

Powerful Insights. Proven Delivery.®



# The Name of the Game Is Risk: Secrets of the Winning Hand

*Enabling the Chief Risk Officer's Success*

FIRST IN A SERIES

**protiviti**®  
Risk & Business Consulting.  
Internal Audit.



## Introduction

---

GREAT POKER PLAYERS KNOW INSTINCTIVELY “WHEN TO HOLD ’EM AND WHEN TO FOLD ’EM.” THEY KNOW WHEN TO LAY BACK AND WHEN TO STRIKE FOR VICTORY. IN SHORT, THEY KNOW THE DISCIPLINE. WHILE IT’S IMPORTANT TO NOTE THAT EVEN THE MOST CONSERVATIVE AND SKILLED POKER PLAYER MOST LIKELY HAS A RISK APPETITE FAR IN EXCESS OF THE APPETITE THAT WOULD BE DEEMED PRUDENT BY MOST ORGANIZATIONS, THERE ARE LEARNABLE LESSONS AND ANALOGIES BETWEEN POKER AND THE ROLE OF THE CHIEF RISK OFFICER (CRO) OR RISK FUNCTION. WE PROPOSE THAT WITH SUCCESSFUL DEPLOYMENT OF THE FIVE SECRETS WE INTRODUCE, CROs WILL BE BETTER ABLE TO ADVISE MANAGEMENT AND THE BOARD WHEN TO PRESS FORWARD AND WHEN TO HOLD BACK, WHEN TO PASS ON SEEMINGLY GREAT OPPORTUNITIES, AND WHEN TO ACT WITH COURAGE AND CONFIDENCE.

---

Managing risk in the age of the financial crisis is akin to playing a poker game – success is tied to active risk/reward assessments and an honest sense of capability. Most great poker players, like most firms great at risk management, are not born but rather evolve. The psychological breakthrough for great poker players occurs when they admit, often after enduring a big loss, that they never truly understood the odds of the game they were playing. Poker players do not manage successfully to the odds early in their careers for several reasons, including underestimating the power of knowing the odds, having the fortune to win without a deep understanding, and simply not working hard enough to factor all available information to position themselves to understand the odds.

Like a poker player’s big loss, the financial crisis was a wake-up call for many chief risk officers (CROs), reinforcement of a vision for a few, and a lesson learned for all. CROs now realize that weak hands, falsely portrayed as better than they are, ultimately are called. And when a bluff is called in financial services, it’s not just the regulators that the institutions need to worry about – it is the marketplace, which may be even more important. In the financial crisis, shareholders paid a huge price and the taxpayers picked up the tab for the cost vis-à-vis bailouts for the weak hands.

Within their organizations, at conferences and through various disclosures in the media, successful CROs read the players at the table to determine who was sincere. They understood the odds when their firms took strategic chances like acquisitions and initiating new products such that they could support or oppose those initiatives. They knew to rely on timeless principles and not to follow strictly rules that others made and methodologies that others built. And while CROs can no more account for the exact level of all risks than a gambler can count cards in a double deck, they kept score of losses and established “what if” sessions with experts as a way to understand better how much the greatest risks might impact their institutions.

These CROs understood that a strategic focus on risk management is about attaining “first mover” status at critical market moments. Those financial institutions that were able to be “first movers” as the financial crisis approached now enjoy a longer-term competitive advantage over those institutions that weren’t. In summary, successful CROs upped their game and are now positioned to take steps to build on their vision, while other CROs have a unique opportunity to establish a new vision based on current realities.

Great poker players know themselves; they know instinctively “when to hold ’em and when to fold ’em.” While it’s important to note that even the most conservative and skilled poker player most likely has a risk appetite far in excess of the appetite that would be deemed prudent by most organizations, there are nonetheless learnable lessons and analogies between poker and the role of the CRO/risk function. With an understanding of the secrets of the winning hand, all CROs can foster a culture within the executive ranks and deep into the organization that integrates performance with risk. The winning hand eliminates wasteful practices in favor of pragmatic risk/reward techniques. Choosing not to embed a disciplined approach to risk management should not be an option in financial services, not when the chips are shareholder value that took decades to build and the rainy day stash of money that comes from taxpayers.

