



Operational Risk Management “The Next Big Thing”

David Kramer, Senior Account Manager

Presentation objectives

- Define Operational Risk Management (ORM) within a business context
- Highlight what is driving ORM as the “Next Big Thing”
- Provide an overview of a practical, easy-to-implement ORM framework.

Background

- Personal Background
 - Senior Account Manager, Consul risk management
 - Business Development
 - Risk Assessments
 - Audit Solutions
 - Previous CPA – both private and public roles
 - Developed, implemented and enforced strategic operating policies and procedures for DATASTORM
 - Managed several reviews and audits while engaged in public work – largely mid Missouri Mutual Insurance company's
 - IT Audit & Security Consultant

Agenda

The state of “Operational Risk Management” (ORM)

A basic review

What the future holds

A simple model ORM for success moving forward

Risk management through the ages

- Humans have been managing risk ever since they were capable of rational thought
 - Weighing the risks of hunting large animals against the reward of a woolly mammoth steak; sacrificing cats and virgins to the gods in expectation of rewards in the afterlife.
 - And we still do it today – worrying over the effect of that third Twinkie on our cholesterol level versus the sugar high we may gladly experience.
- Today, process is logical, explicit and systematic.
 - We rely on sophisticated mathematics and methodologies to determine the likelihood, impact and exposure to risks.
 - After all, when weighing that Twinkie, we need only look at the wrapper to quantify how devastating the effects may be.

Risk management in business

Credit Risk

Operational Risk

Market Risk

- Risk management has evolved into several categories.
 - These categories are defined through different causes and/or effects.
 - In the banking industry, for example, market risk is defined as the systemic risk inherent in the capital market, (i.e. it is the risk that is not diversifiable through trading in financial contracts).
 - Credit risk is defined as loss exposures due to counterparties' default on contracts.
- With respect to operational risk, there does not yet exist an agreed-upon definition.
 - The first definitions were mostly based on the “everything but” principle, such as “all risks but market and credit risk.”
 - Operational risk management (ORM), despite the lack of definition, is being heralded as the next big thing and the reason why all Chief Security Officers may want to pursue an MBA.

What is operational risk management?

- Today's vision of ORM is to optimize the performance of a business by understanding the effects of adverse operational losses on our business activities and assets so that we can insure against them.
- Traditionally, operational risk can be associated with the following:
 - o **Process:** losses that have been incurred due to a deficiency in an existing procedure, or the absence of a procedure. Losses can result from human error or unintentional failure to follow an existing procedure.
 - o **Systems:** losses that are caused by unintentional breakdowns in existing systems or technology.
 - o **External:** losses occurring as a result of natural or man-made forces, or the direct result of a third party's action.
 - o **People:** losses associated with intentional violation of internal policies by current or past employees.

Hold on.... This sounds like BCDR

- Agreed. They sound the same, but are different in the way each looks at risk.
- In an ORM world, risk is a possibility one needs to take steps to address.
- In a Business Continuity/Disaster Recovery world, risk is unavoidable. One needs to plan for that eventuality.
- The difference between operational risk management and business continuity disaster recovery planning is best described in a practical example:
 - BCDR: My CEO will get hit by a bus. Let's create contingency plans for that eventuality.
 - ORM: My CEO may get hit by a bus. Let's break his legs so that he can't cross the street.

Status of Operational Risk Management in today?

- The answer to this question varies according to geographic region.
 - In Europe, for example, there are often more formal, structured, enterprise-wide operational risk programs in the works.
 - Why? Regulators there appear to have been more vocal about operational risk for the past decade, most likely in the wake of events like the Barings rogue trading incident and in reaction to the Basel II Capital Accord.

Hall of Shame....

“Nicholas Leeson was a rogue trader who reduced the value of the venerable Baring Brothers & Co (BB&Co) Bank from roughly **\$500 million dollars to \$1.60**. Leeson traded futures contracts on the Nikkei 225 and on Japanese Government Bonds without authorization while management at Barings, the Singapore International Monetary Exchange, the Osaka Stock Exchange, and other governing bodies in Britain and Singapore disregarded or failed to recognize the potential for financial disaster. The failure of Barings Bank provides a lesson in the risks and responsibilities involved in organizing and monitoring derivatives trading.”

