Operational Risk – An Enterprise Risk Management Presentation

Enterprise risk management

- Significant increase in risks faced by people and organizations
- Corporate governance and disclosure rules, along with the independent board of directors rapidly gaining importance among companies
- Increasing pressure from rating agencies to establish a strong risk management focus in the company
- ERM vital element in most corporations.
- ORM important part of ERM

Operational Risk Management

- Operational risk:
  - Expected and unexpected economic impact of inadequate or failed internal processes, people, system or external events
  - Should be minimized
  - Affects other risks

Operational risk management

- ORM role:
  - Ensure operational risks identified and effectively and efficiently managed
  - Reduce risk to predefined limits in cost-effective manner
  - Ensure legal requirements and internally set limits are followed

Operational risk management

- The ORM structure:
  - Clearly defined
  - Clearly identifies roles and responsibilities
    - Risk owners
    - Risk takers
    - Risk controllers

Operational risk management

- Five key steps of ORM process:
  - Identification and classification
  - Assessment, measurement and mitigation
  - Monitoring and assurance
  - Reporting
  - Steering decisions

Operational risk management

- Elements supporting ORM
  - Risk and control self assessment
  - Key risk indicators
  - Loss-event database
  - Audits
  - SOX
  - ORM awareness

ORM: Risk and control self assessment

- Risk and control self assessment (RCSA) as management tool to
  - Identify
  - Assess
  - Measure
  - Mitigate
- Organization's needs determine level of detail
- Several RCSA systems currently available

ORM: Risk and control self assessment

- Identification and classification of operational risks
  - Identify events that could have a significant negative financial or reputational impact on the company
  - Basel II four risk categories:
    - Process
    - People
    - System
    - External events
  - Usefulness of common definitions and descriptions of risks and risk categories

ORM: Risk and control self assessment

- Identification of controls
  - Key objective: reduce operational risk exposure to acceptable level
  - Preventive and detective controls
  - Recommend no more than six to eight controls per risk
- Possible mitigation of more than one risk by the same control

ORM: Risk and control self assessment

- Assessment
  - Operational risk exposure
    - Severity: most likely monetary loss in the absence of any internal controls
    - Frequency: how often an event of at least the size of severity is expected to occur in the absence of any internal controls
    - Inherent risk: risk measure in the absence of internal controls
    - Residual risk: remaining level of risk after controls in place.

ORM: Risk and control self assessment

- Inherent risk value
  - Identify significant potential loss exposure
  - Identify areas requiring mitigation activities
- Residual risk value
  - Identify inadequate control

– Focus of remediation activities

- Areas with residual risk value outside acceptable limits.

ORM: Risk and control self assessment

- Control assessment
  - Control design effectiveness
    - Level of risk mitigation
    - Rated: very high, high, medium and low
  - Control operating effectiveness
    - Operational control quality in practice
    - Rated: fully effective (“green”), partially effective (“amber”), or not effective (“red”)
- Effective, well-designed controls
  - Reduce the expected loss
  - Reduce the standard deviation of that loss

ORM: Risk and control self assessment

- Measurement
  - Failure rates of control design and control operating effectiveness together with severity and frequency of inherent risk
    - Allow to calculate expected annual loss amounts for every residual risk
    - Basis for calculating required capital for operational risk

ORM: Risk and control self assessment

- Mitigation
  - Compare expected losses with a predefined risk acceptance limit
  - Raise an issue and/or an action plan
  - Take an appropriate mitigation steps

ORM: Key risk indicators

- Key risk indicators (KRI)
  - Measures that provide information about organization or levels of activity indicating potential or actual changes in risk exposure
  - One of the basic elements of an effective ORM
  - Identify areas requiring management attention and/or action
  - Monitor changes in risk profile and controls performance
  - Require meaningful benchmark and margins

ORM: Loss-event database

- Loss event database
  - Loss event: occurrence that leads to a financial cost, lost benefit or both.
  - A loss event database
    - Captures losses and incidents
    - Serves as
      - Learning tool
      - Input to risk quantification

ORM: Audits

- Audits
  - Crucial function of ORM
  - Through audits, operational processes can be checked, issues raised and corrective action determined.
  - Internal or external audits
  - Good control of company operations by thoughtful audit coverage planning and execution
  - Significant help in managing risks through reporting audits' activities, substandard results, and follow up on an audits' open issues

ORM: Sarbanes-Oxley Act

- Sarbanes-Oxley Act (SOX)
  - Introduced by US Congress in 2002 after major US corporate scandals.
  - Compliance with Act by all publicly-traded companies in US
  - One of primary goals to help restore investor confidence.
  - SOX important part of operational risk management process.
  - Compliance with SOX enhances management of operational risks.