In this first installment in a series on the critical challenges faced by the CRO, we seek to define the secrets of the winning hand, secrets that are no more secret than techniques for how the great poker players manage to beat their competition. In subsequent installments, we will elaborate on each secret. While there is much talk about more oversight, more rules and regulations, increased transparency, and better governance, among many other issues, the question arises as to whether such changes will make a significant difference going forward. If the secrets we cite herein and intend to discuss further in subsequent issues of this series are not addressed, chances are the return on those changes will disappoint.

Consider that every large financial institution, whether it failed, struggled or weathered the storm, was subject to one or typically multiple regulators; had independent risk functions with scores or even hundreds or thousands of risk personnel; had invested tens if not hundreds of millions of dollars in technology infrastructure; was audited by both large internal audit functions and external audit firms; was reviewed by rating agencies, equity analysts and others; and produced expansive 10-K reports (e.g., Citi doubled the length to almost 300 pages and J.P. Morgan was up 100 pages to 253 from 2002 to 2009). So why didn’t this investment and activity make a difference for the industry as a whole? We believe lack of adherence to the winning hand secrets we are about to introduce is a primary reason.

As evidenced during the financial crisis, the degree to which organizations successfully apply these secrets will determine victory or failure when the chips are down and their cards are face up on the table. Time is of the essence. Defining the essential components of the winning hand, reducing wasteful spending, and improving performance such that the industry can recover from this crisis as quickly as it seemed to have plunged into it are at stake.

## KEY SUCCESS QUESTIONS

---

Our intent in discussing these secrets is to spark dialogue among directors and C-level executives on how to strengthen the contribution of risk management to the success of the enterprise. However, before describing the secrets, we should define success. A CRO has the winning hand when he or she can answer five straightforward questions:

1. Are the organization's performance objectives at risk of not being met and, if they are being met, are they being met in a manner consistent with the organization's overall risk appetite?
2. If at risk, which objectives are at risk, ranked by order of the greatest risk of not being met, and why?
3. Have actions been defined that will sufficiently mitigate risks to an acceptable level?
4. If not, what are the recommendations for executive management's consideration:
  - a. Change tolerances,
  - b. Lower performance expectations,
  - c. Change investment budgets,
  - d. Change objectives, or
  - e. A combination of the above?
5. When the crucial moment comes where an unacceptable situation must be called out:
  - a. Will risk management be able to tell the full story to decision-makers who matter?
  - b. Will the decision-makers listen?
  - c. Will risk management be allowed to continue to function once access rights are exercised?

The expert poker player is concerned with the risk of opponents getting good cards while he or she receives bad cards. But what constitutes how good or how bad a card is depends on the player's appetite to win balanced by his or her tolerance for losing. A marginally bad card for one poker player could be a good card for another (all things equal); it's not simply deciding on how good or bad an individual card is, but rather how consistently the player manages to his or her appetite to win and tolerance for losing. Similarly, the Key Success Questions balance the risk appetite for meeting defined objectives with the tolerance for sustaining losses in the pursuit of winning. The secrets of the winning hand must enable meeting performance objectives within a pre-specified and organizationally specific tolerance for losses resulting from expected setbacks (cost of pursuit) and unexpected losses (risk).



# Secrets of the Winning Hand

---

WHEN IT COMES TO EXPERT POKER PLAYERS, THEY KNOW THAT HOW GOOD THEY THINK THEY ARE HAS NOTHING TO DO WITH THE OUTCOME OF THE GAME. THE SECRET IS THAT THEY ARE HONEST WITH THEMSELVES ABOUT THEIR CAPABILITIES BEFORE GOING INTO A GAME AND HAVE ESTABLISHED MENTAL THRESHOLDS BY WHICH THEY WILL ABIDE TO GOVERN THE EXTENT OF THEIR LOSSES IN RELATION TO HOW MUCH THEY SEEK TO WIN – THAT IS REAL INTEGRITY.

