WHAT THE R*SK!™

EXPOSING BUSINESS BLIND SPOTS

BONUS FOR *BLIND SPOT INSIDERS*

EPISODE 102

Foundations of Risk Management

BY

LAWRENCE GORDON, CAMS

---

www.RiskBlindSpots.com

CONTENTS

ABOUT THE AUTHOR

Lawrence Gordon, CAMS

With nearly 30 years in financial services at organizations ranging from large banks to FinTech start-ups, and leadership experience across multiple areas of risk, I wanted to take that knowledge and empower you to see where your business blind spots might be and learn how to expose and address them.

As a fractional Chief Risk Officer for operating companies and a risk consultant for financial institutions through Gordon Risk Solutions, I leverage my executive leadership roles across the three lines of risk defense in financial services. I also developed training programs to build strong cultures of compliance.

My holistic view of enterprise risk is rooted in a diverse risk background. My background includes credit knowledge (making commercial loans as a wholesale lender to leading Credit Review departments evaluating thousands of transactions), building risk management programs de novo, and leading regulatory compliance and financial crime programs (Bank Secrecy Act, OFAC (Sanctions), and fraud).

Please Follow on LinkedIn.
https://www.linkedin.com/in/larryjgordon/
https://www.linkedin.com/company/what-the-risk/

FORWARD

Thank you for being a Blind Spots Insider.

We hope you find the information in this **WHAT THE R*SK!** Episode 102 E-Book valuable. This companion guide provides information about the foundational aspects of risk management. We have included graphics and worksheets to use as you identify, size, and manage risk.

You are encouraged to use this episode and e-book as an ongoing reference during your risk identification journey.

This e-book covers the identification and sizing of risk. We start with what Risk IS and IS NOT, followed by nine characteristics of a strong risk culture with examples of Red Flags to watch out for.

The *How to Measure Risk* and the *Application of Risk Measurement* chapters provide tools and a framework that can be applied as you build out your company's risk management program.

We are glad you have joined us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "*I've got this!*" victories.

CHAPTER I

PERCEPTIONS OF RISK MANAGEMENT

We need to start the discussion about the foundations of risk management by level setting perceptions about risk management activities.

Perception matters. Risk Management functions are often associated with the role of "Doctor No!" In a business setting, Dr. No is the evil character that works against the sales force of an organization. This perception is perpetuated from an experience when someone in a Risk (or Legal) department told the sales team "No" when they asked permission to do something that they wanted to do.

When an organization has a strong risk management culture, the relationship between Sales and Risk should not be viewed as an obstacle, but as empowering a business to thrive and generate sales within safe, risk-based parameters or guardrails. Think of it as a prescriptive way NOT to be on Reality TV as a potential news headline OR the next business school case study about a company downfall.

What risk IS and what risk IS NOT:

- Risk is NOT the job of only one person. Everyone in the organization needs to understand that they have responsibility of identifying risk and working through the company's program structure to appropriately address it.
- Risk is NOT a "check-the-box" exercise, neither is monitoring dashboards. Committing time to assess various risks is important.
- Risk is NOT static. It is dynamic and evolving, sometimes based on market conditions and events.
- Avoiding the Risk Management process is NOT a viable risk management plan. Ignoring or avoiding situations, some call this the ostrich method, DOES NOT WORK.
- Risk management is NOT a "one-size-fits-all" process. The most effective way to measure or monitor risk will depend on the specific context and nature of the risks involved. We will cover this in the MEASURING RISK portion of this episode.
- A Risk Assessment is NOT an audit.

When risk management is done correctly, you may not be able to quantify the benefits or savings.

...When it is NOT done correctly, you will know exactly how much risk management could have saved you after an event.

- Risk tolerance (what kind and magnitude of risk is acceptable) IS organization specific and will help drive your risk-based decision-making process.
- Risk management IS NOT *limited* to utilizing risk dashboards.

Driving a business is like driving a car.

Don't get me wrong. Dashboards are valuable. In both a car and managing your business there are metrics that should absolutely be monitored on a "dashboard." Dashboards are designed to monitor what is currently happening or has already happened. In business, dashboards are built based on the size and complexity of the operation.

Here is the big "HOWEVER"...ONLY looking at the dashboard while driving a car is a disaster waiting to happen. It is a matter of when, not if, you will hit a "friction point." Risk leaders, like good drivers, should spend most of their time looking out of the windshield, windows, and mirrors to identify and navigate obstacles (i.e., manage the risks). The ability to identify obstacles, be anticipatory of events, and plan for any potential adjustments to meet objectives will always lead to better outcomes.

The greatest potential risk when driving a car comes from difficulty monitoring the blind spots just over the driver's shoulders. This may not be the direction we need to look at the most, but we do need the right visibility when the time comes. Newer vehicles are now equipped with blind spot detectors on the side mirrors, cross-alerts, lane departure, and surround cameras. All of these technologies help expose driving blind spots.

Similarly, this podcast is designed to help **Expose Business Blind Spots**.

Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.

- Risk management is NOT sexy. If done correctly, you may not be able to quantify the benefits or savings. However, when an adverse event materializes and you have not done it correctly, the potential consequences can be operationally, financially, or reputationally significant. At that point you will know exactly how much risk management could have saved you.
- There IS a difference between risk-management and risk-avoidance.

Risk Management versus Risk Avoidance

Consider this life example: Your child wants to walk to their friend's house on the other side of the neighborhood by themself for the first time. While you are proud of your child's desire for independence, this is a transition point for both of you. Your choices are to not let them go (risk avoidance), take them by car to the friend's house yourself (risk avoidance except for your car trip), or to teach the child how to safely cross streets, follow a planned path, and steer clear of stranger danger. The latter is a risk-management strategy.