ORM:
Sarbanes-Oxley Act

- SOX compliance requirement:
  - All applicable companies must establish financial accounting framework that can generate financial reports readily verifiable with traceable source data.
  - Source data must remain intact and cannot undergo undocumented revisions.
  - Revisions to financial or accounting software must be fully documented

ORM awareness

- ORM awareness
  - Essential part of effective risk management.
  - Raised throughout company by implementing open operational risk culture:
    - Employees openly report operational risks and losses
    - Active learning from mistakes encouraged
  - Active promotion with full support, engagement of senior management, board of directors

- Increased awareness of operational risks triggered by corporate failures made operational risk management integral part of every company
- Shareholders, regulators, and rating agencies dictate tight control to minimize related losses
- Implementing assurance framework helps utilize best practices and provides proactive response to avoid future scandals

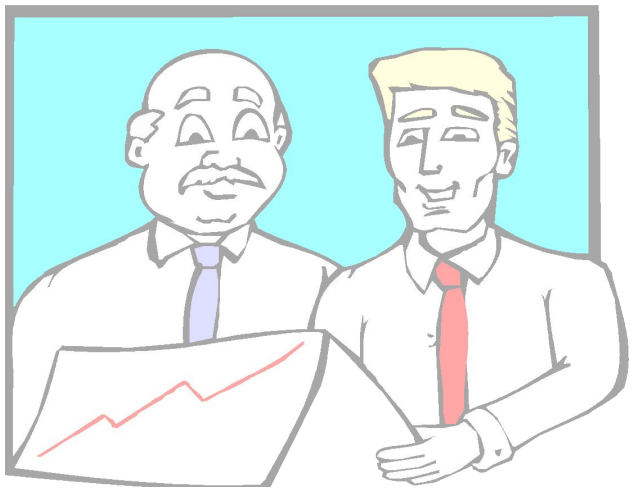
Why ORM?

To Ensure Necessary Risks are Taken

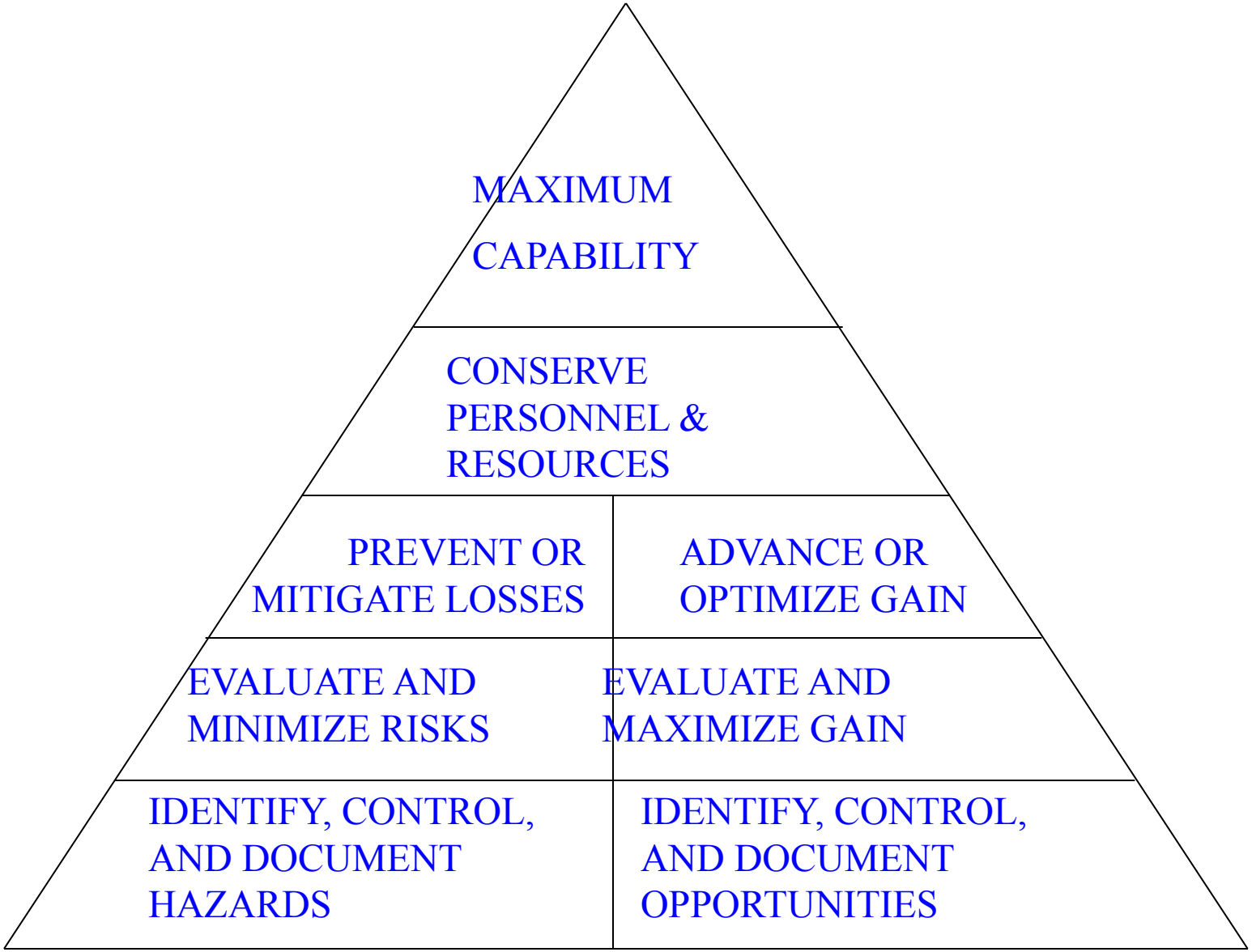
- ORM:
  - Is an important tool for training realism
  - Provides potential to expand capabilities
  - Assures necessary risk taking to enhance superiority

