

A Paisley White Paper

Enterprise Risk Management Assessment Guide

Prepared by:

Bruce McCuaig
Vice President, Risk & Compliance — Paisley



THOMSON REUTERS™

Enterprise Risk Management Assessment Guide

Table of Contents

Introduction	2
Is Your Risk Management Process Really Assessing Risk?	2
Is Your Risk Assessment Context-Driven?	3
Does Your Risk Management Process Address Root Cause of Failure?	4
What Does Your Business Performance Tell You About Risk?	5
What Do Risks Tell You About Your Controls?	6
What Do Controls Tell You about Your Risks?	7
Are You Up For the Task of Risk Management?	8
About Paisley	10

INTRODUCTION

Government bail outs, pro-cyclical financial markets, and an overall economic meltdown have placed a significant focus on the discipline and practice of risk management. In light of these events, risk professionals and organizational leaders are taking an introspective view of their risk management practices. By considering these seven questions organizations and risk professionals will sharpen their daily risk management tools and be better equipped to make tactical improvements to risk management practices.

1. Is Your Risk Management Process Really Assessing Risk?
2. Is Your Risk Assessment Context-Driven?
3. Does Your Risk Management Process Address Root Cause of Failure?
4. What Does Your Business Performance Tell You About Risk?
5. What Do Risks Tell You About Your Controls?
6. What Do Controls Tell You About Your Risks?
7. Are You Up For the Task of Risk Management?

IS YOUR RISK MANAGEMENT PROCESS REALLY ASSESSING RISK

In far too many cases the answer to this question is NO. Many so-called risk management processes are not necessarily identifying and assessing risks. Many risk management practices, as implemented, are simply identifying and assessing the risk of control failure, not the specific risk the control is to mitigate.

Risk-based thinking approaches the assessment with the premise that risks are predictable and avoidable. The risk-based discipline tracks loss events, analyzes root causes, and eliminates or mitigates the cause of the risk failure. Control-based thinking takes the approach that events are unpredictable and unavoidable, and controls are needed to mitigate the risks. Negative impacts are the result of broken controls, not of unidentified or mitigated risks.

It is imperative to know what risks the controls are addressing and to identify those risks first.

A simple indicator on the general emphasis on controls versus risks in common practice is outlined in the table below which reflects the word count comparison of two risk management frameworks (Basel II and ISO 31000) and several well-known control frameworks including the risk-based PCAOB AS5, ISO 27001, and the COSO *Guidance on Monitoring Internal Control Systems*. The word count is a simple tally of where the words risk and control appear in the referenced documents. The relevant emphasis on risk and control is evidenced in the word counts.

Word Count Comparison		
	Risk	Control
Basel II	1,500	67
ISO/DIS 31000	339	5
COSO Monitoring (Volumes 1 and 2)	175	641
ISO 27001:2005	65	192
AS5	168	635

If a risk is defined as a broken or failed control, a control-based approach is in use and controls are primarily being assessed, not risks.

If inherent or residual risks are not measured and assessed, a control-based approach is being used and controls, not risks, are being assessed.

If an organization reports on control effectiveness over risks, controls and not risks are being assessed. Risks are just there to hang controls from, not to be understood and managed.

There is nothing wrong with identifying and assessing controls. It is a perfectly valid approach. But by itself it is insufficient and has proven to be inherently unreliable. It is imperative to know what risks the controls are addressing and to identify those risks first. For example, little faith would be put in a doctor who prescribed medication without identifying symptoms, e.g., performing a risk assessment. Don't trust control assessments where no risk assessment is conducted (or vice versa).

IS YOUR RISK ASSESSMENT CONTEXT DRIVEN?

Black swans hide where no one thinks to look. The history of risk assessment suggests that at least half of the problem is not looking in the right place for

risks. The other half is looking in the right places and failing to find the risk. Context-driven risk assessment refers to the process of identifying all the topics or areas that need to be risk assessed. Contexts can be accounts, strategies, laws and regulations, organization entities, lines of business or any other relevant topic areas.