---

So, what are the secrets? What select few concepts promote behaviors that will give the CRO the best chance to have a winning hand? Our experience and research suggest that there are five fundamental tenets that the truly successful CROs have established within their organizations that enable success in good times and bad.

1. Integrity to the Discipline
2. Constructive Board Engagement
3. Effective Risk Positioning
4. Establish a Learning Culture
5. Set Appropriate Incentives

## 1. INTEGRITY TO THE DISCIPLINE

---

The most pervasive secret for success in risk management is integrity to the discipline. Integrity means having a clear grasp of business realities and being truthful to the board and executive management about the needed risk capabilities that will maximize the chances of achieving your organization's objectives while protecting enterprise value. When it comes to expert poker players, they know that how good they think they are has nothing to do with the outcome of the game. The secret is that they are honest with themselves about their capabilities before going into a game and have established mental thresholds by which they will abide to govern the extent of their losses in relation to how much they seek to win – that is real integrity. There are many things that are done in organizations that bypass this first secret. Consider the following common examples, some strategic and some tactical, of integrity failures:

- **Failure to grasp business realities clearly** – The global financial crisis is a good example of what can happen when the inherent risks associated with aggressive, growth-oriented market strategies are discounted, ignored or never considered. The root causes of the industry's staggering losses from subprime mortgages are many – breakdowns in time-tested underwriting standards, failures to provide or obtain adequate disclosures, and excessive reliance on third-party assessments of structured products, to name a few. But not every financial institution played the subprime game at the same level. The firms

that succeeded in minimizing their losses not only understood that a pervasive deterioration in the housing market would be devastating to large portfolios of subprime loans, but they also took proactive steps to monitor the market. For example, some firms identified the sources of significant risk as early as mid 2006 and had up to a year to evaluate the magnitude of the risk and implement cost-effective plans to reduce their exposure. Skeptical of third-party assessments, other firms developed their own in-house expertise to assess credit quality. Some even tested their assessments by selling a small percentage of assets to obtain reliable pricing data points. These and other actions resulted in a significant redirection of market focus and gave the firms a seat in the ring when the proverbial music stopped, leaving less fortunate competitors standing as the market collapsed.

- **Failure to understand what “risk” is in the first place** – Based on our experience, many firms struggled with their risk programs because of confusion as to exactly what constitutes a risk. They saw risk as isolated threats requiring tactical solutions rather than a numerical value of unexpected loss. Identifying threats is certainly important for defining a register of what could go wrong and assessing the quality of the supporting control environment; however, that exercise is not where risk management ends but rather where it begins. The secret is to link threats to risk such that the relationship between overall risk, including capital, is aligned with day-to-day management of threats (sometimes referred to as risk factors or sources of risk). A true understanding of these differences and the intrinsic relationship between risk and threats allows CROs to build effective risk programs where terms like appetite and tolerance have meaning and differences in responsibilities with compliance, internal audit, Sarbanes-Oxley and other second-line-of-defense groups are defined. CROs who say they are managing risk when they are only managing threats and/or not linking threats to risk lack integrity to the discipline whether they want to acknowledge it or not – the difference may seem subtle but the implications can be significant.
- **Failure to tie risk tolerance to performance** – How often has the question been asked, “Are we over-controlled or under-controlled?” We see organizations ask these questions without realizing that they haven’t established the benchmark of risk tolerance. That risk tolerance is essential to effective management is a well-known and widely accepted tenet of risk management, but it was all too frequently forgotten by firms that notably struggled during the financial crisis. How would you even know that you are doing an efficient job of managing risk when you don’t know how much risk is tolerable? Integrity to the discipline of risk management means declaring the obvious – that performance and risk must be integrated and defining thresholds is essential. Asking employees to perform risk and control assessments that never tie to tolerances is a waste of time and money for the CRO who wants a winning hand, as illustrated by the fact that the first Key Success Question listed on page 4, regarding whether performance objectives are at risk of being met, cannot otherwise be answered. In fact, our experiences indicate that too many risk professionals are not fully aware of what the expected performance levels of a product line or division are, much less how much loss in their pursuit is tolerable. Surely, a poker player considers risk tolerance with each bet placed; so, too, should CROs with the winning hand.
- **Failure to deploy risk management fully by limiting it to a compliance activity** – Spending considerations for most projects typically require one of four general reasons for management approval:
  1. Revenue generation
  2. Cost mitigation
  3. Brand protection
  4. Regulatory requirements