From a more technical perspective...risk management is an approach that involves identifying, assessing, and mitigating risks along with continuous monitoring. It aims to minimize the impact of potential risks while allowing for reasonable risk taking.

Risk avoidance, on the other hand, focuses on eliminating or steering clear of risks entirely. It involves consciously deciding not to engage in activities or situations that carry significant risks. Strategies for risk avoidance include eliminating, abstaining, or substituting risky elements.

If you are the parent in the above analogy, you want to be thoughtful and evaluative without overlaying unnecessary or unrelated bias in your risk approach.

As a business leader, a banker, or as an investor, it is in your nature to seek a higher return on your investment or resources by actually taking risks. So think about activities with a risk management lens rather than perceive a risk program as just risk avoidance.

CHAPTER II

CULTURE OF RISK MANAGEMENT

What does a strong risk management culture look like? What characteristics would demonstrate that an organization has a mature risk management program?

Overall, a strong risk management culture is one that promotes a holistic approach to risk management, is supported by effective policies and procedures, and is embedded in the organization's values, vision, and mission. Here are nine characteristics and common Red Flags. Keep in mind that these are just some examples of red flags. There are many more.

Tone from the top: A culture of risk management starts with the tone from the top. This means that senior leaders of the organization demonstrate a strong commitment to risk management and set an example for others to follow.

- **Red Flag**: If management talks about one person that is solely responsible for risk management, it is not in the culture of the organization. If the one person is not an executive officer, it may be viewed as a "check the box" activity.

Clarity of roles and responsibilities: There is clear understanding of roles and responsibilities related to risk management throughout the organization, including the Board of Directors, senior management, risk management staff, and business line staff. Roles and responsibilities can be defined through job descriptions and committee charters.

- **Red Flag 1**: There is no risk management experience on the Board of Directors or there are no standing Board agendas to discuss risk management topics.

- **Red Flag 2**: Discussions with employees about general or role-specific risks that they have in their job results in a "deer-in-the-headlights" response. This means that they do not understand the impact that their jobs could have on the organization and may not recognize a problem early enough for it to be addressed.

Effective communication: Indicators of effective communication include risk management policies, procedures, and requirements throughout the organization, including committee/working group activities, regular training, and awareness programs.

- Red Flags: 1) Policies that appear to be cut/paste from an online source without being customized for the organization. 2) Simplistic procedures that allow for interpretation and inconsistency of desired outcome.
  - Policies, when applicable, should leverage industry, state, or Federal regulations to ensure they are appropriate for the organization.

Policies and Procedures

Think of Policies as the "What" documents that establish the overall direction, principles, and expectations of an organization. Example: "Our company will comply with this Regulation."

The Procedures are the "How" documents that provide detailed instructions and guidelines for carrying out specific tasks or activities in a standardized, consistent, repeatable, and reproduceable manner. Example: "This is how we specifically process each customer in order to comply with the Regulation."

Policies set the framework, and procedures define the operational implementation.

The Great British Baking Show provides a great motivational example to develop good procedure documentation.

Great Procedures Lead to Consistent Outcomes

Businesses need to focus on the importance of having very clearly documented procedures. A great demonstration of this can be found on "The Great British Baking Show" (known as "The Great British Bake Off" in the UK). Each episode has a segment called the "Technical Challenge."

In the Technical Challenge, the bakers are presented with a recipe for a specific baked item, such as a cake, bread, pastry, or dessert. The recipe provided is often incomplete or lacking in specific instructions, requiring the bakers to rely on their baking knowledge, skills, and intuition to fill in the gaps and produce a successful outcome. This challenge tests their ability to follow instructions, adapt to unfamiliar recipes, and showcase their technical proficiency in baking.

Away from the contestants, the hosts show the audience how the final product is supposed to look and taste along with any skill applications that are particularly challenging.

Even though each of the contestants has all of the raw ingredients to be successful, very rarely does a contestant get it perfect because of the incomplete instructions. In fact, at the judging table with all of the contestant entries lined up, there is a visual difference and a wide variance across the contestants' final products.

Too often procedures are less than complete, like in the Baking Technical Challenge, which leads to a wide variance of outcomes. In the Six Sigma world "Variance is the Enemy!"

Set your teams up for success by providing specific step-by-step details, pictures, etc. so each time the procedure steps are completed they are perfect.

Data-driven decision-making: Risk management decisions are based on accurate and timely data that is analyzed and effectively interpreted.

- **Red Flag**: When there are too many decisions being made without facts or verifiable information. Strategic plans and organizational decisions made this way means that there is little basis for such decisions. Some people call these SWAG (Someone's Wild Ass Guess) decisions.

Continuous improvement: A strong risk management culture is one that is constantly looking to evolve and improve its risk management practices through ongoing monitoring, evaluation, and feedback.

- **Red Flag**: Comments like "Our program was put in place a while ago and has been working fine." Or "If it ain't broke, don't fix it." This indicates that management is not adjusting to changing risks.

Risk awareness: All employees are aware of the risks associated with their role and are empowered to raise concerns when necessary.

- **Red Flag 1**: Having someone working in a potentially risk-impactful area state that they do not escalate issues "because management knows what they want done." This indicates that there is a communication barrier that likely has multiple root causes. This can be the direct result of a manager that does not want feedback about a potential significant risk, and an employee that felt uncomfortable escalating an issue up the chain of command.

- **Red Flag 2**: An employee's lack of confidence in their ability to understand a real risk, which can be rooted in a lack of training.