(SOURCE: http://www.thunderbird.edu/pdf/about_us/case_series/e06990021.pdf)

Operational risk management in the U.S.

- Risk management efforts have been focused on tactical initiatives and activities:
 - measurement
 - assessment
 - mitigation and remediation,
 - monitoring
- Efforts focused within a business line, or around a specific operation.
- Often, efforts within this area are identified as security management efforts, which are often driven by the need to comply with minimum-security standards. In other words, compliance.

Risk Management Focus Areas

- Compliance management solutions *tend* to solve problems associated with one or more “categories” of risk

Category	Systems	Database/Transactions	Process	Information
Compliance requirement is associated with:	<p data-bbox="611 889 1871 1101">Operational Risk Management requires that organizations not look at discrete categories, but at business operations in the whole</p>			
Common problems the compliance requirement is intended to manage:				
Problem owner:				

Are we seeing a move toward ORM in the U.S.?

- Yes. Absolutely.
- In the U.S., the number one factor accelerating development of ORM as a field is the Sarbanes-Oxley Act of 2002 (SOX).

Agenda

The state of “Operational Risk Management” (ORM)

A basic review

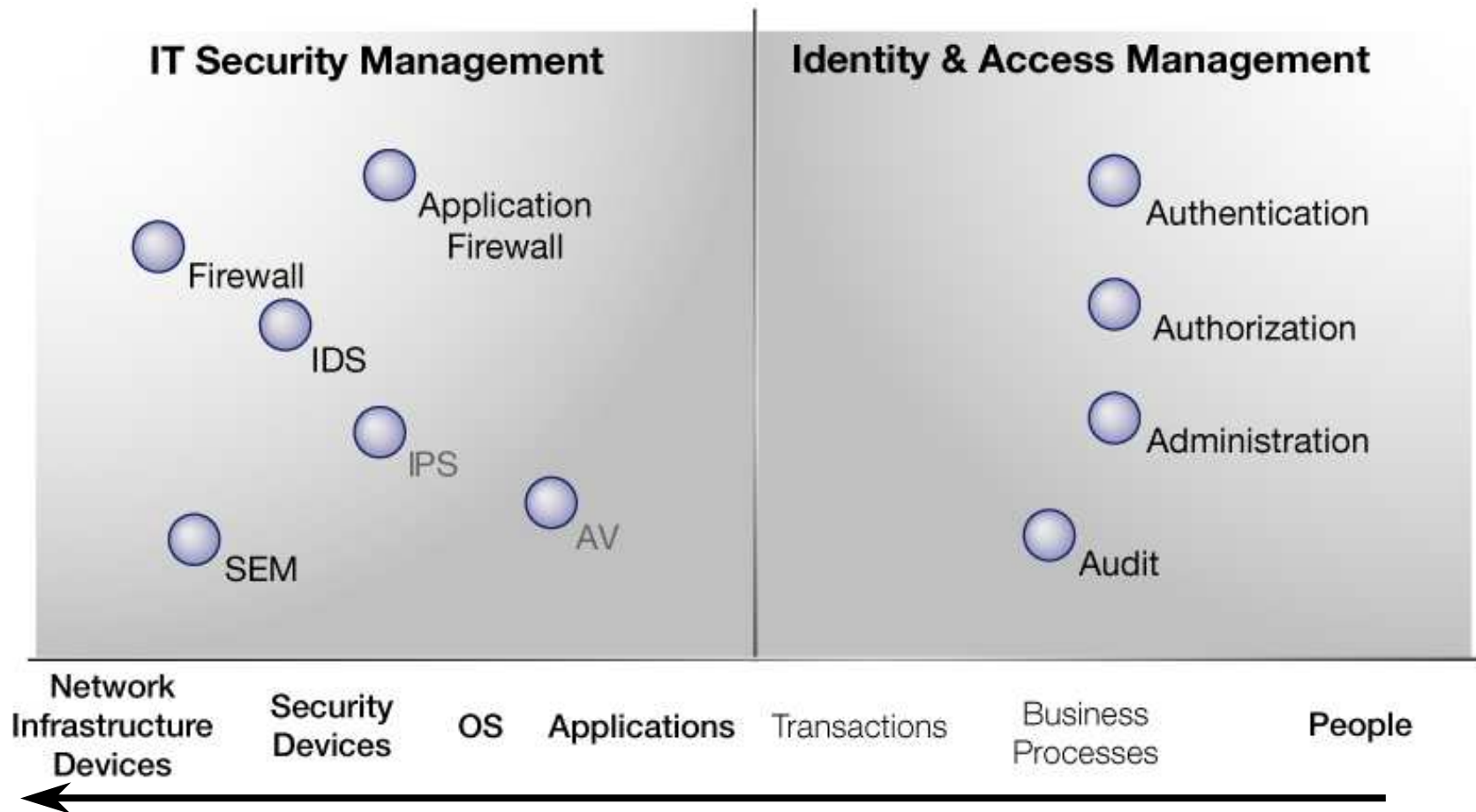
What the future holds

A simple model ORM for success moving forward

The Sarbanes Oxley Act Objective

- Better **Information** to Investors
 - Management's responsibility and its discharge
 - Enables evaluation of management's performance
- More **reliable** financial statements
- Corporate **discipline** :
 - devotion of resources to **Internal Control Framework Review**
 - identify weaknesses/deficiencies in advance of breakdown,
 - help companies detect fraudulent financial reporting earlier
 - deter/minimize financial fraud and adverse effects.

IT Asset Security versus Information Security



Results of a failure to comply

- Establishes a maximum fine of **\$1,000,000** and a maximum prison sentence of 10 years for CEO's and CFO's that **certify** a financial statement knowing that it is not consistent with all of the sections of the Act.
- Establishes a maximum fine of **\$5,000,000** and a maximum prison sentence of 20 years for CEO's and CFO's that **willfully certify** a financial statement knowing that it is not consistent with all of the sections of the Act.