It is wrong to believe that the right contexts will be identified and addressed from within the organization by business operational managers and professionals. These leaders have typically been proven to be blinded by narrow vision, short range thinking, or do not have perspective across the entire entity to have a good handle on the enterprise-wide risks. Therefore, context must be identified at the organization level and the related risk assessments must be coordinated by senior management and the board.

DOES YOUR RISK MANAGEMENT PROCESS ADDRESS ROOT CAUSE OF FAILURE?

With control-based approaches, there is typically no requirement for root cause analysis. In the control-based approach, control breakdowns simply need to be identified and reported, regardless if the root cause remains obscure.

For example, with Auditing Standard No. 5 there is no requirement for the identification, reporting or remediation of any related root cause. Publicly-reported significant deficiencies and material weaknesses do not require and seldom receive any root cause analysis. The COSO *Guidance on Monitoring Internal Control Systems* does not require root cause analysis nor does ISO 27001.

It would be unthinkable today for an airplane to crash or a bridge to collapse without a detailed public report on the root cause and measures taken to ensure the problem does not reoccur. This degree of scrutiny does not generally exist in the risk management professions. Notable exceptions are the quality, safety and environmental movements. Generally speaking, if incidents, near misses and loss events are not tracked, the root cause of failure will not be analyzed. If the root cause of failure is not addressed the problem will be repeated. The following table, created by the U.S. General Accounting Office lists the causes of bank failures in the U.S. Although created in 1987, it could have been written last week.

Generally speaking, if incidents, near misses and loss events are not tracked, the root cause of failure will not be analyzed.

Many risk and control practitioners fail to consider business performance when assessing either risk or control.

Root Causes of Bank Failures (1987)	% of Banks
Management Philosophy and Operating Style	
Inadequate board supervision	49%
Over reliance on volatile funding sources	32%
Presence of dominant figure	37%
Excessively growth oriented philosophies	26%
Management Operational Practices	
Lack of general lending policies	79%
Poor loan administration	42%
Poor loan documentation/inadequate credit analysis	41%
Inadequate loan loss allowance	29%

WHAT DOES YOUR BUSINESS PERFORMANCE TELL YOU ABOUT RISK?

Many risk and control practitioners fail to consider business performance when assessing either risk or control. In other words, it is not only possible, but common, to get a passing mark on risk management or control effectiveness when business performance is screaming the contrary. Here are some common symptoms of business performance issues that suggest risks are not being managed:

- Process performance/error rates are off target
- Key performance indicators are consistently outside target
- Key performance indicators are never outside target
- Budget/actual variances are material (positive or negative)
- Capital projects are delayed or over/under spent
- Earnings volatility is out of line with peers
- Variances cannot be explained by known risks
- Clean 404 opinions are followed by material weakness disclosures
- Internal audit recommendations always increase vs. decrease controls

Most risk and control frameworks fail to consider business or process performance. Neither SOX nor the PCAOB AS5 pay much attention to business performance. COSO monitoring prefers testing to monitoring performance. Basel II does support key risk indicators and key performance indicators. The premise here is that over time, on target, consistent business or process performance is de facto evidence of effective risk and control management.

Performance variances should be explained as unidentified or unmanaged risks. Unusual business performance should be explained by unusual risks. But risk and control assessment not tied to business or process performance is not helpful and may be dangerous.

WHAT DO RISKS TELL YOU ABOUT YOUR CONTROLS?