The successful CRO requests funding for projects for any reason but regulatory. Stating that the need for funding is to meet regulatory requirements alone passes the buck at worst and marginalizes the project at best. If a risk management project request does not objectively improve revenue performance, lower costs or protect the brand, then in almost all circumstances it should not be done as part of risk management. Perhaps it should be done as part of a compliance effort or not done at all. Integrity to

---

INTEGRITY TO THE DISCIPLINE FOLLOWS FROM A STRONG TONE AT THE TOP... AN OFTEN OVERCITED BUT CRITICALLY VITAL ELEMENT THAT ULTIMATELY DEFINES THE IMPORTANCE AN ORGANIZATION PLACES ON RISK MANAGEMENT. IF IT IS LACKING IN ANY SIGNIFICANT WAY ... RISK MANAGEMENT FACES AN ALMOST INSURMOUNTABLE CHALLENGE TO MAKING A DIFFERENCE.

---

the discipline means knowing that undertaking initiatives to manage uncertainty (risk) in the pursuit of business objectives is not a regulatory requirement. The “regulatory” checkbox is too often used as a cop-out. No question, there are times when an organization has to make changes – anti-money laundering measures, for example. In such instances, compliance should run and own the initiative, not risk management. Alternatively, the lines of business should view the initiative as a necessary process that protects and sustains the brand by doing business with reputable customers.

These examples illustrate that integrity must permeate every aspect, every level and every action within the organization as it relates to risk management. The critical assumptions underlying the corporate strategy must be understood at the highest levels of the institution and the external environment monitored to ensure that these assumptions remain valid over time. Managing risks and managing threats are not the same thing. Risk is the uncertainty of loss or impairment of ability to meet performance objectives related to credit, market, operational, liquidity, strategic and reputational goals. Hoping that risk management is implemented sufficiently while knowing that business realities are not actively monitored, risk is not understood, tolerance levels are not set, or projects are performed solely to meet regulatory guidelines is an indicator that integrity to the discipline is lacking.

Integrity to the discipline follows from a strong tone at the top – what the CEO stands for, how he or she provides leadership with respect to the appropriate governance, control and behavior around doing the right things in the right way, and ensuring the affairs of the business are conducted in a transparent manner and at arm’s length. Tone at the top is an often overcited but critically vital element that ultimately defines the importance an organization places on risk management. If it is lacking in any significant way and the executive team isn’t paying attention to the warning signs when they are posted, then risk management faces an almost insurmountable challenge to making a difference.

## 2. CONSTRUCTIVE BOARD ENGAGEMENT

---

The second secret is constructive board engagement. Board members who demand integrity know that everyone in the organization is, by definition, accountable to them. Board members must be constructively engaged such that they are able to exercise their judgment as to the changing risk profile in the context of their companies’ performance objectives. Successful poker players know everything that is going on at the table. They are not judgmental, but rather extremely discriminatory. The best poker players discern actions, words, tempo; they make it their business to estimate the other players’ ability to take a financial loss and personal embarrassment – any piece of information is weighed and considered in this context. They are engaged. So should board members be.

Could boards have made more of a difference in staving off the financial crisis? As the debate over this question continues, the focus turns to the future. Through the risk oversight process, the board:

- Obtains an understanding of the risks inherent in the corporate strategy and the risk appetite of management in executing that strategy,
- Accesses objective information from internal and external sources about the critical assumptions underlying the strategy,

---

THE GREAT POKER PLAYERS CONSTANTLY CHALLENGE THEMSELVES ON WORST-CASE SCENARIOS; THEY ARE THEIR OWN DEVIL'S ADVOCATE. SUCH A CYNICAL VIEW FORCES CRITICAL THINKING AND SHIFTS ENERGY TO OPTIMAL PERFORMANCE.