- **Red Flag 3**: Risk management principals are not formally addressed during employee performance evaluations as a reinforcement of corporate priorities.

Accountability: Individuals and teams are held accountable for managing risks within their areas of responsibility, and there are consequences for failing to do so.

- **Several Red Flags**:
  - When there is no process to test or monitor activities.
  - When there is no process to allocate costs associated with a loss.
  - When there is no forum to learn from mistakes. This is a valuable learning opportunity for employees to work with their leaders to understand the mistake and correct for the future.

Flexibility: A strong risk management culture has flexibility to respond quickly and effectively to changing market conditions, regulatory requirements, and emerging risks.

  - **Red Flag**: Companies that have no internal communication plan to evaluate external changes or the ability to appropriately respond. Imagine looking up from the car's dashboard while driving, seeing an object in road, and not being able to make adjustments to avoid it. There needs to be a process in place to adjust to external factors.

Customer focus: Without customers, your business goes away. Risk management cultures account for the needs and interests of customers. It then balances a risk-based approach with the organization's mission and strategic objectives.

  - **Red Flag 1**: Having a mantra of "the customer is always right and we must make the sale." I have personally seen a company willing to make a sale because they needed the transaction for cash flow reasons. They did not recognize that actually making the sale would likely have bankrupted the company because they did not consider the regulation they were about to violate. This is a severe blind spot. There were likely two root causes. Part of the problem was that they did not have the appropriate aspects of risk management in place. The other factor that may have also existed is that employees (if they were aware of the regulatory issue) were fearful of objecting to management about the sale because of potential backlash.

- **Red Flag 2**: On the other extreme, having customer requirements that are so rigid from a risk perspective that customers find it hard to do business with the company. If you are in a regulated environment, this may not apply. Within the parameters of any regulatory requirements, there should be thought given for appropriate empowerment of your front-line team to make risk-based decisions once they are well educated on the risks that they may be taking.

CHAPTER III

HOW TO MEASURE RISK

Transparency of the process is important because risk cultures are built so that everyone knows the rules of the road as it applies to your organization. Once a risk is identified, it needs to be measured.

CAUTION!

Set your risk thresholds when you are not in a crisis and when you are able to put thought and logic into the levels. Changing the meaning of your dashboard indicators because they are not "convenient" distorts reality and amplifies risk.

We used the car analogy earlier. Here is a second transportation analogy. I have friends that are pilots. One of them told me that every time he goes to the airport to fly, he looks for every reason NOT to fly that day while he is on the ground.

This sounds a bit counterintuitive. He continued to explain that during his pre-flight check if things are not exactly how he expects them to be, then he does not fly because it could lead to a problem in the air and the landing may "be more impactful than it should be."

Another pilot friend of mine explained how a pilot has to rely upon their instruments when they are in a situation without visibility. He explained that if you are second guessing your instruments and making repeated judgment calls this will only compound your risk and you may not be able to recover once you regain visibility.

In other words, establish your risk parameters when you can thoughtfully set them. Trying to determine what your risk tolerance should be during an event will likely lead to bad outcomes.

There is no "one-size-fits-all" answer when it comes to the measurement of risk. The most effective way to measure risk will depend on the specific context and nature of the risks involved. However, seven common ways to measure risk are included as follows:

1. **Probability and impact**: Assessing the likelihood and potential impact of a risk occurring, and assigning a numerical value to each, can help quantify the overall level of risk.

2. **Historical data analysis**: Examining historical data related to similar risks or events can help identify patterns and inform risk assessments.

- When the term "informing risk assessments" is used it means that organizations are appropriately understanding the risks and documenting them. This activity helps the management team identify and prioritize risks, estimate their potential impact, and determine appropriate risk management strategies to mitigate or address them effectively.

3. **Scenario analysi**s: Create hypothetical scenarios and evaluate the impact of each scenario to help identify potential risks and inform risk mitigation strategies.

- One way to accomplish this is by conducting a table-top exercise. Include representatives from all parts of the company to walk through various scenarios step by step and discuss actions that will need to take place under each case you develop. What does HR have to do? What about IT, Customer Support, etc.?

4. **Stress testing**: Simulate extreme market conditions and assess the impact on your operations to help identify vulnerabilities.

- Do you know what happens to your business if gas prices double or triple? Remember, it is not just what your company spends at the pump that matters. What happens to the costs in your supply chain? How does this change the buying patterns of your business customers or consumers?

5. **Expert judgment**: Seek input from subject matter experts or experienced professionals on how to measure certain risks. They can provide valuable insights into risks and risk management strategies.

6. **Risk appetite**: Establish a clear risk appetite or tolerance level. Setting levels helps guide risk management decisions such as prioritizing resources and efforts. By way of example, these are just some of the thresholds that should be determined by each business:

- Determine if your organization can tolerate one or more events that would cost $10,000 each? $100,000 each?
- Can your organization withstand an event that impacts half of your workforce?
- What about adding a day to customer delivery SLAs (Service Level Agreements)?
- Evaluate the risks and benefits of utilizing third party providers for services. Determine the potential weakest links in your business model.

7. **Risk indicators**: Establishing key risk indicators (KRIs) can help monitor and track risk levels over time and inform risk management decisions. KRIs are designed to provide early warning signals or indicators of potential risks before they materialize into significant issues or threats. Tracking them over time will also help identify trends.

Overall, the best way to measure risk will depend on the specific context and goals of the risk assessment. No one way is always the right way. A combination of different methods may be most effective.

CHAPTER IV

APPLICATION OF RISK MEASUREMENT

The application of risk measurement starts with understanding the functional terminology and methods that you can apply in your business. These terms will be used throughout the podcast. Let us revisit the first item under risk measurement: Probability and Impact. Probability and Impact tie back to the concept of Inherent Risk and Residual Risk. We will use the analogy of driving a car.