Putting this into context...

1 - 2 years	Escaping from prison
3 - 5 years	Kidnapping involving Ransom
10 - 20 years	Fraudulent SOX Certification
11 - 14 years	Second Degree Murder
20 - 25 years	Hijacking

COSO

- While Internal Control was not defined in the Act, the COSO definition has been accepted by the US government and its agencies, incorporated in US auditing standards (AU 319), and is a generally accepted integrated framework for control infrastructure. Under regulations for Section 404, the SEC will use AU319 as the reference.
- COSO identifies five components of control that need to be in place and integrated to ensure the achievement of each of the objectives.

IN SUM: COSO is an integrated framework for internal control which, when implemented, provides a baseline to establish a control structure that meets Section 302 requirements and supports 404 attestation.

Internal Control Definition

Internal Control is broadly defined as a ***process***, implemented by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Each objective has relevance to the five components of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication)

Practical Example:

- **Risk:** A shipment is made but the related sale is not recorded
- **Process:**
 - **Who:** Shipping Clerk
 - **What:** Shipment to customer is electronically logged. Log is used to ensure shipment and invoice the customer
 - **When:** Daily
- **Internal Control Evaluation Criteria:**
 - Has the “process” been documented?
 - Has the integrity of the process been assured ?
 - Is there evidence that shipments occurred that were not logged within this process architecture?
 - Does the organization have the capacity to report failures of the process on an as needed basis?

Summary...

- Management must document assess and test all significant controls. Not how it should work but how it actually works...
- Every step of process must be documented (Actor/Act/Asset). No documentation = significant weakness
- One material weakness = qualified ICFR report

Agenda

The state of “Operational Risk Management” (ORM)

A basic review

What the future holds

A simple model ORM for success moving forward

The COSO Evolution (the future)