---

- Is alert for organizational dysfunctional behavior that can lead to excessive risk taking, and
- Provides input to executive management regarding critical risk issues on a timely basis. If directors lack the industry knowledge and expertise to carry out these responsibilities, the risk oversight process will not be effective.

The board is handicapped in terms of providing effective risk oversight if:

- The composition of the board membership is not conducive to accumulating sufficient knowledge of key industry and business issues giving rise to risk.
- Directors do not develop their own independent views of risk by obtaining other sources of insights rather than relying solely on management's understanding of the firm's risks.
- Directors aren't asking the tough questions about risk and risk management.
- Directors can't get the information they need to make critical decisions because the company's ability to effectively measure and report on key risks is limited.
- The board is inundated with *too much* data and information, making it virtually impossible for directors to sift through the mountain of paper to unearth the key nuggets of insight.
- The board is engaged by executive management after key decisions are made rather than in a timely and appropriate manner.
- Risk is an afterthought to strategy and risk management is an appendage to performance management.

The "information for decision-making" issue cannot be emphasized enough. Boards are often overwhelmed with reporting yet frustrated by the organization's inability to measure and report on risks and the greatest sources of, or threats to, performance limits. Therefore, effective and insightful risk reporting is vital to constructive board risk engagement.

### 3. EFFECTIVE RISK POSITIONING

---

The third secret is effective positioning of the risk management organization. These are the people responsible for executing the risk program and for providing another line of defense. No other group in the organization has the charter or luxury to view performance exclusively from a risk perspective – not internal audit, not compliance, not executive or line management. The secret is not simply to have a risk management organizational structure with names in boxes, but rather to have knowledgeable professionals take an objective, often contrarian, perspective without repercussions to their compensation and careers, a perspective that is appreciated and expected. Quite simply, the question is whether risk management is positioned to be successful within the organization. CROs with successful programs achieve a level of collaboration between business and risk teams unattainable by their less fortunate peers.

The outcome of collaboration between risk professionals and line managers should be value-added in the forms of both tangible contributions to performance-oriented decisions and perceived benefits resulting from insights not otherwise considered. The great poker players constantly challenge themselves on

worst-case scenarios; they are their own devil's advocate. Such a cynical view forces critical thinking and shifts energy to optimal performance. When risk professionals are excluded from key decision points or their thoughts are dismissed with little regard, either line management does not have the organization's best interests in mind or the risk professional is a poor communicator of his or her value, or both. Couple this issue with the board not being sufficiently engaged and you've got an organization lacking the benefit of a true risk perspective. Perhaps business line managers view risk professionals as compliance functions – clearly a fatal flaw in risk management.

At the crucial moment when someone must play a contrarian role to protect the shareholders' interests, how can a CRO who is paid to manage uncertainty ever stand down a CEO who is driven to achieve performance goals at any cost when the CEO controls his or her career progression, salary and bonus? And, if the CEO doesn't believe in the value of risk management – game over, as risk didn't have a seat at the table when it mattered. That's akin to a poker player betting without concern for the odds. While risk team positioning is certainly related to the first secret around integrity to the discipline, the secret here is to establish an organizational structure that enables collaboration and leads to a risk culture desired by the board. The CRO must have an equal seat at the table.

Elements of ineffective positioning include:

- The CRO is not viewed as a peer with business line leaders in virtually all respects (e.g., compensation, authority and direct reporting to the CEO) and likewise down through the business hierarchy.
- The CRO has no direct reporting line to the board.
- The board, senior management and operating personnel believe that managing risk is a single person's or function's job and is not an organizational imperative or everyone's job.
- The CRO faces constraints in reporting to the board.
- The CRO is entangled in the minutiae of managing compliance.
- The CRO is constantly fighting turf issues.
- Management does not value risk management as an equal discipline to opportunity pursuit, or sees it as a necessary compliance function, or worse, as a blocker to getting things done.
- There is a lack of clarity or definition in the CRO position and how it interfaces with senior line and functional management.

