editor. To comment on this article or to suggest an idea for another article, contact him at namato@aicpa.org or 919-402-2187.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

By **Donna Galer, Kristina Narvaez, Max Rudolph**

Some have said that looking at company's financial condition is like looking in a rear-view mirror. It shows how well they have historically performed, but not how well they are likely to perform in the future. Others disagree, expressing their view that the past is a predictor of the future. In addition, the more solid a company's financial footing is, the more it will be able to handle risks and losses that may materialize. In the case of insurance companies, it is paramount that the capital and reserves they carry be sufficient to cover losses they are contractually bound to cover and can withstand unexpected internal and external risks to which they are subject.

An examination of a company's financials, therefore, should include a review of the company's risk profile, risk capacity, risk appetite and risk tolerances because they provide some insight about how future risk is being managed and how their solvency level is being protected. For a regulatory examiner, looking at such components during an exam will lead to a better understanding of the company's risks and controls that are not previously addressed in either the basic exam or an ORSA Summary Report. However, these components should be addressed in the full report since the NAIC's Own Risk Solvency Assessment Guidance Manual - Section 1 requires a Description of an Insurer's Enterprise Risk Management Framework. An effective ERM framework should, at minimum, incorporate the following five key principles:

1. Risk Culture and Governance
2. Risk Identification and Prioritization
3. Risk Appetite, Tolerance, and Limits
4. Risk Management and Controls
5. Risk Reporting and Communication

In this article, we will review the definition of risk profile, capacity, appetite, and tolerance and provide some examples. It should be kept in mind that some of these terms are evolving and not consistently defined by standard setting and regulatory organizations. Thus, there are more than one set of definitions in existence.

What are risk profile, risk capacity, risk appetite, and risk tolerance?

The **risk profile** is a composite picture of the risks an organization carries by virtue of what business it is in, its business model, strategy, and objectives. Each company has a unique risk profile. This composite view provides management with either a starting place at process inception or, once an ERM framework is in place, *a current risk state* to monitor and revise its risk capacity, risk appetite and risk tolerances, as well as to structure its approach to identifying, mitigating and reporting risk. The profile also helps to highlight where correlated risks might exist.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

For example, a regional mono-line workers' compensation insurer has a different risk profile than a national, multi-line commercial insurer, and it is different again from a national life or regional health insurer. Each insurer also has an investment strategy that combines asset specific risks with interactions tied to asset-liability management strategies. Although each insurer has a unique risk profile, there will be similarities among those which have similar business models. For example, an excess and surplus insurer which does not recognize and prepare against the uncertainties of competition and soft pricing from primary insurers during poor economic times does not comprehend its own risk profile. For other types of insurers, competition may take place for different reasons and take different forms.

Risk capacity is defined as the maximum amount of risk a company is *able* to absorb in the pursuit of its strategy and business objectives while remaining viable. For insurers this threshold identifies constraints from regulators and other stakeholders. How much risk an insurer can sustain is influenced by such things as: 1) what kind of business it writes, for example, short tail versus long tail; 2) how strong its reserves are; 3) what its cash flow dynamic is; and 4) its degree of resiliency.

An organization needs to know its ultimate risk capacity in order to frame its risk appetite. **Risk appetite** refers to the amount of risk it is *willing* to take to achieve its strategy and objectives. Risk appetite should be no greater than risk capacity.

An insurer will typically have overall risk appetite statements for the company as a whole. For example, it may say that it will take as much risk up to but not more than that which might be expected to yield a specific (e.g., A-excellent) financial strength rating from A.M. Best. Risk appetite statements will also exist for different functions and levels in the organization. For example, it may require that only investment grade bonds will be bought for the investment portfolio. Or, it may state that underwriting in coastal areas be capped based on premium or maximum probable loss predicted by CAT (catastrophic) models. Risk appetite statements may be qualitative or quantitative. In either case, they must leave no ambiguity.

Risk tolerances will further refine and parameterize risk appetite statements by putting specific directives or *limits* on the amount of variation compared to the risk appetite that will be tolerated. These may be presented as a single value or a range. Risk appetite and risk tolerance establish guidance which influences decisions and behaviors. The goal is to ensure that company strategy and objectives are met by not exceeding agreed upon levels of risk acceptance.

It is expected that risk appetites and/or tolerances will be adjusted infrequently over time to reflect changes, both internal and external, to the

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

company. The important point is that these statements need to be clearly expressed, communicated, and monitored within the organization to be effective. Examiners should be able to ask for and see them, as part of the company's corporate governance.