Internal Control



Old



Enterprise Risk Management

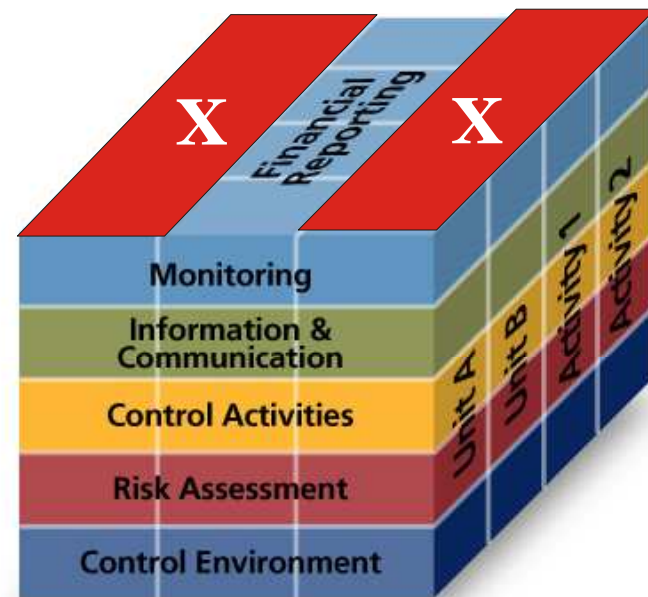


New*

Released in September 2004

IC-FR does NOT include:

- **effectiveness and efficiency** of a company's operations (except financial reporting operations), and
- **compliance** with applicable laws and regulations,
 - (except laws and regulations directly related to the preparation of financial statements)



COSO Enterprise Risk Management Framework...

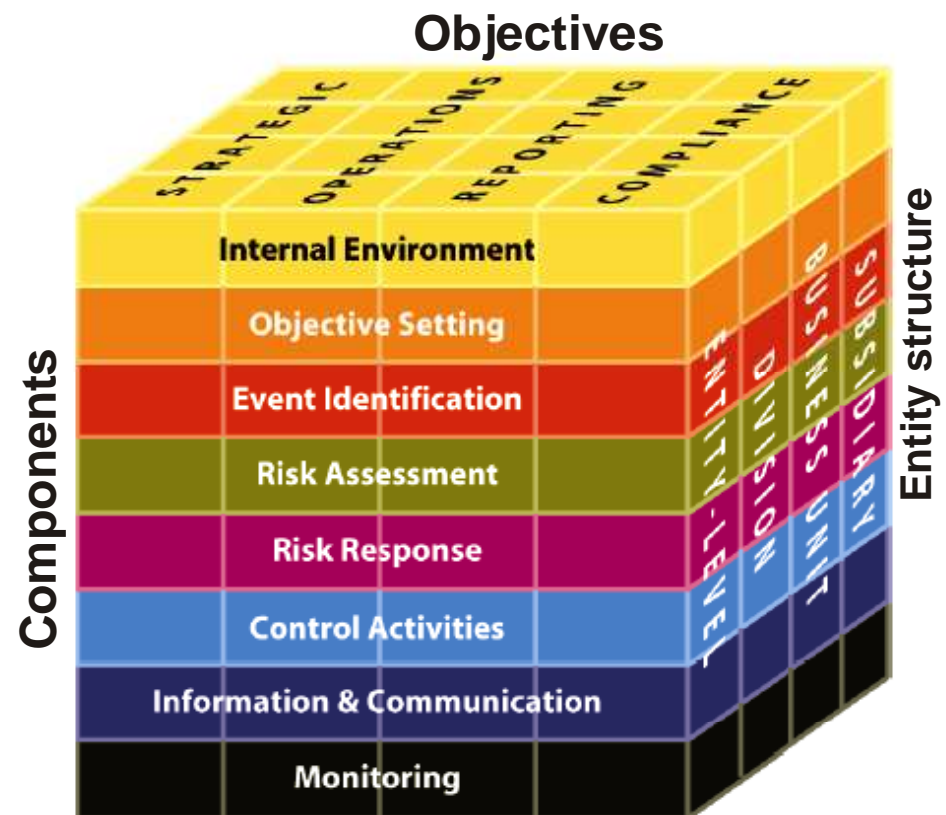
ERM is a **process**, effected by an entity's board of directors, management and other personnel,

applied in strategy setting and across the enterprise,

designed to identify potential events that may affect the entity, and

manage risks to be within its risk appetite,

to provide **reasonable assurance** regarding the achievement of entity objectives.



Source: COSO- Enterprise Risk Management Framework

ERMF: What is it (in layman's terms)?

- It is a broader and more refined extension of “Internal Control – Integrated Framework.”
- Internal control is an “integral part” of enterprise risk management.
- Because “Internal Control – Integrated Framework” is the basis for existing laws and regulations, it remains in place.

ERMF: How is it different?

- Expanded model.
- Expanded vocabulary.
- More explicit and, therefore, more practical.
- Does a better job of relating internal control to the overall management process.