One or more of these elements may signify a red flag that the CRO, or an equivalent executive, is unable to fulfill the strategic demands of the job and lacks real authority or influence. As a result, risk management may be set up to fail.

## 4. ESTABLISH A LEARNING CULTURE

---

The fourth secret is establishing a learning culture with regard to risk. The successful CROs reached a point, at least within key pockets of their organizations, where blaming individuals for failures gave way to recognition that we all learn from mistakes with a focus on improving policies and processes continuously over time. Mistakes can only be acted upon and shared across the company when they are discussed, not hidden. Postmortem analysis of key losses, near misses and control failures can often be one of the most valuable exercises an organization can engage in. CROs need centers of excellence, not protocols for punishment.

Blame almost always leads to rationalizing away critical opportunities to learn from mistakes and to protect the organization in the future. Programs that reward disclosure of close calls and encourage scenario sessions reap benefits many times over the cost to conduct such activities when done properly (and we've seen many that are not done properly due to a lack of integrity to the discipline). Unfortunately, many institutions belittle capturing close calls or near misses, resulting in an inability to be proactive. These organizations rob themselves of unique opportunities to learn and to improve policies and processes. The great poker players are smart, witty and seemingly impulsive at times; they are this way because they are aggressive learners poised to take advantage of each turn of the cards. They cherish near misses and learn from them, using them to improve their game.

Learning should never be confined to within. Sometimes the best lessons are learned by others external to the organization, particularly when the lessons are publicly disclosed. Lessons learned by others provide the opportunity for CROs to apply the circumstances to their own companies. Too often we have heard executives talk about why something “can't possibly happen here” or “we're different” without fully analyzing the circumstances and root causes to determine how applicable such events can be to their own organizations.

While learning is fun and motivational, creating an environment where people and teams disclose failures, weaknesses and shortcomings is difficult. Successful CROs paint a long-term picture of reward and performance, not a short-term picture of punishment and risk. Many of us who have played or watched poker games see the best players continuously evaluating risk, learning from every play and sizing up their opponents while keeping their attitudes positive and their moods steady. They learn from every movement and from each pause. Risk management permeates the fabric of the poker player like safety has come to permeate the fabric of aviation. The successful CROs find a way to have risk management become woven into daily activities and welcomed as part of the agenda of all important meetings.

## 5. SET APPROPRIATE INCENTIVES

---

The fifth secret is setting appropriate incentives. Incentives are not established simply to pay for attention to risk but rather are intended to recognize individuals, divisions and the enterprise for heightened risk awareness behaviors in the context of pursuing performance goals. Incentives are also reviewed to ensure they do not drive behavior that results in unacceptable risks. The old saying, “What gets rewarded, gets done,” is as true with risk as with any other activity. This secret falls last on the list because the program that begins with integrity to the discipline and ends with rewarding people for the desired behaviors has in place the bookends that depict the winning hand. The behaviors needed for successful risk management seem obvious but are often missing, such as collaboration, forthcoming of failures and long-term focus – so, too, are incentives related to these behaviors.

This “secret” is certainly not a surprise, yet risk management is often poorly incented and misunderstood by human resource departments, which are often involved in establishing incentives. In today's fishbowl

---

DISCONNECTS IN THE ORGANIZATION'S COMPENSATION STRUCTURE AND AN EXCESSIVE NEAR-TERM FOCUS CAN LEAD TO THE WRONG BEHAVIOR, NEUTRALIZING OTHERWISE EFFECTIVE OVERSIGHT BY THE BOARD, THE CRO AND OTHER EXECUTIVES.