Inherent risk is the danger of driving a car on the road without considering any of the benefits associated with the implementation of risk mitigation tools or safeguards. Driving encompasses risks such as accidents, road conditions, weather hazards, or other drivers' behaviors. These **risks exist regardless, without any safety precautions** you could possibly take and are inherent to the activity of driving.

In business, think about this as having NO controls at all. No policies, procedures, or processes.

Control Effectiveness refers to how well the risk controls or mitigation measures have been implemented and to the extent that they actually work to reduce or manage the identified risks. Control Effectiveness measures how successful controls, such as procedures, processes, or systems, are in minimizing or mitigating the probability of an event even happening or reducing the potential impact of an event if it does occur. In the car analogy for instance, controls would be wearing a seatbelt, following traffic rules, and maintaining the vehicle's steering and brake systems.

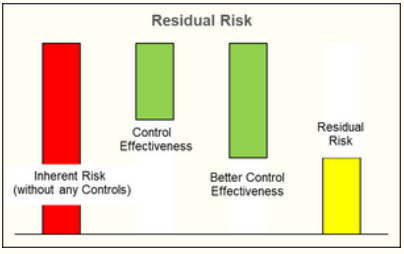
In business, controls include, but are not limited to client contracts, POS registers, inventory management, IT policies, or HR processes.

Residual risk is the risk that remains after implementing risk mitigation, controls, and safety measures. The inherent risk may be reduced to a lower level of residual risk but the controls do not serve to completely eliminate risk. Residual risk represents the remaining level of danger or risk that persists despite these safety precautions.

Returning to our driving a car analogy, the driving risks that can be controlled serve to lower the residual risks. The activities that cannot be controlled, such as other drivers' behaviors or unexpected debris in the road are residual risks that require risk awareness to mitigate as the situation arises.

Each identified risk should also include a **Direction of Risk** designation (e.g., increasing, decreasing, or stable) with a time horizon of the next 12-18 months. These ratings are utilized to identify potential threats and facilitate monitoring over time. This knowledge empowers organizations to make informed decisions, prioritize actions, and adapt their strategies to maintain a favorable risk profile.

The chart below shows the concept of Residual risk by starting with Inherent risk, without any controls, in red. This is where there is 100% exposure to all risks. There are two green bars that represent control effectiveness. The value of any type of control that an organization puts in place is dependent on their risk tolerance. If there is a higher acceptance of risk (e.g., financial, regulatory, etc.) then the types and effectiveness of controls may be lower, resulting in more Residual risk. If the organization wants lower residual risk, additional controls or more prescriptive guiderails may be in order.



The evaluation is not as simple as "more controls are better." It is about the value and risk tolerance. While some controls may be easy to implement at a low cost, others can be expensive, such as when system programming or projects are involved.

Control costs and risk costs should be evaluated. Factors to be considered in the risk-cost decision may include, but are not limited to, the cost of event loss, reputation or lost business impact, legal litigation costs, or insurance costs.

The most overlooked cost in risk management is the value of a business leader's time spent focusing on a risk event rather than leading the business.

Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.

HOW DO WE DETERMINE INHERENT RISKS?

There are two primary components: probability and impact. These two components are used together to assess the overall level of risk associated with a particular event or situation.

Probability refers to the likelihood or chance a particular risk event will occur, typically expressed as a percentage or a frequency (e.g., once per week, once per year, once per decade). Probability can be assessed using various techniques such as statistical analysis, historical data, expert judgment, or scenario analysis. As covered earlier, the higher the probability of a risk event occurring, the higher the overall level of risk.

Impact refers to the potential consequences or severity of a particular risk event if it were to occur. Companies can be impacted in multiple ways from a single risk event. Impact can be assessed in terms of financial, reputational, operational, or other relevant dimensions, including customer harm, complaints, and social media.

The impact of a risk event can be expressed in quantitative terms (e.g., dollar value of losses, number of customers affected) or qualitative terms (e.g., damage to reputation, disruption to operations). The higher the potential impact of a risk event, the higher the overall level of risk.

By considering both probability and impact, risk business leaders can better prioritize risks and allocate resources to the risks that pose the greatest threat to the organization. For example, a high-probability, high-impact risk warrants more attention and resources than a low-probability, low-impact risk.

Let's think about this in a more tangible way by quantifying the risk.

Start by establishing three levels of risk tolerance by creating a simple t-shirt size grid for the Probability (Small, Medium, and Large or Low Risk, Moderate Risk, High Risk) for the frequency of occurrence. For simplicity, let's say that Low Risk is once a decade, Moderate Risk is once a year, and High Risk is weekly. (Note: Risks are company-specific and some may have a time horizon that is materially shorter than the examples, such as a 3-5 year time frame for a Low Risk.)

The process to determine risk is less about math and more about magnitude.

Probability Value Grid

Probability	Example Description	Linear Value	Non-Linear Value
Low (Unlikely to occur)	Event likely to occur less than once every 10 years	1	1
Moderate (Reasonably possible)	Event likely to occur once per year	2	3
High (Likely to occur)	Event likely to occur at least weekly	3	9
		Average: 2.00	4.33

Then we do the same process for the thresholds in the Impact buckets, such as how much money it will cost us if we experience this event. Again, for simplicity, let's say that Low = $10,000; Moderate = $100,000; High = $1,000,000.