Unfortunately, performing a good job of stating and communicating its risk appetite and risk tolerance does not guarantee the staff will act in accordance. Aligned behavior is a function of culture and governance. Determinants of how staff will act in regard to risk controls include: 1) does the CEO and senior team consistently adhere to the risk appetite and risk tolerance statements, 2) is performance against these statements measured and monitored, and 3) what happens when risk appetite and risk tolerance thresholds are approached and exceeded.

What follows is an example of how risk appetite and risk tolerance work in tandem to control risk. In this simple case study, the insurer is willing to write some coastal property business (risk appetite) but not willing to write more than a certain amount (risk tolerance).

Risk Appetite	Risk Tolerance
1. Business will be written in coastal areas but will be capped. 2. GWP will grow organically by up to 10%.	1. Total NWP from coastal property related policies will not exceed $200M in any Calendar Year. 2. GWP growth in excess casualty will not exceed 5%.

GWP, gross written premium

NWP, net written premium

It should be clear from this example that risk appetite statements are more strategic, and risk tolerance statements are more operational or tactical.

Why are risk profile, risk capacity, risk appetite and risk tolerance important?

Risk appetite and risk tolerance are created on the basis of a risk-return tradeoff relative to key risks. There must be an understanding and estimate of the potential change in enterprise value based on the possible downside of loss and upside of gain based on varying degrees of risk taking. The risk-reward computation is critical in decisions such as mergers and acquisitions, investments, underwriting limits, aggregations, reinsurance, and pricing.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

Another reason these constructs are important is because they promote a risk aware culture. A culture where risk is never discussed, guidelines are absent or not communicated, and where the idea of balancing risk versus return is not an operating principle leads to risk-taking that quickly spirals out of control.

Insolvencies of insurance companies often emanate from a poor understanding of risk capacity (i.e., how much risk the insurer can afford to take in order to pursue its strategic goals within its risk appetite). In other words, how much risk is the insurer willing to take?

Per an A.M. Best (2016 Special Report updating a publicly available insolvency report from 2004) report on impairments, the primary internal causes identified for insurers becoming insolvent are 1) fraud 2) investment losses and 3) rapid growth. The earlier report also highlighted deficient loss resources and inadequate pricing, noting that problems associated with rapid growth occurred most frequently during a period of soft market conditions with weak industry profits.[2] It is noteworthy that these reasons do not include: 1) extreme catastrophe activity or 2) capital market crashes. So, how were the insolvent companies managing these concentrated risks? How were they weighing the risk/reward of marginally adequate reserves or pricing that failed to reflect the cost of capital? Why did they grow faster than their surplus and other resources could support? Despite the many regulatory safeguards which have been put in place in both P&C (e.g., Economic Capital under stress scenarios) and Life (e.g., Risk Based Capital) insurance segments, insolvencies are not completely preventable.

Without aligning the constructs of risk profile, risk capacity, risk appetite, and risk tolerance to guide the business, decisions could be made with good intentions but disastrous results due to a misunderstanding about how much risk the organization could retain or how much risk-taking was approved. As stated above, risk appetite and risk tolerance statements must be clearly communicated and used in daily management decisions to be meaningful.

How to develop risk appetite statements

Just as it is impossible to identify and manage every potential risk to the organization, it is impossible to have an appetite statement for every risk. Thus, the universe of risks must be pared down to those that are most critical. What are the existential risks to the company? What risks put its solvency level in jeopardy? What are the top ten risks on the ERM heat map?

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

To start, a list of business categories can help to hone the group of risks which need a risk appetite statement. For insurers, common categories include:

- Solvency
- Earnings
- Liquidity
- Investments
- Claims
- Underwriting
- Reinsurance – Gross to Net, Reinsurer Ratings
- Actuarial – Adequacy/Confidence Level
- Reputation
- Compliance

Typical risk appetite statements for some of these could be:

Solvency: Maintain economic capital level at 400% of NAIC RBC (risk-based capital), thus avoiding the risk of regulatory supervision.

Earnings: Earnings will meet plan objectives four out of every five years, thus avoiding the risk of an earnings free fall and the implications thereof.

Investments: Book value for below investment grade bonds will not exceed 50% of statutory surplus, reflecting the investment policy statement requirements and avoiding a risk concentration in this asset class.

Claims: Claims leakage will be kept below 3%, thus avoiding the risk of exceeding the combined ratio objective.

Underwriting: Combined ratio will not exceed planned objective by more than 5%, thus avoiding the risk of reduced profitability and stakeholder confidence.

Actuarial: 90% confidence level for carried reserves will be maintained, thus avoiding the risk of inadequate reserves and the implications thereof.

Reputation: 100% integrity and honesty will be used in all business transactions, thus avoiding the risk of harming the brand and the implications thereof.