Expanded Vocabulary

- Stakeholder value
- Strategic objectives
- Risks / opportunities
- Risk / desired return
- Risk philosophy
- Risk culture
- Risk appetite
- Risk profile
- Risk portfolio
- Resource allocation
- Event identification
- Risk tolerances
- Risk response alternatives
- Cross-enterprise risk
- Inherent risk
- Residual risk
- Internal environment

Span of Enterprise Risk Management

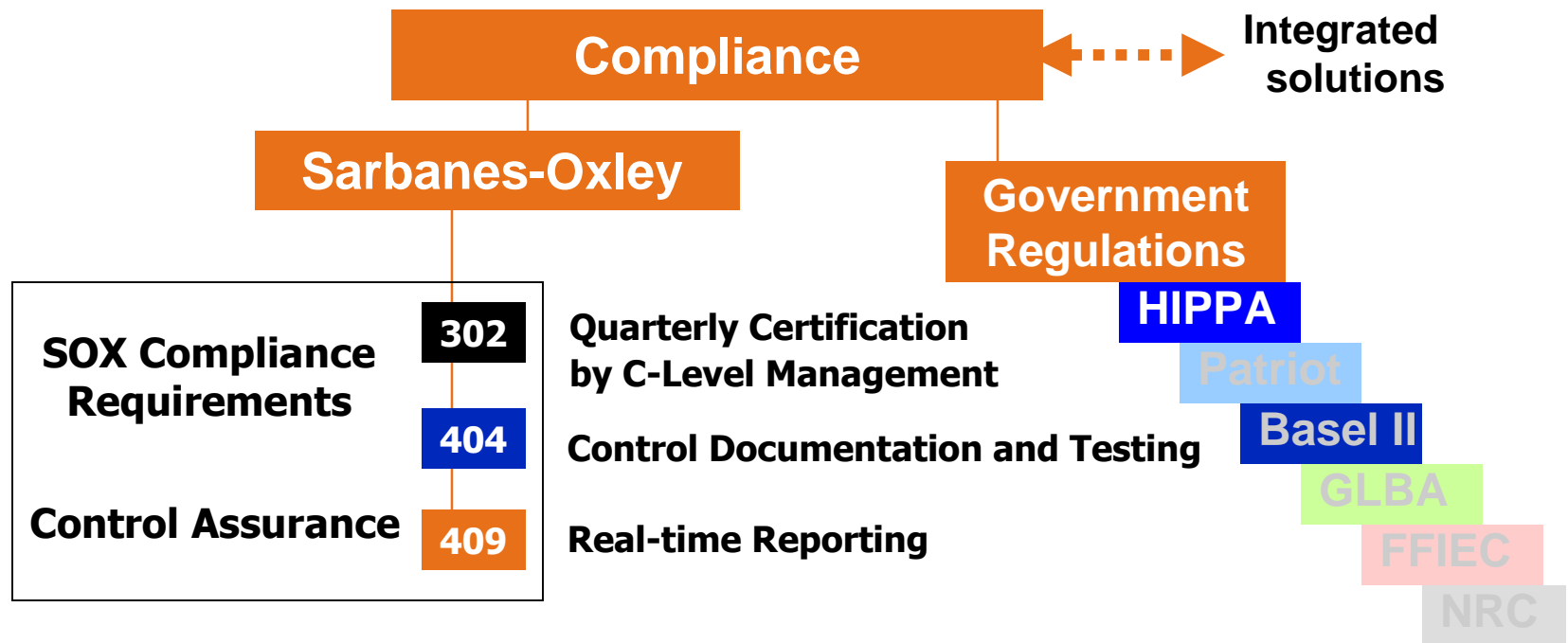
Credit Risk

Operational Risk

Market Risk

Enterprise Risk Management (ERM)

Overall compliance



What this means to you

- The reporting and effectiveness objectives are much broader in ERM than in the initial internal controls framework.
 - In the Enterprise Risk Management Framework (ERM), reporting covers all reports developed by the entity, disseminated both internally and externally, and the scope expands to include not just financial information for "financial reporting", but non-financial information as well.
- Also, unlike internal controls, ERM has "strategic" objectives, which means that the framework's objectives flow from an entity's mission or vision, and the operations, reporting and compliance objectives should be aligned with them.
- In Sum, Operational Risk Management (ORM)

Agenda

The state of “Operational Risk Management” (ORM)

A basic review

What the future holds

A simple model ORM for success moving forward



Start with an ORM Vision

“Create a culture in which all personnel manage operational risk such that all **strategic objectives** are successfully completed at the **least possible cost.**”

What is operational risk?