Impact Value Grid

Impact Grid	Example Description	Linear Value	Non-Linear Value
Low Impact	$10,000	1	1
Moderate Impact	$100,000	2	3
High Impact	$1,000,000	3	9
	Average:	2.00	4.33

We will use a 3x3 matrix for the first example (three columns and three rows). The 9-box grid will have Probability on one axis and Impact on the other. Inherent risk rating (IRR) is calculated by multiplying the assigned Probability (P) Level value to the assigned Impact (I) Level value.
(Formula: IRR = P * I)

To simplify, let's assign a simple numbering to the levels. We will start with a 1, 2, and 3 value for Small, Medium, and Large T-shirt sizes. This is simple and linear. When a simple linear score is used, the average will provide the user with a false reliance on averages because risk by its nature is non-linear and the magnitude has not been accounted for.

Using simple math, lets say that there are three (3) impact events, one event at each level. Take the value of each level or "bucket" and do a simple average. The sum of the three values is six (1 + 2 + 3 = 6). Divide the sum by count of three values (6 / 3 = 2). The average is two (2). When we reference the table to translate that average into an expected value of the impact, our table leads us to believe that an average event will have a value of $100,000.

The table below shows the IRR Scores based on linear values. It has some, but not much separation between each color band of risk.

Inherent Risk Rating Score (Linear Values)

IRR Score	Impact (Value)		
Probability (Value)	**Low (1)**	**Moderate (2)**	**High (3)**
Low (1)	Very Low (1)	Low (2)	Moderate (3)
Moderate (2)	Low (2)	Moderate (4)	High (6)
High (3)	Moderate (3)	High (6)	Very High (9)

Averaging linear risk is analogous to putting one hand in a hot oven and one hand in a freezer and saying that on average your temperature is just fine. It avoids the risk extremities that need to be managed.

A better way to think about risk is a non-linear approach. Start by assigning Low Risk a value of 1. Moderate Risk should be three times the risk of Low, so use a value of 3. High Risk should be three times the risk of Moderate, so use a value of 9. When using judgment to assign ratings to each event, the High Risk level may be used less frequently based on the significant difference in value above the Moderate Risk.

These non-linear values are included in the Probability and Impact Value Grids above.

Again, using simple math, let us say that there are three (3) impact events, one event at each level. Take the non-linear value of each Impact level and do a simple average.

The sum of the three values is 13 (1 + 3 + 9 = 13). Divide the sum by count of three values (13 / 3 = 4.33). The average is 4.33, which does not have its own box as a reference in the table to determine the expected value of the impact. Clearly this method creates skewing toward the elevated risk because it is more impactful.

When we compare the two value methods, we see that the mid-point of the linear values is actually smaller relative to the expected value of the weighted risk, which is higher than the $100,000.

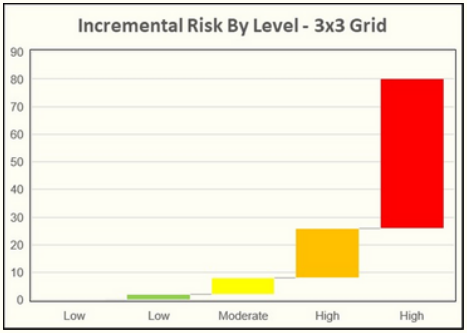
This process is less about mathematical formulas and more about the magnitude of risk. Regardless of how your organization may decide to approach risk tiering, it is important to focus on the magnitude of risk.

When you multiply the Probability value and the Impact value, the risk scores in the 3x3 grid using non-linear risk values start to show the magnitude change as the risk score difference grows between boxes. Overall, the probability and impact measurements of risk are useful tools for assessing and prioritizing risks. It can inform risk management decisions and strategies. Clearly the mitigation of Inherent risks with a score of 81 (9x9) would be prioritized above a score of 27 (9x3).

Inherent Risk Rating Score (Non-Linear Values)

IRR Score	Impact (Value)		
Probability (Value)	**Low (1)**	**Moderate (3)**	**High (9)**
Low (1)	Very Low (1)	Low (3)	Moderate (9)
Moderate (3)	Low (3)	Moderate (9)	High (27)
High (9)	Moderate (9)	High (27)	Very High (81)

The Non-Linear Values IRR Score table above shows the risk scores and is accompanied by a graph that demonstrates the incremental magnitude of risk by gradation.



Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.

WORKSHEETS:
Now it is time to start building a functional risk management framework to start identifying inherent risks. Start with the Three Tier Probability table below. Enter the description that is most appropriate for the business and events being evaluated.

Probability Value Grid

Probability	Example Description	Your Description	Score
Low (Unlikely to occur)	Event likely to occur less than once every 10 years		1
Moderate (Reasonably possible)	Event likely to occur once per year		3
High (Likely to occur)	Event likely to occur at least weekly		9

The Three Tier Impact Grid below shows a simple financial metric as an example to establish financial levels for your organization. Later in this chapter there is an Impact Grid table with additional sample descriptions of each level of risk. Ideally, establishing a quantitative or easily measured qualitative description helps identify objective metrics and removes subjective assessments. Use the blank template in Appendix A to build out risk factors and their levels. Enter descriptions that are most appropriate for the business and events being evaluated.

Impact Value Grid

Impact Grid	Example Description	Your Description	Score
Low Impact	Low (<$10,000)		1
Moderate Impact	Moderate (<$1000,000)		3
High Impact	High (≥$100,000)		9

CHAPTER IV

THREE TIER VS FIVE TIER GRIDS

The three-tier risk management program helps identify risk and is a great jumping off point for new risk programs. As the business develops and becomes more mature or the complexity of the business requires, such as in a regulated sector, movement to a five-tier program may be appropriate.

