

MAXIMIZING PERFORMANCE . . . with an Eye on Risk

by Jeffrey C. Grubbs, CPA, MST

Acknowledging that risk is inherent in any business, Thomas Aquinas stated, “If the primary aim of a captain were to preserve his ship, he would keep it in port forever.” Rather than keep their vessels in the safety of the harbor, late 17th century ship owners sought to finance the risks inherent in their business. They did so in places like Edward Lloyd’s coffeehouse in London, where ship owners and merchants gathered to share reliable shipping news and negotiate insurance deals. These were the early years of risk management.

Risk can be broadly defined as the “uncertainty of outcomes.” Risk Management is the process of assessing and managing such outcomes. Enterprise Risk Management (ERM) takes the process several steps further to include a risk-based approach to managing an entire enterprise by integrating concepts of strategic planning, operations management, and internal control. The collapse of AIG and Lehman Brothers will likely result in the publication of numerous ERM case studies.

The CFO plays a critical role in managing risk, and is ultimately responsible for financing it. A well-rounded risk management program consists of four basic components: **Identification**, **Prevention**, **Mitigation**, and **Financing**. Directly or indirectly, it is the CFO’s responsibility to see that all four elements are addressed. Let’s review each in a bit more detail.

Identification

Whether identified or not, risk still exists. Unknown or unattended risk is simply being self-insured. Self-insurance is a viable alternative for financing risk – as long as the potential exposure is recognized. In the absence of that awareness, the results can be catastrophic.

The following can serve as a checklist to determine which exposures you have covered, and which may require attention in the future.

- Workers’ Compensation (mandated in all states)
- Auto Liability (mandated in many states)
- Auto Physical Damage (collision and comprehensive)
- General Liability (third-party property damage and bodily injury)
- Product Liability (lawsuits and reputational risk)
- Slander & Libel (directed at others by your staff, or by others toward your company; usually included in GL)

- Employment Practices (harassment; discrimination; the messy stuff)
- Property & Equipment (damage from fire or vandalism)
- Boiler & Machinery (those big HVAC units on your roof)
- Business Interruption (insurance money may not be enough to save a business)
- Environmental Impairment (inadvertent leakage of gases or chemicals into the environment)
- Storage of Electronic Data (files, programs, email, etc.)
- Terrorism (new to American businesses in 2001)
- Natural Disasters: Earthquake/Flood/Hurricane/Severe Weather (much of the country is affected by at least one of these)
- Loss of Officers/Key Personnel (again, money may be insufficient to replace lost talent)
- Identity Theft (personal or corporate)
- Errors & Omissions (negligence and malpractice)
- Directors & Officers Acts (protects leadership)
- Embezzlement/Theft (internal controls do not always catch everything)
- Intellectual Property Theft (use of registered trademarks, copyrights, and patents)

A consultation with your broker or an independent risk consultant can help you compile a comprehensive list that includes areas specific to your industry, and an evaluation of the adequacy of current coverage.

If you are not sure your broker fully understands your needs, consider conducting a broker review with the help of a consultant. The review need not result in a change of broker; if done correctly, it can strengthen your relationship.

Prevention

The next step involves loss prevention – often referred to as risk control. A well-rounded safety and risk control program is essential and much less expensive than paying for losses after they occur.

Prevention can include some or all of the following.

- Perform a comprehensive hazard and property inspection.
- Perform a loss trend analysis. Ask your broker or claims administrator for a loss run, organized by type of loss, and look for patterns and common causes.

- Perform an employee perception survey. Structure drives behavior. Is management's desired behavior (concern for safety) being supported by the underlying management structure? A perception survey will identify the gap between management's desire for a certain behavior and how well its efforts are received by rank and file staff. Remember, employee perception is their reality. If a gap is discovered, you can begin work to close it.
- Perform a security and technology audit. This can assist in exposing potential vulnerabilities in your technology infrastructure, and the risk associated with your network or data being compromised or corrupted.
- Provide web-based training. While not the total solution, it is an effective method to assure compliance with state and federal regulations and should be considered in any comprehensive, loss prevention plan.
- Provide periodic, live interactive training. This can range from brown-bag lunch events to tailgaters to half-day events with experts in defensive driving, employment practices, ergonomics, lift and carry techniques, and other areas that can immediately impact cost savings.
- Consider where you should have duplication of essential records, such as electronic files and email. Your IS Department is probably working on this, but check in with them periodically to ensure electronic redundancy is completely and consistently in place and not just "being worked on." Also, consider where you (or identified subcontractors) can provide cross training for staff performing certain essential functions. Are you dependent on any key suppliers? What if they suffer a catastrophic loss? Consider identifying alternative supply sources.
- Segregation is a familiar concept to finance executives. A thorough review should be conducted periodically to make sure your internal controls are up to COSO standards. Take time to consider its use beyond the walls of the finance function. Consider the effects of losing one warehouse or office to fire. Are too many essential functions housed in the same location?
- Accident/Incident Investigation is the single most important step in preventing future losses. This does not mean filling out a claim form. It means treating every accident as a business threat requiring management action. The key to a successful accident investigation is to look for the management system breakdown that allowed the loss rather than assigning blame. Find out what management can do to prevent a similar incident in the future.

Finally, check with your insurance broker as to any loss control services your insurer may be able, or required, to provide. Many states require insurance carriers to provide loss control services to the insured.

Mitigation

What do you do when losses occur? Mitigate their impact. Following the occurrence of a loss, there is often a period of time where you can influence its financial impact. Consider the following.