---

environment, when shareholders, politicians and regulators alike are focusing on incentive compensation as if it were a lightning rod, it is critical to avoid:

- Large amounts of cash compensation from short-term activities driving growth and transaction volumes without regard for the risks arising from such activities and the potential consequences from the longer-term tail risks, and
- Compensation structures that allow for management payouts to get significantly out of balance with long-term shareholder returns.

The new proxy enhancements issued by the Securities and Exchange Commission take steps to create transparency that encourages a more balanced compensation structure.

Disconnects in the organization's compensation structure and an excessive near-term focus can lead to the wrong behavior, neutralizing otherwise effective oversight by the board, the CRO and other executives. For example, if lending officers are compensated based on loan volumes and speed of lending without regard for asset quality, reasonable underwriting standards and process excellence (e.g., their compensation is not adjusted for borrower and collateral riskiness, portfolio concentrations and the likelihood of unexpected losses), the institution may be encouraging the officers to game the system to drive up their compensation and, thus, exposing the company to unacceptable credit risk. The question arises as to whether these disconnects remain part of the landscape given recent experiences, correlating them with unacceptable concentrations of market, credit, liquidity and other exposures that accumulate over time. For this reason, understanding the impact of the compensation structure on risk taking in financial services will likely be a priority for all stakeholders for some time. Too often, attention is placed at the top of the house on C-suite executive compensation and upper management. However, just as important is an understanding of the incentive plans driving behavior on the "factory floor" where production occurs, as this is where the individual "moments of truth" occur that add, subtract or neutralize the buildup of risk within the organization, each and every day.



## First Steps to Building the Winning Hand

We believe an understanding of the secrets is fundamental to forming a clear vision and road map of risk management. When risk management infrastructures are built to provide transparency and insight, are enforced by those ultimately accountable, and truly reward employees who pursue performance goals mindful of risk tolerances, CROs have a winning hand.

Following are examples of activities intended to reaffirm or re-establish the risk management function in light of the five secrets of the winning hand:

1. **Current and Future State Gap Analysis** – Conduct a current and future state gap analysis to define the value proposition for improving risk management.
2. **Risk Culture Analysis** – Conduct a risk culture analysis to determine whether the board of directors, executive leadership and company personnel in lines of business and key corporate functions all see the organization's risk culture the same.
3. **Common Risk Language Development** – Based on a true definition of risk (delineating the intrinsic relationship between risk and threats), develop a risk language that inventories the common risks (e.g., credit, market, operational, etc.) germane to the business as well as a register of sources of these risks (i.e., threats that give rise to risk).
4. **Risk Organizational Structure Analysis** – Perform a risk organizational structure analysis to understand the strengths and limitations of the current organizational structure and the alternatives for improving it.
5. **Measurement and Reward Structure Analysis** – Execute a measurement and reward structure analysis to address the current compensation structure, particularly in light of the forthcoming regulatory expectations.
6. **Board Risk Oversight Agenda Evaluation** – Evaluate the board's oversight agenda in terms of its effectiveness in overseeing risk and risk management, and particularly focusing on the clarity and content of board risk reporting.

Following are examples of key outcomes resulting from re-energizing the risk management function:

- Crisp policy structure setting forth clear accountabilities and establishing clear ownership over key risks, eliminating gaps and overlaps
- Tone set for valuing risk management the same as opportunity-seeking behavior, and communication protocols established to facilitate sharing of bad as well as good news
- Risk committee or other oversight structure in place along with a CRO, or equivalent executive, effectively positioned for success
- Reward system in potentially risky areas aligned with longer-term performance, with managers historically rewarded based on volume and growth metrics also held accountable for the risks inherent in their respective business activities driving those metrics
- Enterprise risk assessment process in place using a common risk language, including customized risk definitions

---

IF RISK IS AN AFTERTHOUGHT TO STRATEGY AND RISK MANAGEMENT IS AN APPENDAGE TO PERFORMANCE MANAGEMENT, THE BOARD'S OVERSIGHT ROLE WILL BE DIFFICULT TO FULFILL AND THE CRO'S ROLE LESS RELEVANT.