- Operational Risk represents the losses that follow from acts undertaken (or neglected) in carrying out business activities. Further clarified, Operational Risk can be associated with the following:
 - **People:** losses associated with intentional violation of internal policies by current or past employees.
 - **Process:** losses that have been incurred due to a deficiency in an existing procedure, or the absence of a procedure. Losses can result from human error or unintentional failure to follow an existing procedure.
 - **Systems:** losses that are caused by unintentional breakdowns in existing systems or technology.
 - **External:** losses occurring as a result of natural or man-made forces, or the direct result of a third party's action.

The ORM Concept

- All are responsible for using ORM.
- Risk is inherent in all operations.
- Risk can be controlled.
- It is impossible to control all risk.

The Compliance Culture – Is NO LONGER OK

- My job is to comply with the standard.
- I am told what the standard is.
- If I am not told, I don't usually act.
- When I am given a standard, the standard is my objective.
- When I meet a standard, that's it.

The Performance Culture – The Future

- My job is to optimize risk - to perform.
- I'm given a standard, but that is only a baseline. I use ORM to exceed it.
- Standards are only a start point.
- Meeting a standard means little. I continuously improve.

ORM Principles

- Accept no unnecessary risks.
- Make risk decisions at the appropriate level and at the appropriate time.
- Integrate ORM into planning at all levels.
- Accept risks when benefits outweigh costs.



Again....

Accept risk when benefits outweigh costs

The ORM 6 - Step Process



Using the ORM process

- Apply the steps in sequence.
- Maintain balance in the process.
- Apply the process as a cycle.
- Involve people fully.

Step 1: Identify hazards

Hazard: Any real or potential condition that can cause operational degradation, injury, illness, or death to personnel or damage to or loss of equipment, property, or other assets.



Step 1: Identify hazards

- This step starts with brainstorming.
 - Staff should identify key operational processes and list every hazard **practically** imaginable for these activities.
 - As part of this process, it is important to ensure that as part of this step, the actors, acts and technologies involved in this operation should be listed as well.



Step 1: Identify hazards, an example

- **Operational Process:** Sales Booking Process
- **Actors:** Sales Operations, Accounting
- **Acts:** Sales Operations books a sale within the Sales Registration dB. Upon completion of the registration, notification is automatically sent to Accounting where the sale is reviewed and an invoice is generated.
- **Systems:** Local workstations, Sales Registration Database, Finance and Accounting System
- **Hazards:**
 - Sales Operations deliberately/inadvertently miskeys critical information
 - Notification from Sales Registration dB to Accounting Fails, thus the invoice is not generated
 - Information is captured/sniffed and relayed to a competitor regarding the terms of the sale



Step 2: Assess Risks

The Process which associates “hazards” with “risks”.



Step 2: Assess Risks

- Go through every item on the “brainstorming list” of potential hazards associated with key processes and ask two questions:
 - How likely is it for this hazard to occur? Give the answer using one of the following probabilities
 1. Frequent
 2. Likely
 3. Occasional
 4. Seldom
 5. Unlikely
 - Given that this event does occur, how severe would it be? Give the answer using one of the following severities:
 1. Catastrophic
 2. Critical
 3. Moderate
 4. Negligible



Step 2: Assess Risks

- Once hazards have been identified and an event likelihood and severity value associated with each, it is time to “rack and stack” the risks within a “Risk Assessment Matrix”.
- Through use of this matrix, one can define, within the context of the organizational risk appetite, how much attention needs to be devoted to a particular risk.

severity	frequent A	likely B	occasional C	seldom D	unlikely E
catastrophic 1	[Red to Yellow gradient bar]				
critical 2	[Red to Green gradient bar]				
moderate 3	[Yellow to Green gradient bar]				
negligible 4	[Light Green to Green gradient bar]				
	risk levels				