What is Operational Risk Management?

- Natural evolution from traditional risk management
- Systematic decision-making tool that balances risk cost & benefits



OBJECTIVE AND GOALS



4 KEY ORM PRINCIPLES

1. Accept no unnecessary risks.
2. Make risk decisions at the appropriate level.
3. Accept risks when benefits outweigh costs.
4. Integrate ORM into doctrine and planning at all levels.

1. Accept No Unnecessary Risks

BUT.... NOBODY TAKES "UNNECESSARY" RISKS?

If all the hazards that could have been detected have not been detected then unnecessary risks are being accepted.

The single greatest advantage of ORM over traditional risk management is the consistent detection of 50%+ more hazards.

2. Make Risk Decisions at the Appropriate Level

Factors below become basis of a decision-making system to guide leaders

- Who will answer in the event of a mishap?
- Who is the senior person at the scene?
- Who possesses best insight into the full benefits and costs of a risk?
- Who has the resources to mitigate the risk?
- What level makes the most operational sense?
- What level makes these types of decisions in other activities?
- Who will have to make this decision in combat operations?

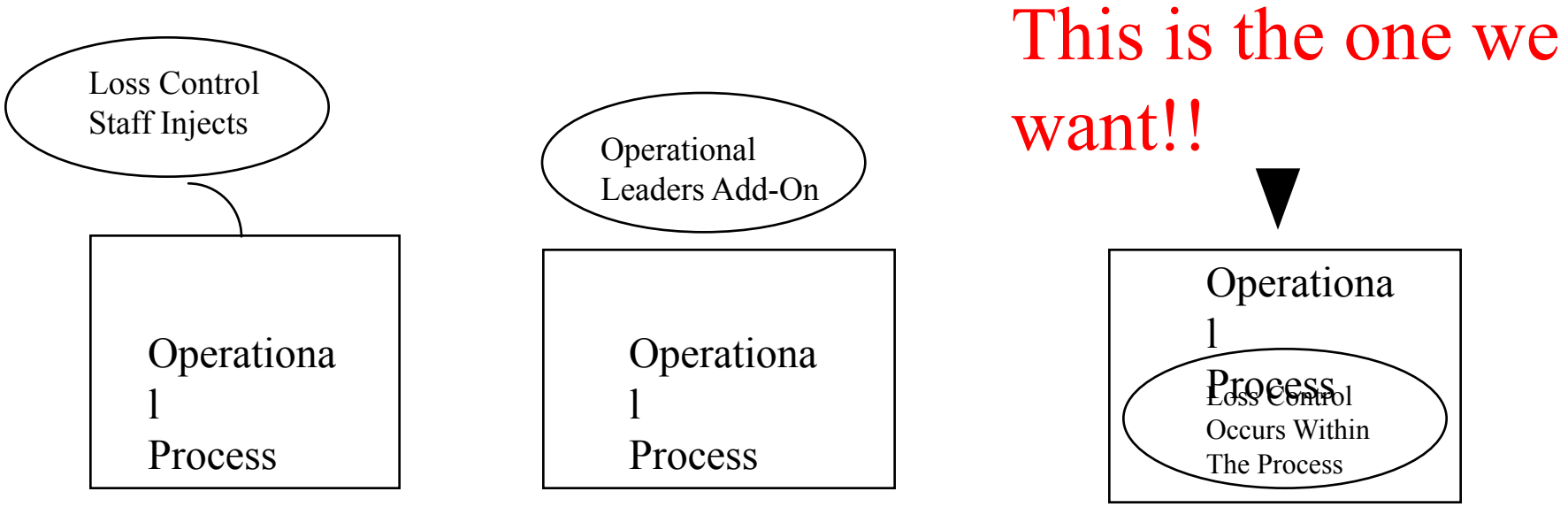
3. Accept Risks When Benefits Outweigh Costs.