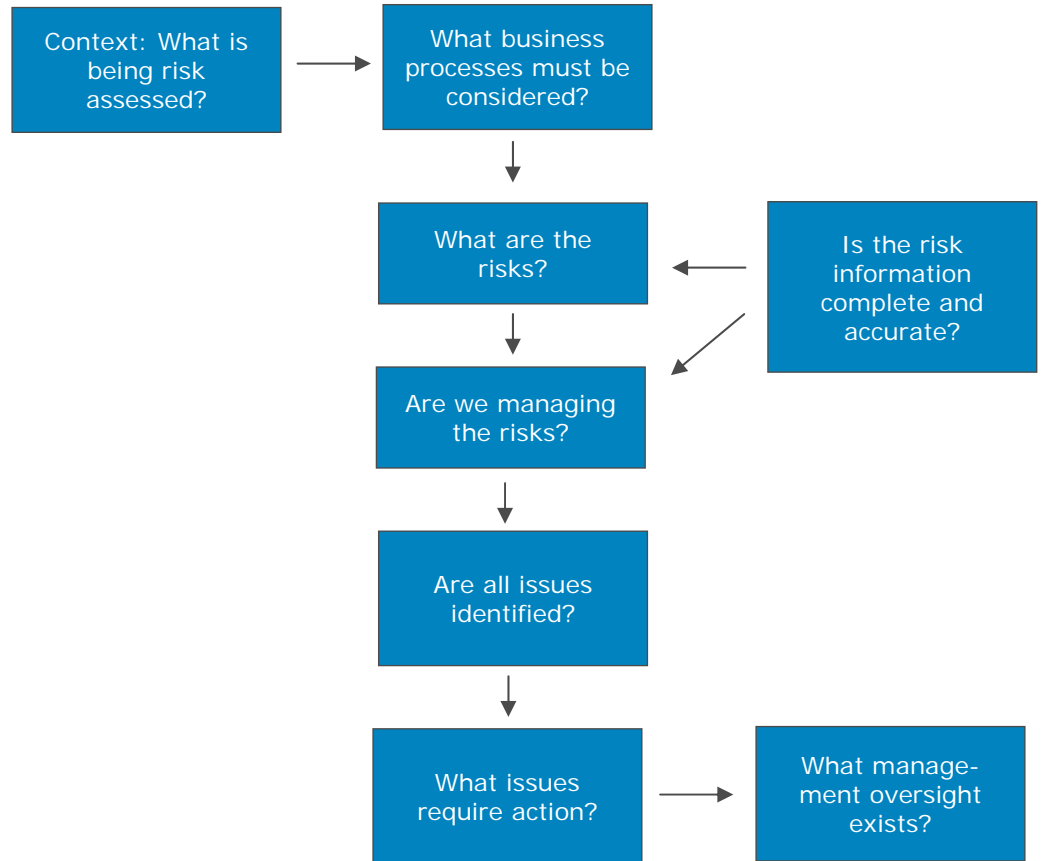
In late 2007, Standard & Poor's issued a discussion paper outlining their proposal to assess corporate risk management practices as part of their credit rating process. In the normal course of events, most companies would be expected to encounter most of these risk types, quite often in multiple locations or contexts. Not only that, but the nature and level of these risks will change constantly.

In short, most risks cannot be controlled, they must be managed.

In short, most risks cannot be controlled, they must be managed.

Standard & Poor's Sample Risk Types			
Environmental risks	Financial risks	Supply risks	Management risks
Business continuity	Capital availability	Commodity prices	Corporate governance
Business market	Credit counterparty	Supply chain	Data security
environment	Financial market risk		Employee health and safety
Environmental	Inflation		Intellectual property
Liability lawsuits	Interest rates		Labor disputes
Natural disasters/weather	Liquidity		Labor skills shortage
Pandemic			M&A/restructuring
Physical damage			Managing complexity
Political risk			Outsourcing problems
Regulatory/legislative			Project management
Terrorism			Reputation

Risk management involves an ongoing process similar to the diagram below. It involves clarifying accountability and decision rules and continuously updating information and reporting. Risks need managing, not controlling.



More controls do not mean less risk; the opposite is often true.

You are beginning to manage risks if

- You can identify in which contexts these risks exist
- You can track frequency distributions of instances of risks by type
- You recognize risk identification and assessment in your compensation/ reward system
- You track incidents/loss events/issues and actions associated with key risks
- You have identified risk tolerances and appetite

WHAT DO CONTROLS TELL YOU ABOUT YOUR RISKS?

More controls do not mean less risk; the opposite is often true. Too many controls may be evidence of lack of effective risk management practices. Good risk management considers a variety of risk responses, of which con-

trols are only one. The proliferation of control-based approaches to risk has led to extensive identification, documentation, testing and reporting of controls. That can be a mistake if carried to an extreme. If you have gathered more knowledge about controls than about risks, and focus on the control side of the equation, it is a clear indication of bad risk management practices.