Step 2: Assess Risks

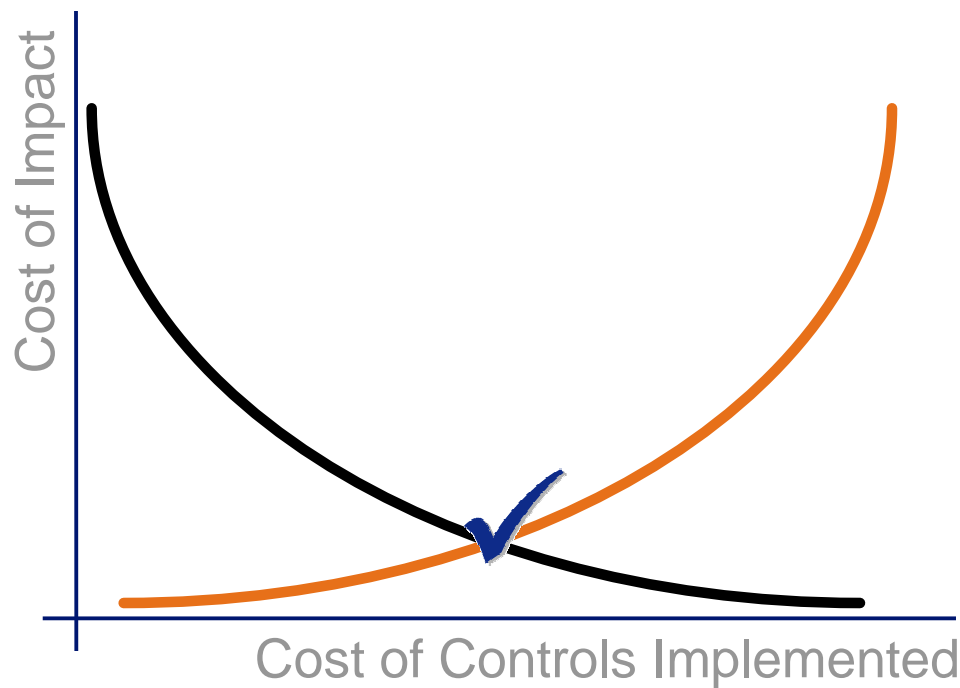
- Next, prioritize the risks by using the Risk Assessment Matrix to clearly define the risk for each defined hazard on your list.
- Using the example delineated in Step 1, the Risk Matrix would yield the following:

Potential Hazard	Probability	Severity	Code	Risk
Sales operations deliberately/inadvertently mis-keys critical information (i.e. wrong invoice address, wrong sales price)	Frequent	Critical	A2	Very high risk
Notification from Sales Registration dB to accounting fails, thus the invoice is not generated	Occasional	Critical	C2	High risk
Information is captured/sniffed and relayed to a competitor regarding the term of the sale	Unlikely	Moderate	E3	Low risk



Step 2: Assess Risks

By ranking our risks, we can approach them on a worst first basis. This is vital because risk control resources are limited and should be directed at the big problems first to assure maximum bang for the buck.



Step 2: Beware the pitfalls

- Over-optimism
- Misrepresentation
- Alarmism
- Indiscrimination
- Inaccuracy



Step 2: The Test of Maturity

In the fully mature ORM world, every individual benefits from the knowledge of the priority of risks that exist. A key obligation of managers is to see that their subordinates possess this knowledge.

- Traditional RM - Personnel can't name or prioritize risk -- can only name generic hazards.
- ORM - Personnel can name and prioritize RISKS that impact them and the operation.



Step 3: Analyze control measures



Step 3: Analyze control measures

Identify control options

Determine Control Effects

Prioritize Risk Control Efforts



Step 3, Action 1: Identify Control Options

- Tools Available:
 - The Major Risk Control Options
 - Risk Control Options Matrix



Step 3: Major Control Options

- Reject
- Accept
- Delay
- Transfer
- Mitigate
- Reduce



Step 3: Control Options matrix

- Administrative
 - Policy & Procedure
 - Train & Educate
 - Improve Task design
- Technical
 - Protect
 - Detect
 - Respond
 - Monitor
- Physical



Step 3, Action 2: Determine Control Effects

- What is the impact on probability?
- What is the impact on severity?
- What will the risk control cost?
- How will various risk control options work together (synergies)?