WHAT HAPPENS WHEN AN ORGANIZATION STOPS TAKING RISKS?

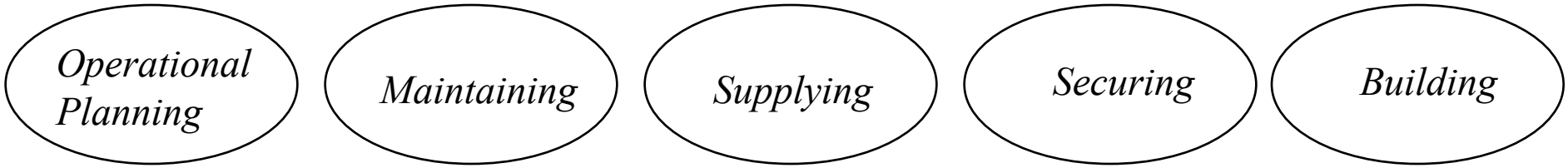
WEBSTER: "BUREAUCRACY: A system of administration characterized by lack of initiative and flexibility, by indifference to human needs or public opinion, and by a tendency to defer decisions to superiors or to impede action with red tape."

MAINTAINING A BOLD, RISK-TAKING ORGANIZATION IS ALWAYS A CHALLENGE WHEN YOUR UNIT IS NOT ON A MISSION. ORM HELPS.