While you can move from a 3 tier (9-box) grid to a 5 tier (25-box) grid as you develop more sophistication in your risk program, using more than five (5) tiers is not advisable.

There are a couple of key differences as you move from a three-tier to a five-tier program.

- In order to improve the accuracy of our risk assessment, we need to make some adjustments to the values 1, 3, and 9. Remember that each level in our three-tier program is three times greater than the one below it. So, to create more precise distinctions, we are adding new values that fall between 1 and 3 (adding a value of 2), and between 3 and 9 (adding a value of 6). These new values help maintain the non-linear nature of the risk levels, which is important for understanding the increasing magnitude of risk as we move up the scale. You can see this relationship visually in the Incremental Risk by Level graph on the next page that illustrates the gradual increase in risk as we move from one level to the next.

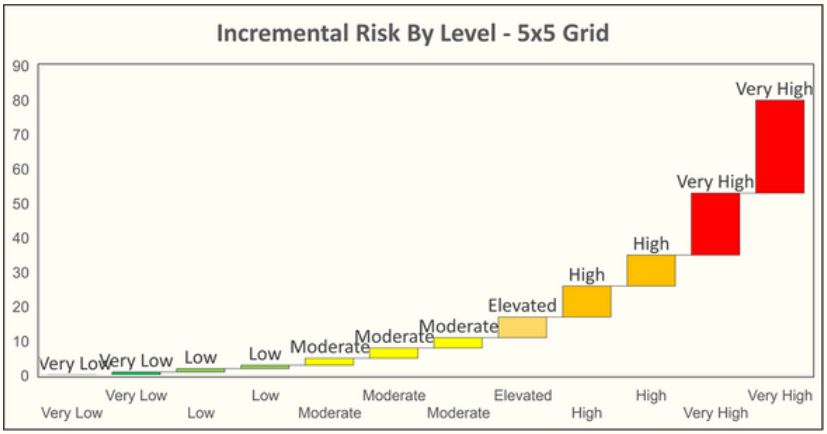
- There is another noticeable difference in the IRR Score grid. Instead of having five risk bands, there are now six, and an extra category called "Elevated" indicating higher risk. This change is due to how the scores separate along the continuum of magnitude. Previously, the Moderate range spanned from 6 to 12, representing a doubling of the risk magnitude. However, with the addition of the Elevated category, it is assigned a numerical value of 18. If we were to classify it as Moderate, it would mean that the Moderate range would have an upper limit that is three times higher than the lower limit. This would make the range too broad for effectively prioritizing risks.

Inherent Risk Rating Score (5x5 Matrix)

IRR Score	Impact (Value)				
Probability (Value)	**Very Low (1)**	**Low (2)**	**Moderate (3)**	**High (6)**	**Very High (9)**
Very Low (1)	Very Low (1)	Very Low (2)	Low (3)	Moderate (6)	Moderate (9)
Low (2)	Very Low (2)	Low (4)	Moderate (6)	Moderate (12)	Elevated (18)
Moderate (3)	Low (3)	Moderate (6)	Moderate (9)	Elevated (18)	High (27)
High (6)	Moderate (6)	Moderate (12)	Elevated (18)	High (36)	Very High (54)
Very High (9)	Moderate (9)	Elevated (18)	High (27)	Very High (54)	Very High (81)

The IRR Score table above shows the risk scores in a 5x5 Risk Grid.

The graph below demonstrates the incremental magnitude of risk by score and risk-band gradation.



The Five Tier Probability and Five Tier Impact Grids are provided on the next page with sample descriptions separated into five-tiers. Blank templates are shown in Appendix B to build out risk factors and their levels. Enter descriptions that are most appropriate for the business and events being evaluated.

Probability Value Grid

Probability	Example Description	Your Description	Score
Very Low (Remote probability)	Event with a remote probability to occur		1
Low (Unlikely to occur)	Event likely to occur on an annual basis		2
Moderate (Reasonably possible)	Event likely to occur on a monthly basis		3
High (Likely to occur)	Event likely to occur on a weekly basis		6
Very High (Almost certain)	Event with an ongoing effect or occurring on a daily basis		9

The Five Tier Impact table below also incorporates a Three-Tier Impact table with sample descriptions.

Example of Three and Five Tier Scoring of Impact Factors

Impact Factors	Score				
Five-Tier	1 Very Low	2 Low	3 Moderate	6 High	9 Very High
Three-Tier	1 Low		3 Moderate	9 High	
Legal implications	Breach of best practices, no legal/regulatory implications	Minor disputes and proceedings with regulators	Disputes and proceedings with regulators	Criminal charges	Loss of license
Reputational damage	Insignificant impact on the company's market [as defined]	Local and limited public media attention. Slight decrease in credibility / customer trust in local market	International media interest having long-term implications on the company's and group's reputation. Hindered vendor relationships	Significantly undermined reputation for integrity and compliance. Decrease in credibility / customer trust. Limitation of vendor products / services due to risks.	Loss of trust and goodwill of stakeholders and general public
Financial loss	Financial loss to company is less than 0.03% of the annual revenues for this product	Financial loss to company is between 0.03% and 0.1% of the annual revenues for this product	Financial loss to company is between 0.1% and 1% of the annual revenues for this product	Financial loss to company is between 1% and 2.4% of the annual revenues for this product	Financial loss to company is more than 2.4% of the annual revenues for this product
Employee morale implications	Isolated employee dissatisfaction	General employee morale problems	Widespread employee morale problems	Widespread employee morale problems and turnover	Widespread employee morale problems and multiple senior leaders leaving
Continuity implications	No business disruption	Isolated, localized business disruption	Disruption of business processes resumed within target due date	Significant disruption to key business processes for <24 hours	Prolonged interruption of critical business process for > 24 hours
Overall business effect	No or only very minor financial penalties, no negative impact on the company's financial performance or position.	Low financial penalties and some customer complaints, but without a negative impact on the company's financial performance or position.	Financial penalties, complaints from and loss of some customers, but no significant effect on the financial performance or position.	Significant financial penalties; Significant loss of customers, relationships, and contracts with certain partners / stakeholders. There is a significant negative impact on financial performance of the company but without threatening its continued existence.	Loss of key customers, of relationships or contracts with key partners and stakeholders, negative effect on share price. / Serious threat to the company's financial performance and position as well as its continued ability to operate.

Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.

LOGGING YOUR RISKS:

Now that you have identified the risks and quantified the risks scores according to the tier thresholds, it is time to log them in a Risk Register with their corresponding values and scores. There are very advanced systems that can be used for tracking risks, controls, testing, remediation, reporting, etc. I have also seen effective Excel spreadsheets used for tracking. This is an organizational decision based on risks, complexity, objectives, and of course, budgets.

As you build out your Probability and Impact grids using the tables in Appendix A and Appendix B, it is time to create a spreadsheet to track your risks with the following columns:

- Risk Number – It is recommended to develop a numbering taxonomy for easier tracking.
- Risk Description – These should be clearly stated in the form of risk statements.
- Impact – Name and value number
- Probability – Name and value number
- Inherent Risk – Name the scored level of risk
- Additional columns that you will find useful will be:
    - Risk Category (e.g., IT, Finance, HR, Operations, Regulatory, etc.)
    - Related Policy
    - Related Procedure

The Sample Risk Register entry below shows the four primary columns. This example highlights the Risk Description statement about launching a product without involving the entire team to ensure all risks are evaluated together.

Sample Risk Register Entry

Risk Description	Impact	Probability	Inherent Risk
New products or modifications to existing products are rolled out to customers without proper assessments from the cross-functional team established to ensure all aspects of the product are within the Cmpany's risk tolerance and all potential risks are identified and approved along with appropriate mitigation and controls.	Very High (9)	Moderate (3)	High

This example is multi-faceted. There should be a process to engage finance, marketing, operations, customer experience, legal, HR, IT, and any other aspect of your company that are responsible for a successful launch. Without a multi-disciplined approach, the Impact—a failed launch—would be rated as a Very High (9) risk because it is likely that a ball will be dropped by one or more stakeholders along the way.

The Probability was rated Moderate (3) because without controls in place there is a moderate chance that not all parties and stakeholders will be engaged appropriately. Therefore, the Inherent Risk is rated High (27) and should rise to the level of priority for the organization.

A strong control could mitigate this High level of inherent risk. An example of a good control for this risk is to have a company policy in place about product launches and a formal New Product Risk Assessment (NPRA) form that the management team is required to physically approve before a launch can begin. If the control is designed and implemented well, this could be a strong control that would lower the Residual Risk by reducing the Probability of launching a product without stakeholder approval.

CHAPTER V

TYPES OF RISK

When conducting a thorough risk assessment, it is important to consider various areas and types of risk. Sometimes these are known as risk pillars or risk factors.

Specific factors should be tailored and may vary depending on the context, operations, and industry. It is important to involve key stakeholders and subject matter experts during the risk assessment process to ensure comprehensive coverage of all potential risks.

Here are some common risk types to consider. The related but distinct types of risks are grouped together. It is common for risk events to have cross-impacts to other risk classifications.

Strategic Risks

Assess risks related to achieving organizational objectives, such as changes in market conditions, competitive landscape, technological advancements, or shifts in customer preferences.

Financial Risks

Consider risks that can impact financial stability, such as fluctuations in exchange rates, interest rates, credit risks, liquidity risks, or inadequate financial planning.

Operational Risks

Evaluate risks associated with day-to-day operations, including process failures, supply chain disruptions, equipment breakdowns, human error, or inadequate internal controls.

Project Risks

Evaluate risks associated with specific projects, such as project delays, cost overruns, scope creep, resource constraints, or inadequate project management.

Reputational Risks

Assess risks that could damage the organization's reputation, including negative public perception, social media backlash, ethical breaches, or publicized scandals.

Supply Chain Risks

Identify risks associated with the organization's supply chain, including supplier disruptions, logistics failures, quality control issues, dependence on single suppliers, or geopolitical risks impacting the supply chain.

Risk Types (Continued)

Legal and Regulatory Risks

Legal Risks

Identify risks related to potential lawsuits, legal disputes, intellectual property infringement, contractual obligations, or non-compliance with laws and regulations.

Ethical Risks

Evaluate risks associated with ethical considerations, including unethical behavior within the organization, non-compliance with ethical standards, conflicts of interest, fraud, or breaches of corporate governance.

Compliance Risks

Identify risks arising from non-compliance with laws, regulations, or industry standards. This includes legal risks, regulatory changes, data protection and privacy, or failure to meet contractual obligations.

Technology and Security Risks

Technological Risks

Assess risks related to technology infrastructure, including system failures, data loss, software vulnerabilities, compatibility issues, or reliance on outdated technologies.

Security Risks

Evaluate risks related to information security, cybersecurity threats, data breaches, unauthorized access, or physical security vulnerabilities.

Human Capital Risk

Human Resources Risks

Assess risks associated with human capital, such as employee turnover, skills gaps, labor disputes, talent acquisition and retention, or health and safety risks.

Health and Safety Risks

Evaluate risks related to the health and safety of employees, customers, or other stakeholders. This includes workplace accidents, occupational hazards, exposure to hazardous substances, or non-compliance with health and safety regulations.