Generally speaking, good risk management practices will produce a 3:1 or greater ratio of risks to controls. Risk-based approaches gather more knowledge about risk than control. Today that ratio is often reversed. Risk control ratios of 1:3 are common. Some balance is required, but generally a risk control ratio of >1 is desirable. Risks can be documented and tested too, and should be continually assessed. If you get the risk side wrong, you can't get the control side right.

Low risk:control ratios indicate business management has not been involved in risk identification, is unwilling to be candid or is not completely honest. In a healthy and safe environment, business managers, if asked, will provide a wealth of detailed information. Rich, detailed knowledge of risks provides a basis for far more efficient-and-effective control portfolios. The more and better the knowledge of risk, the more effective and efficient the control portfolio. Expect fewer, not more controls, but expect them to be better, more powerful controls.

Standard & Poor's, in assessing ERM, looks for compliance-based approaches to risk management and scores them poorly. Low risk:control ratios are indicative of compliance-based approaches to risk management.

ARE YOU UP FOR THE TASK OF RISK MANAGEMENT?

Risk management requires the mastery of a body of knowledge, specific skill sets and the appropriate use of technology. A sample of the knowledge and skill requirements is set out below.

Knowledge and Experience Requirements for Risk Management Leaders

1. Technology implementation for risk management which includes knowledge of best practices in a wide range of topics such as developing proc-

... good risk management practices will produce a 3:1 or greater ratio of risks to controls.

ess structure, KPIs, KRIs and selecting or designing other critical contexts for risk management

2. Experience leading and completing ERM assessments for the organization as a whole or major business units or functions, completing SOX certifications and ORM and other process level risk assessments
3. Selection and application of risk models and use of the risk identification and rating desktop for identifying and classifying all relevant risks
4. Tools and techniques for root cause analysis and business process improvement
5. Development of reliable descriptions of loss events, incidents and issues or actions with respect to the context selected
6. Understanding the major approaches to self-assessment and business reasons for adopting self-assessment approaches to risk and control management
7. Understanding organizational risk and control self-assessment (RCSA) barriers and implementation of effective tactics and tools for RCSA
8. Understanding of generally accepted control criteria including all major control and quality models (COSO/CobiT/COCO/ISO/OTOL, etc.)
9. Understanding of generally accepted risk criteria including the leading risk standards and frameworks (COSOERM, AS/NZ4360, ISO31000, etc.)
10. Linkages between SOX legislation, relevant PCAOB audit standards, the Basel II and Solvency 2 ORM requirements and other major regulatory frameworks governing risk and control such as Turnbull, J-SOX and *IIA Professional Practice Framework*, etc
11. Understanding and implementing major industry specific risk and control assessment frameworks.

Risk management is a young profession with huge potential to help address and resolve some of the worst problems we are experiencing on a day-to-day basis. But true professionals are rooted in public service and some degree of altruism. There is a long way to go to achieve that goal. But fundamental tools, practices, knowledge and skills exist today. Risk managers must proceed carefully but quickly.

Risk managers must proceed carefully but quickly.

ABOUT PAISLEY

Thomson Reuters is the world's leading source of intelligent information for businesses and professionals. The company combines industry expertise with innovative technology to deliver critical information for leading decision-makers in the financial, legal, tax and accounting, scientific and healthcare markets.

Paisley, acquired by Thomson Reuters in 2008, is the governance, risk and compliance platform business unit of Thomson Reuters. Combining Paisley's market leading software with the comprehensive Thomson Reuter's intelligent information solutions delivers the most comprehensive GRC solution for audit, risk and compliance professionals. Over 1,400 organizations, spanning 60 countries and serving more than 140,000 users in a wide range of industries, utilize Paisley GRC solutions to streamline processes, reduce costs of compliance, manage and mitigate risks, and provide visibility, oversight and assurance.

The Paisley GRC solutions include functionality for audit management, financial controls management, enterprise risk management, operational risk management, IT governance, and compliance. Paisley offers several software delivery options including on-premises, hosted application deployment, or software as a service (SaaS) delivery.

*For more
information,
call:
320.286.5870,
email:
info@paisley.com
or visit:
www.paisley.com*