4. Integrate ORM Into Doctrine and Planning At All Levels.

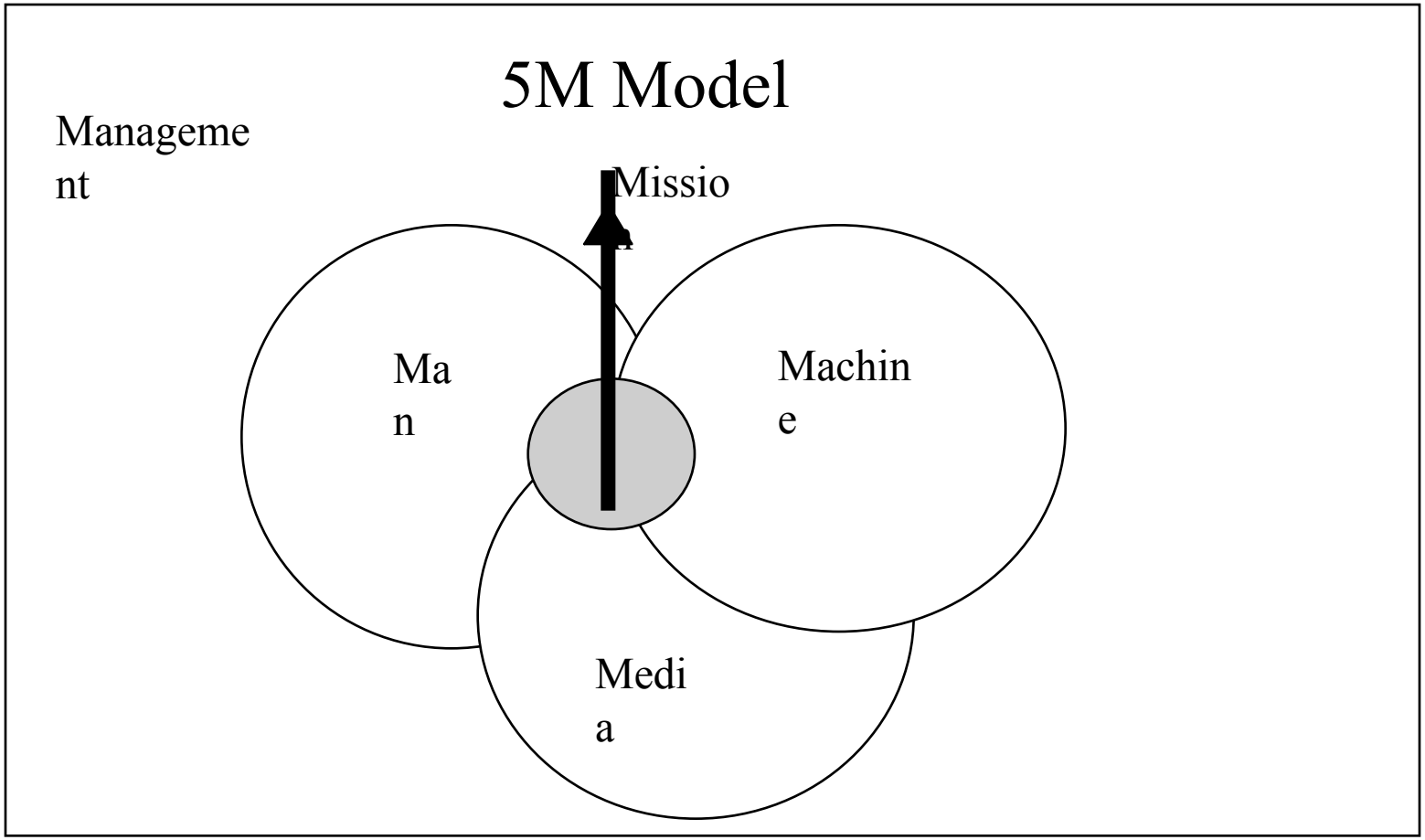


WHAT IS AN "OPERATIONAL PROCESS"?

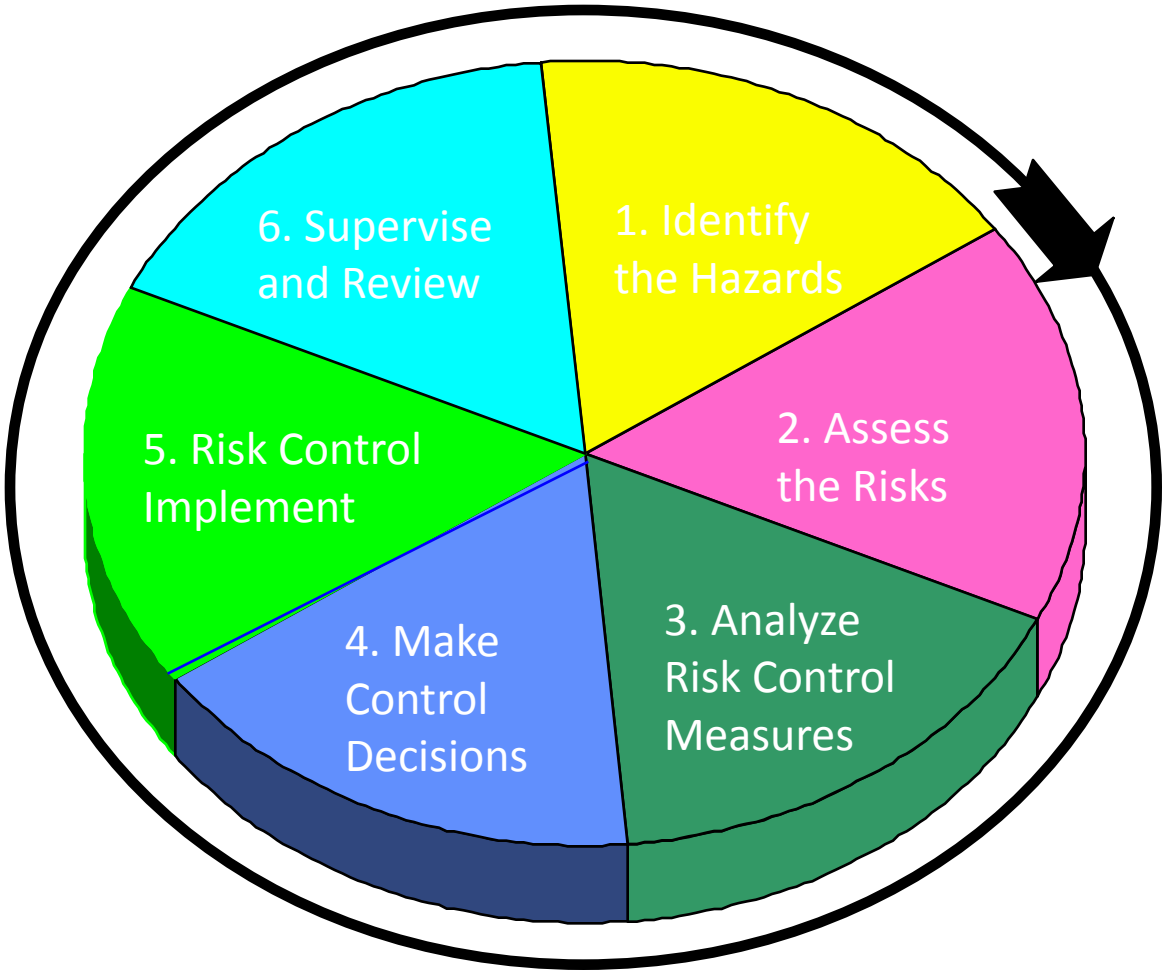


and all their sub-processes

ORM IS BASED ON SYSTEMS MANAGEMENT CONCEPTS



THE ORM 6-STEP PROCESS



Step 1 - Identify the Hazard

Process: Emphasize hazard ID tools. Adds rigor and early detection.