Compliance: Duties and actions will be performed with an expectation of total compliance to all laws, regulations and rules, thus avoiding the risk of fines, penalties, reputational damage, etc.

How to develop risk tolerance statements

Given what has been set as the organization's risk appetite, risk tolerance statements are developed to be consistent with and align with the risk appetite targets.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

Management should determine what operations or decisions might pose a significant risk to staying within the overall risk appetite, and then establish a risk tolerance limit. For example, a commercial P&C company which does a lot of fronting business should have a risk tolerance statement about collateral or reinsurance levels for that book of business, a life insurance company might use its investment policy statement to limit exposure to mortgage backed securities or equities. Similarly, any company doing a major technology project should have a tolerance statement on budgeted expenses. If a 20% overage in costs eliminates or pushes the benefit out too many years and a new solution might be better, then management should want to review the project. The risk tolerance statement should state at what point and at what percentage a budget overrun will cause a project to pause and review its likelihood of completion. A possible way to address this would be: a 15% overrun at the last quarter milestone of the project will be tolerated, and a 10% overrun in the first quarter of project will not be tolerated. In other words, the tolerance statement is creating the limits of variability from the target which will trigger an automatic review of the project.

More examples of tolerance statements are below:

Underwriting	Net MPL exposure on any single risk not greater than 5% of statutory capital
Cash Flow	Over 90 day accounts receivable on policy billings will be kept under 2% of total receivables
Revenues/ Retention	Unit linked policies lapse ratio will be no greater than 8% in first five years

MPL, maximum probable loss

Even with today's high industry surplus levels, there is always the potential that an individual company will have difficulty managing its risks. For example, consider Tower Group International in 2014 when it was almost put into liquidation and now its acquirer's (ACP Re) position when it pulled out of A.M. Best's rating pool in 2016 after it was downgraded.[3] On the life side, the American Medical and Life Insurance Company were placed into liquidation in 2016, and the Superintendent of Financial Services of the state of New York was appointed as liquidator.[4] Suffice it to say, these companies lacked risk controls.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

Among a very real host of current uncertainties or risks faced by the insurance industry, here are a few:

Line of Business	Macro-economic	Competition/ Technology
Personal and Commercial Auto-Severity Increase	Interest Rates	New Insurer Tech Start-ups
Florida Homeowners-Assignment of Benefits	Inflation	Driverless Cars, Cyber Crime Escalation

On the other hand, there are positive or upside potentialities for insurers such as: infrastructure projects which could facilitate top line growth, an upward trend in interest rates, and benefits stemming from productive use of big data analytics.

The insurance market is evolving at a rapid rate. As investments in Insurtech, new business models and new product innovations ratchet up, and as the possibility for terrorism, social unrest and climate change escalates, it becomes even more important for insurers to master the nuances of the risk-reward equation for establishing specific levels of risk appetite and risk tolerance. They will need to be able to recognize not only usual and current risks, but also unusual and emerging risks. Those judging the financial health of insurers need to assess how robustly risk is being managed, because that will impact upcoming financial performance and solvency.

Conclusion

Strong corporate governance requires an ERM framework incorporating everything from culture to reporting and communication. An examiner needs to consider this both in context of ORSA but also in the evolving Corporate Governance regulation. The risk profile provides information about exposures and interactions between risks. The tools that align these practices throughout a firm are the risk appetite, risk capacity, and risk tolerance. Risk appetite defines the amount of risk the board is willing to accept, while risk capacity is the amount they are able to take and still be within constraints. Risk tolerances refine these targets and thresholds for everyone in the organization to manage their specific function. When insurers and regulators proactively review risks, the probability of insolvency is greatly reduced and controls can focus on the drivers of potential risk events.

How do Risk Profile, Risk Capacity, Risk Appetite, and Risk Tolerance Help Financial Examiners View Solvency

(continued)

Notes

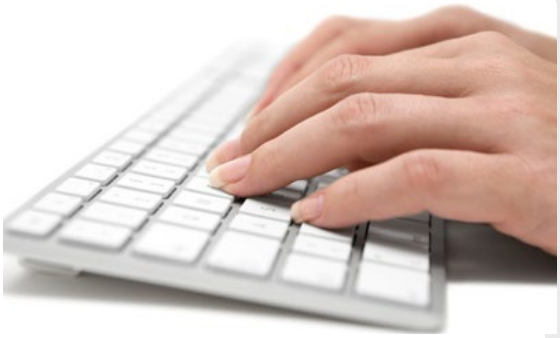
1. NAIC. Own Risk Solvency and Assessment Guidance Manual, July, 2014
2. A. M. Best. Press Release, A.M. Best Publishes 34-Year Property/Casualty Insolvency Study May, 24, 2004 http://www3.ambest.com/ambv/bestnews/presscontent.aspx?altsrc=108&refnum=8621
3. Carrier Management. "ACP Re Pulls Out of A.M. Best Rating Process After Downgrade" July 4, 2016 (Source: A.M. Best)
4. New York Liquidation Bureau. http://www.nylb.org/AmMedNLifeIns.htm