- In the area of workers' compensation, a Structured Return-to-Work Program will get employees back to work quickly, potentially reducing total claim costs by 20% to 30%.
- Active claims management is essential. Early accident investigations and close contact with potential claimants to demonstrate your concern for them can be the difference between a lawsuit and a minor out-of-pocket resolution. Make sure those managing your claims are involved and innovative in their approach.
- Know when to fight and when to pay. There is wisdom in having a litigation manager on call to oversee large exposure claims and to monitor attorney billing.
- Provide outlets for employee frustrations and concerns – such as hotlines, an employee assistance program, or grievance teams. Employees whose frustrations are heard are less likely to sue their employer or have a questionable "work-related" injury.
- Fire sprinklers are the most common form of property loss mitigation. The cost of installation can often be fully recaptured over time through lowered insurance premiums. Keep detailed, fixed asset records – including assets that have been fully depreciated – for loss reporting.
- Familiarize yourself with your industry's laws and regulations concerning the loss of client data and information. Failure to notify clients of potential losses (a stolen notebook computer, for instance) can result in serious financial consequences.
- Regularly review and test systems, policies, and procedures associated with physical and electronic data retention, backup, and recovery. With the rapid growth of e-discovery as the newest weapon in the litigation arsenal, you must make sure your data retention policies are enforced.

- A Business Continuity Plan is essential. What will you do if you lose 30% of your workforce to the Asian Bird Flu? (Remember, epidemics affect an entire community, so replacing your workforce could be challenging.) What if a key office or manufacturing facility in New Orleans or Galveston is suddenly flooded and closed indefinitely? Much of the country is located in a danger zone for flood, earthquake, hurricane, or some other type of natural disaster – and all are now at risk for a terrorist attack. Money, which is all insurance provides, may not be enough to allow recovery from these types of major disasters.

Financing

The final step is financing losses. The easiest way is to purchase insurance with a zero deductible, which can be very expensive and is often fiscally irresponsible. Insurance can play a major role in any risk management program, especially for catastrophic coverage, but it's not the only option.

The cost of insurance is affected by more than cost of the risk itself. Other influences include the insurer's investment return (or lack thereof), and the cost of past losses that exceeded original expectations. The result is a cyclical market which can provide many entities with a good opportunity to consider retaining a greater level of risk.

Here are a few other items to consider.

- Review deductibles (or retained limits) and coverage limits carefully. The general rule of thumb for a deductible is to base it on the amount of coverage you can afford to pay without adversely affecting operations. The appropriate size of your deductible is largely dependent on the size of your entity; the cash reserves you have set aside; and, most of all, management's appetite for risk. A retained limit of \$500,000 or \$1,000,000 can save a lot in premium, but requires having a plan in place to pay for one or more losses of this magnitude.
- For large claims that simply must be paid, work with your attorneys to consider early disposition of structured settlements whenever possible.
- Add Hold Harmless/Indemnity clauses to all contracts, thereby transferring potential liability to the other contracting party. This applies to both service and construction contracts. Require the contractor to provide proof of coverage (Certificate of Insurance), and always make sure you are notified of cancellation. For extended contracts, develop a diary system to request updated

certificates when your contractor's insurance comes up for renewal.

- Additional insured endorsements from your contractor's carrier are always needed. They create a direct coverage relationship with the insurance company that allows you the same defense and indemnity as if you were the primary insured.
- Check the rating of your contractor's carrier and that of your own carrier. We recommend allowing only carriers with an AM Best rating of "A" or better. Unless you are very familiar with your contractor, do not hesitate to ask for audited financial statements. If they go bankrupt, any transferred liability could fall back onto your entity. One final note on purchased insurance: retain all policies forever.
- Set aside a reserve fund. The amount to set aside can only be determined after you have fully identified all potential risks. For high frequency risks, like workers' compensation and general liability, an actuary can assist in calculating the value of your expected liabilities below any purchased coverage.
- In some states, if you are large enough and have the appetite, you can file for a certificate to self-insure your workers' compensation coverage.
- Consider setting up or joining a single or multi-parent captive. This can provide tax advantages, but may have more expensive administrative costs.
- For entities too small to self-insure themselves, they can share their losses with other similar entities by joining a self-insured group for workers' compensation coverage. These are similar to multi-parent captives, but less costly to set up and administer. Joint and several liability is a concern, along with ensuring that the group's administrator is reputable and conservative. Many government entities have been managing their risk this way for decades.

A note about self-insured groups. While they can provide many advantages, they should be viewed as a long-term solution to managing risk. SIGs are not designed to beat market rates year after year.

Finally, always keep cash flow in mind. Structuring your investment of idle cash with an eye on risk is very important. After all, business continuity is essential.

While risk is unavoidable, disciplined attention to the foregoing principles can eliminate a lot of uncertainty and improve financial and operational performance. As General George S. Patton has said, "Take calculated risks. That is quite different from being rash."



Jeffrey C. Grubbs, CPA, MST
Chief Financial Officer
Bickmore Risk Services & Consulting

In his role as Chief Financial Officer, Jeff Grubbs oversees the financial management of the firm. Among his responsibilities are budgeting and forecasting; cash management; financial modeling; analyses of contract pricing, performance metrics; operational efficiencies; and contract negotiation. Jeff has 19 years of experience in the risk management industry that includes having served as Finance Manager and Assistant Treasurer for several JPAs and self-insured group clients. He currently serves as the General Manager of our Conservatorship Unit.

Jeff holds an MS in Taxation from Golden Gate University, and a BS in Accounting from California State University, Sacramento. He is a member of the American Institute of Certified Public Accountants, Vistage International, and Financial Executives International.



Bickmore Risk Services & Consulting

Corporate Office

1750 Creekside Oaks Drive, Suite 200
Sacramento, CA 95833

Industry Leaders in Risk Management and Self Insurance

www.BRSrisk.com

| 800.541.4591

Sacramento

Long Beach

Portland