Output: Significant (50%+) improvement in the detection of hazards.

7 Primary Hazard ID Tools

BROAD RANGE OF APPLICATION AT ANY LEVEL

- Operations Analysis/Flow Diagram
- Preliminary Hazard Analysis
- What If
- Scenario
- Logic Diagrams
- Change Analysis
- Cause and Effect

Specialized and Advanced Hazard ID Tools

- Specialized tools accomplish specific ORM objectives.

  Map analysis, interface analysis, mission protection tools, training realism, opportunity assessment

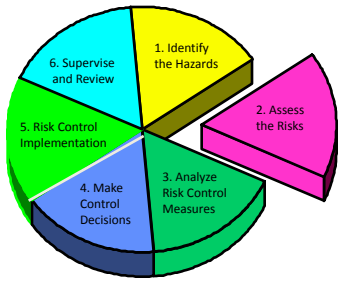
- Advanced tools are used by specialists and professionals to add depth to ORM applications

EXAMPLE:
THE DRIVE TO WORK

WHAT IF ANALYSIS

- What if the car catches fire.
- What if a carjack is attempted.
- What if I have to take an unknown detour.
- What if I run out of gas.
- What if another car rear ends me.

Step 2 - Assess the Risk



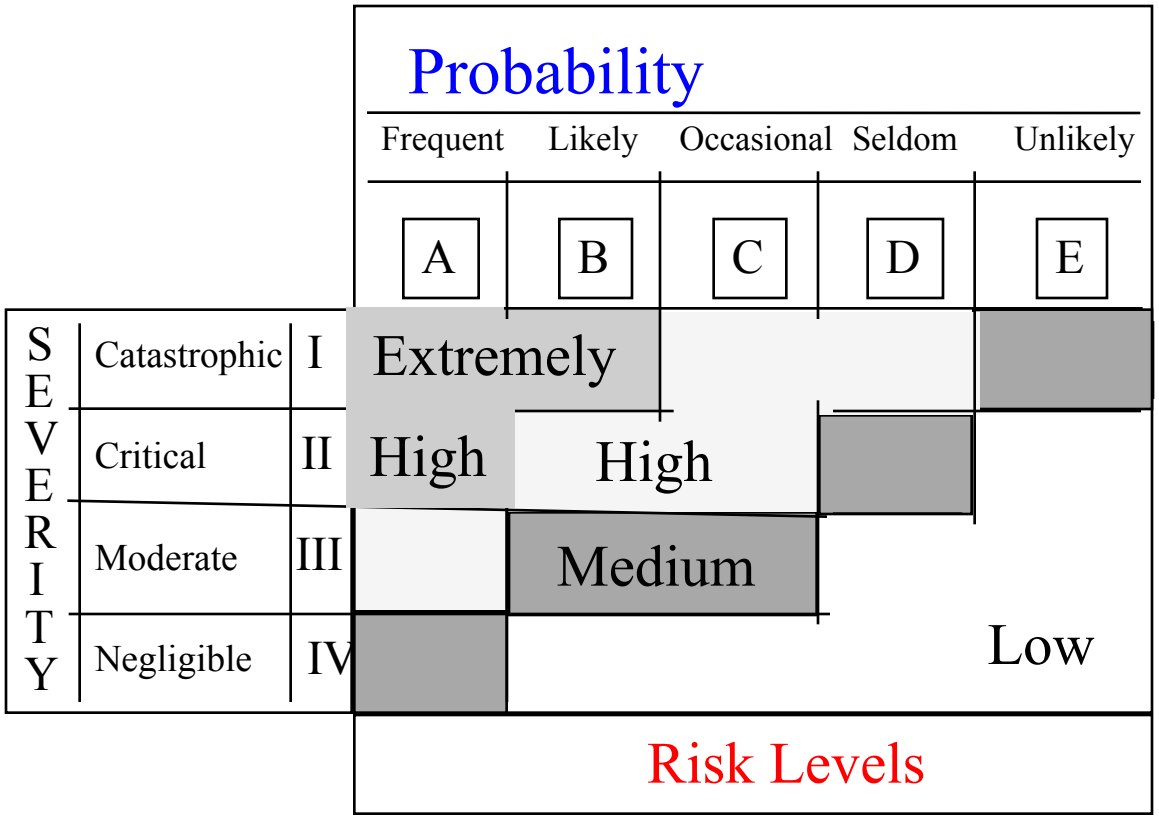
Process: All hazards evaluated for total impact on mission or activity. Root causes determined and risk levels assigned (EH, H, M, L)

Output: Personnel throughout the organization know the priority risk issues of the command and of their function.