About the Authors

Donna Galer, former EVP and Chief Administrative Officer at Zurich Insurance's Global General Insurance ($36 Billion GWP) with responsibility for strategy development, is now a consultant, lecturer and author. Her co-authored top selling book, Enterprise Risk Management - Straight To The Point, is used in a number of universities in the RM curriculum. She joined Hanover Stone Solutions in 2016 as a senior advisor. She has served on numerous industry related boards and Business Insurance named her one of the Top 100 Women in Commercial Insurance in 2000.

Kristina Narvaez, is a two time Spencer Education Foundation Graduate Scholar (2001, 2002) and won the Anita Benedetti Scholarship in (2002) from RIMS. She has also won two national awards for risk management papers she wrote as an undergraduate student at the University of Utah. She now teaches business strategy at BYU and online ERM at UCLA and has authored and co-authored 45 published articles and two books on the topics of ERM and Board Risk Governance. She joined Hanover Stone Solutions as a senior advisor in 2015.

Max J. Rudolph, FSA CFA CERA MAAA is associated with Hanover Stone Solutions and helps companies develop their strategic ERM process. He is also an adjunct professor at Creighton University and a private investor.



AUTHORS WANTED

The Publications Committee is looking for members to write articles for the quarterly Examiner magazine. Authors will receive six Continuing Regulatory Credits (CRE) for each technical article selected for publication.

Interested authors should contact the Publications Committee Chair, **Tian Xiao**, via **sofe@sofe.org**.

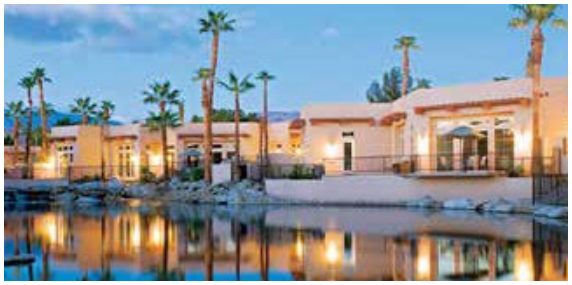
Mark Your Calendars | Upcoming SOFE Career Development Seminars

Details as they are available at: www.sofe.org

2017

July 23–26
Marco Island, FL

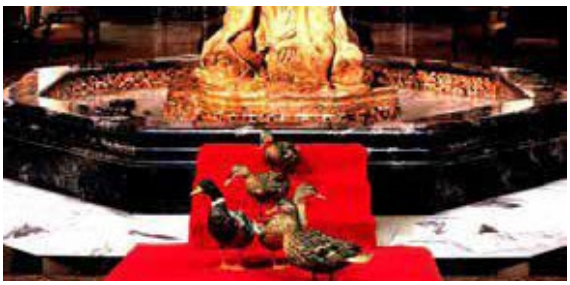
JW Marriott Marco Island



2018

July 15–18
Indian Wells, CA

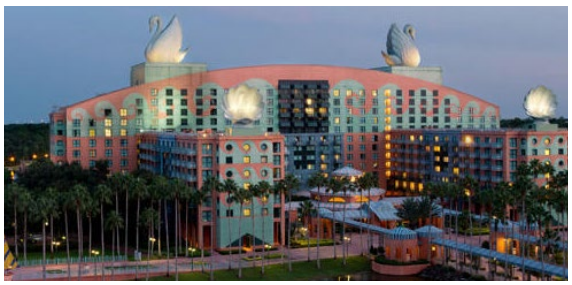
Hyatt Regency Indian Wells Resort & Spa



2019

July 21–24
Memphis, Tennessee

The Peabody Memphis



2020

July 19–22
Orlando, Florida

Walt Disney World Swan Hotel

We are a nation of symbols. For the Society of Financial Examiners®, the symbol is a simple check mark in a circle: a symbol of execution, a task is complete. The check mark in a circle identifies a group of professionals who are dedicated to the preservation of the public's trust in the field of financial examination. Our symbol will continue to represent nationwide the high ethical standards as well as the professional competence of the members of the **Society of Financial Examiners®.**

Society of Financial Examiners®
7044 S 13th St.
Oak Creek, WI, 53154

Tel 414.908.4930
Fax 414.768.8001
www.sofe.org