Step 3, Action 3: Prioritize Risk Control Measures

- Get user input.
- Focus risk controls where they have maximum impact.
- Benchmark already existing controls.



Step 3: Analyze control measures, the example

Potential Hazard	Probability	Severity	Code	Risk	Control
Sales operations deliberately/inadvertently mis-keys critical information (i.e. wrong invoice address, wrong sales price)	Frequent	Critical	A2	Very high risk	Apply dB integrity measures at the field level. Use the CRM systems to institute sign off processes
Notification from Sales Registration dB to accounting fails, thus the invoice is not generated	Occasional	Critical	C2	High risk	Monitor process using event management technology.
Information is captured/sniffed and relayed to a competitor regarding the term of the sale	Unlikely	Moderate	E3	Low risk	Institute hardware encryption solution.



Step 4: Make Control Decisions



Step 4: Make Control Decisions

Action 1:
Select Risk
Controls

Action 2:
Make Risk
Decision



Step 4, Action 1: Select Risk Controls

- Make decisions at the right time.
 - As late as possible. Why?
 - More time to improve ORM
 - The need for the risk may go away
 - But never too late
 - Radically increase costs.
- Make decisions at the right level.
 - Who will take the heat if it goes bad?
 - Who has the best grasp of the risk and the opportunity issues?
 - Who can commit the risk control resources?



Step 4: Always remember

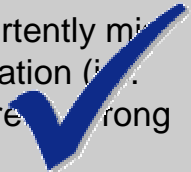

Push the average risk decision down the hierarchy wherever possible

- WHY? Because the detail and understanding of the implications of the decision increases the closer to the operator you get...

BUT... Make sure you are using the same taxonomy. Example:
What does the term “internal control” mean to an average IT guy?



Step 4, Action 2: Make Risk Decisions

Potential Hazard	Probability	Severity	Code	Risk	Control
Sales operations deliberately/inadvertently miskeys critical information (e.g. wrong invoice address, wrong sales price) 	Frequent	Critical	A2	Very high risk	Apply dB integrity measures at the field level. Use the CRM systems to institute sign off processes
Notification from Sales Registration dB to accounting fails, thus the invoice is not generated	Occasional	Critical	C2	High risk	Monitor process using even management technology.
Information is captured/sniffed and relayed to a competitor regarding the term of sale 	Unlikely	Moderate	E3	Low risk	Institute hardware encryption solution.

- Use a cost benefit analysis
 - Always reject the risk when total costs outweigh total benefits.



Step 5: Implement Risk Controls



Step 5: Implement Risk Controls

Action 1:
Clarify
implementation

Action 2:
Establish
accountability

Action 3:
Provide
support



Step 5: Risk Controls should be fully integrated

- Should be integrated fully within the plans, processes, and operations with which they are associated.
- Within the area in which they are integrated, risk controls should compete for resources and time based on their relative significance to the mission of the corporation.
- Risk control should be compatible with the “system”.



Step 5: Why should controls be fully integrated?

- Integration captures more of the knowledge and experience of large numbers of in-house operators.
- Integration reduces the number and diversity of consultants needed to do the job right.
- Integration eliminates redundancy and gaps between functions.
- Integration strengthens accountability.
- Integration reduces costs and workloads.



Step 6: Supervise and Review



Step 6: Supervise and Review

Action 1:
Supervise

Action 2:
Review

Action 3:
Feedback



Step 6: Supervise and Review

- Things to Remember:
 - Use rates and numbers when they have a sound statistical basis.
 - Use direct measures of risk to supplement rates and numbers or when rates and numbers are not statistically valid.
 - Systematically assess the results of the ORM process in lessons learned sessions, etc. Was the benefit worth the cost?
 - Adapt and reapply ORM as necessary.



Summary

- Risk is inherent in all organizations.
- To meet these corporate governance regulations an enterprise must implement a framework for identifying and managing risk beyond financial reporting.
- Not only can they mitigate this risk by implementing ORM, but they can also maximize business performance throughout the organization.
- The ORM vision is to create an environment where all personnel manage operational risk, and all strategic objectives are completed at the least possible cost to the organization.
- ORM raises the bar—a compliance culture is no longer acceptable.



Questions?