Risk Types (Continued)

External Risks

Market Risks

Consider risks related to market dynamics, including changes in customer behavior, demand fluctuations, entry of new competitors, pricing pressures, or loss of key clients.

Emerging Risks

Stay updated on emerging risks that may impact the organization in the future, such as new technologies, geopolitical changes, social trends, or industry disruptions.

Political / Regulatory Risks

Assess risks arising from political instability, changes in government policies, shifts in regulations, trade disputes, or geopolitical tensions that could impact operations or market conditions.

Economic Risks

Consider risks associated with economic factors, such as inflation, recession, currency fluctuations, changes in interest rates, or trade restrictions.

Sustainability & Continuity Risks

Disaster Recovery and Business Continuity Risks

Assess risks related to the organization's ability to recover from disruptive events and maintain business continuity. This includes risks associated with data backups, alternative work locations, emergency response plans, or IT infrastructure resilience.

Crisis Management Risks

Identify risks associated with crisis situations, such as natural disasters, pandemics, terrorist attacks, product recalls, or reputational crises. Evaluate the organization's preparedness and ability to respond effectively.

Environmental Risks

Consider risks associated with environmental factors, such as natural disasters, climate change, pollution, or regulatory requirements related to sustainability.

CHAPTER VI

CONTROL EFFECTIVENESS

We previously discussed having controls and their effectiveness in managing risks. It is crucial to be able to measure how much of the inherent or initial risk is actually reduced by these controls. This measurement helps us determine the residual or remaining risk. In simpler terms, we want to understand how effective the controls are at minimizing the overall level of risk we face.

Control Example 1: Imagine you never want your car to exceed the speed limit to avoid speeding tickets. To achieve this, you decide to install a device in your car called a governor. The governor would automatically adjust your car's speed to match the speed limits on freeways and in school zones. By doing so, you would successfully address the risk of surpassing the speed limit.

However, it is important to understand that this solution only tackles one specific risk: speeding. It does not eliminate or address other potential risks you may encounter while driving, such as distracted driving, road conditions, or other drivers' behaviors. So, while the governor helps with one aspect of risk, there are still other factors that need to be considered for overall safety on the road.

Control Example 2: If it is necessary for your business to have a phone number provided with every order, one way to ensure a phone number is provided is by programming your computer system to prevent the sale from advancing to the next stage unless a phone number is entered. This control helps address the risk of orders being placed without a phone number being entered in the data field.

However, it's important to consider that this control only addresses the presence of a phone number; it does not guarantee that the phone number provided is valid or verifiable. So, while the control helps mitigate the risk to some extent because most people tend to provide their real phone numbers, it doesn't completely eliminate the risk of receiving inaccurate or false phone numbers.

Control Example 2 (continued):

Another factor to keep in mind is the possibility of an employee finding a way to bypass or work around this control. If an employee understands how to circumvent the system requirement for a phone number, they could potentially introduce risk to the order process. This highlights the importance of ensuring that employees adhere to established controls and follow proper procedures to minimize any potential risks that may arise

Just like we rate the level of risk in terms of Inherent Risk, we also need to rate the effectiveness of controls on a scale from Ineffective to Strong. This rating helps us understand how well the controls are able to reduce the inherent level of risk. To determine the Residual Risk, the remaining risk after controls are applied, it is important to clearly define and specify how these controls systematically reduce the Inherent Risk.

All of this information should be logged into the Risk Register

This e-book is focused on the identification and measurement of risks as the first stage of the risk management journey. Design of the controls, determination of the control effectiveness, and assessments of residual risk are beyond the scope of the Foundations of Risk Management e-book.

CONCLUSION

As a Blind Spot Insider, we hope you found the information in this e-Book valuable to document and expose the potential risks in your business. I encourage you to use this e-book as a reference tool during your risk identification journey.

The WHAT THE R*SK! Podcast is designed to be a "safe-space" to learn about risk, how to think about risk, and how to Expose Business Blind Spots. This e-book and the podcast are about empowering you as a business leader to reduce the stress of the unknown risks in your business and mitigate the impact of potential events.

Let's expose these blind spots, and educate you how to mitigate, manage, or avoid these risks.

After reading this e-book, you should have a better understanding of how to identify and size risk, including enhancement opportunities for the risk management culture. The tools and framework provided are applicable to all businesses, but the implementation will depend on the specific context, complexity, and nature of the risks involved and the risk management program being developed.

If you found this e-book and the podcast helpful, please **Share the podcast with peers.** You and your peers will be exposed to what you didn't know existed in the risk blind spots. Learn from elite thought leaders across industries and business functions.

The title of this podcast is a vivid reminder of the emotion you do not want to experience and the actions you can take to prevent stressful business situations.

WHAT THE R*SK! – Exposing Business Blind Spots.

Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.

APPENDIX A

Blank Impact Grids

Blank Three Tier Impact Grid

Impact	Your User-Defined Impact Factors						Score
	[Factor]	[Factor]	[Factor]	[Factor]	[Factor]	Overall business effect	
Low							1
Moderate							3
High							9

* Include as many factors that are applicable and meaningful to your business.

Blank Five Tier Impact Grid

Impact	Your User-Defined Impact Factors						Score
	[Factor]	[Factor]	[Factor]	[Factor]	[Factor]	Overall business	
Very Low							1
Low							2
Moderate							3
High							6
Very High							9

* Include as many factors that are applicable and meaningful to your business.

Join us on this journey, as we learn to ask the right questions, expose potential pitfalls, and turn those "**WHAT THE R*SK!**" moments into "I've got this!" victories.