THE ASSESSMENT TOOLS ADD OBJECTIVITY TO THE EVALUATION OF RISK

- Risk assessment matrix: Requires specific evaluations of severity, probability, and when necessary, exposure
- Totem pole: Induces the prioritization of risk issues across functions and across the organization

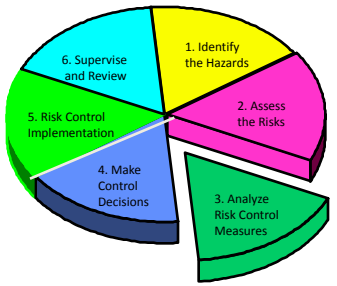
THE RISK ASSESSMENT MATRIX
KEY TOOL FOR RISK ASSESSMENT



EXAMPLE:
THE DRIVE TO WORK

MED	• What if the car catches fire.
HIGH	• What if a carjack is attempted.
LOW	• What if I have to take an unknown detour.
MED	• What if I run out of gas.
MED	• What if another car rear ends me.

Step 3 - Analyze Risk Control Measures



Process: Comprehensive risk control options are developed for risks based on a worst-first basis.

Output: A full range of cost effective, mission supportive, risk controls for the consideration of the decision maker.

The Risk Control Option Tools Add Scope & Depth

- Basic or "macro" risk control options: Reject, Avoid, Delay, Transfer, Spread, Accept, Compensate, Reduce

- Risk control options matrix: 46 specific "reduce-focused" control options - applicable at up to four levels in the organization

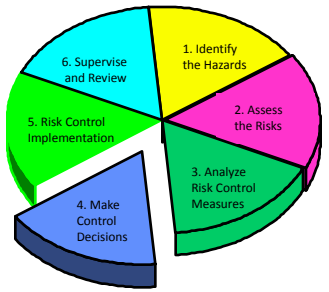
EXAMPLE:
THE DRIVE TO WORK

What if the car catches fire MEDIUM

Macro options:

- Transfer - Insurance
- Reduce (use Control Options Matrix) -
  - Engineer gas tank
  - Drive defensively
  - Focused maintenance
  - Emergency response plan & equipment

Step 4 - Make Control Decisions



Process: A decision-making system gets risk decisions to the right person, at the right time, with the right support.

Output: Personnel know their decision-making authority and limitations and take necessary risks.

ORM Uses Proven Decision-making Tools

- Decision-making systems get the decision to the right person, at the right time, with the right support
- Basic cost benefit and return on investment analysis assure maximum benefit for the risk control $
- Decision-making matrices and other modern decision-making tools improve decision quality
- The leader question list induces better staff inputs

ESTABLISHING A DECISION MAKING GUIDELINE

EXAMPLE

RISK LEVEL	DECISION LEVEL
Extremely High	Wing Commander or specifically authorized designee
High	Group Commander or specifically authorized designee
Medium	Flight leader, or senior leader on the scene
Low	Any person in a leadership position

EXAMPLE:
THE DRIVE TO WORK

What if the car catches fire MEDIUM

Who decides: Vehicle owner(s)

Control: Emergency response plan & equipment

Decision:

Cost of loss	Cost of control
$500 - Deductible	$15 Fire extinguisher
Rate increase?	
Car down-time	
Repair/Replacement hassle	

Step 5 - Risk Control Implementation

Process: Leaders lead, operators are involved, all are accountable.

Output: ORM initiatives always have positive mission impact.

ORM Implementation Tools & Guidelines Help Controls Click with Operators

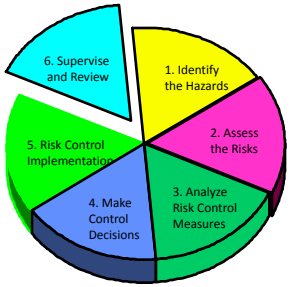
- The involvement continuum guides the high degree of operator input to ORM actions
- The leader involvement actions list and the leader opportunity job aid help assure effective leader influence
- The motivation model makes application of modern behavior management techniques easier

EXAMPLE:
THE DRIVE TO WORK

What if the car catches fire MEDIUM

- Transfer - Insurance OPR: Dad
- Reduce -
  - Engineer gas tank OPR: Ford
  - Drive defensively OPR: Driver
  - Focused maintenance OPR: Dad
  - Emergency response plan & equipment OPR: Team Mom & Dad