---

- Using the common risk language or inventory to drive robust “enterprise risk dialogue” over strategic and operating plans, product expansion, and other key performance-enhancement tactics
- Board organized for risk oversight with board-level risk management skills leveraged, specifically as related to the industry and specific key business risks

Activities that are traditionally the focus of risk programs, such as policies, frameworks, analytics and reporting, fall into place when all five secrets are built into the program. A winning hand has the benefit of improving relationships with regulators and clarifying funding priorities. While the time period of evolution of the best risk programs is measured in years, the sense that the organization is on the right path comes quickly. The tone at the top becomes less of a concern because the culture in the middle is aligned with a performance and risk-integrated management methodology.

## SUMMARY

---

In this initial release of our “CRO Series,” our intent is to introduce the secrets of the winning hand that we believe must be addressed to ensure that risk management is an effective contributor at the table in managing the business. Our purpose is to help organizations build a winning hand where “winning” is defined as making risk management a strategic contributor to the organization’s success. In the future, we plan to issue separate discussion papers on each of the secrets to illustrate the evolution of risk programs applying them.

Our objective is to contribute to the dialogue among directors and executives on how to make meaningful progress in addressing risk issues and provide a basis for formulating commonsense solutions. Given that these issues have been around a long time and continue to fester and be realized at least every decade or so, our hope is that this and subsequent discussion papers will assist more organizations in making progress toward addressing them.

If risk is an afterthought to strategy or risk management is viewed as an appendage to performance management, the board’s oversight role will be more difficult to fulfill and the CRO’s role will be less relevant. If the organization is drowning in data without any real information and interpretive insight, or there aren’t any risk-based measures of return or profitability, or there is an inadequate postmortem on significant loss events with the attendant failures to understand, learn and make process adjustments, there will be insufficient value add from the risk reporting process. If there is a lack of crisp key risk indicators and trending measures and/or an emphasis on using short-term horizons when looking forward, it will be difficult to answer the Key Success Questions. We seek to help CROs know and articulate whether their companies are riskier today than yesterday, as well as why and how the underlying risks are trending.

As we have suggested with our analogy, great poker players know “when to hold ’em and when to fold ’em.” They know when to lay back and when to strike for victory. In short, they know the discipline. We propose that with successful deployment of the five secrets we have introduced, CROs will be able to advise management and the board when to press forward and when to consider holding back, when to pass on potentially great opportunities, and when to act with courage and confidence. Choosing not to adhere to one or more of the secrets should not be an option, not when the chips are hard-earned shareholder value, brand image or reputation, or even the money of taxpayers who fear being forced to fund the kitty through bailouts again. Time is of the essence. The stakes are high but the secrets are out.

## About Protiviti

---

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

### About Our Financial Services Industry Team

We assist financial services companies in identifying, measuring, and managing the myriad risks they face. With our commitment to service, people, resources, and values, we are the service provider of choice for financial institutions of all types and sizes.

Our consultants are experienced professionals. Many have decades of experience working in the financial services industry. Located in offices across the globe, they include former industry executives, former regulators, and a broad range of subject-matter experts who have first-hand knowledge of the issues on which they provide advice. Our internal commitment to training ensures that our consultants remain current on important industry issues. Armed with tested tools and methodologies, our consultants provide pragmatic, cost-effective and value-added solutions to your company.

At Protiviti, we understand the challenges faced by financial services companies. Our solutions are designed to help your company turn these challenges into competitive advantages.

### Contact

Carol Beaumier  
Managing Director  
+1.212.603.8337  
[carol.beaumier@protiviti.com](mailto:carol.beaumier@protiviti.com)

Cory Gunderson  
Managing Director  
+1.212.708.6313  
[cory.gunderson@protiviti.com](mailto:cory.gunderson@protiviti.com)

Giacomo Galli  
Managing Director  
+39.02.6550.6303  
[giacomo.galli@protiviti.it](mailto:giacomo.galli@protiviti.it)

### Acknowledgements

We thank Jim Ryan, Cory Gunderson and Jim DeLoach for leading the project to develop this white paper.