Step 6 - Supervise and Review



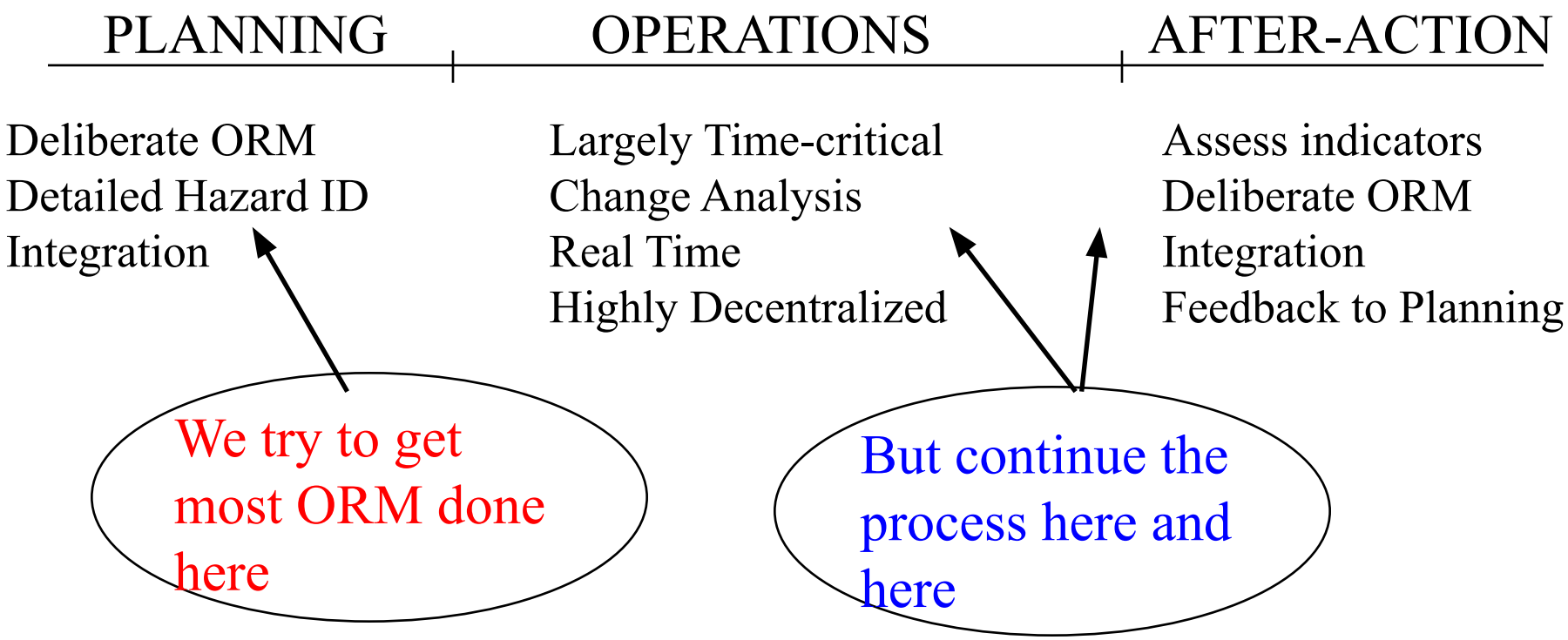
Process: Progress measured through increased mission effectiveness, mishap results and direct indicators of risk.

Output: ORM performance status determined real time.

Review and Feedback Procedures
Measure & Leverage ORM Results

- Eliminate invalid statistical uses of mishap rates and numbers
- Refocus measurement on direct measures of risk (critical behaviors, knowledge, conditions, etc.)
- Radically improve the effectiveness of feedback systems through modern data and communications systems

USING THE 6-STEP PROCESS
THE RISK MANAGEMENT CONTINUUM



USING THE 6-STEP PROCESS
LEVELS OF EFFORT

TIME CRITICAL DELIBERATE STRATEGIC

Little Time Resources Risk

Lot of Time Resources Risk

SELECTED PRIMARY PRIMARY SPECIALIZED ADVANCED

Integrating the ORM Process

Overview

- Why integration is critical?
- 12 Strategies for ORM integration.
- The importance of pace.

WHY INTEGRATION IS CRITICAL?

Integration:

- Forces balancing of loss control and other mission needs
- Captures more of the knowledge and experience of large numbers of operators
- Reduces the number and diversity of references needed to do the job right
- Eliminates redundancy and gaps between loss control functions
- Strengthens accountability
- Reduces costs and workloads (in plans, materiel development cycles, etc.)

THE TWELVE STRATEGIES FOR PROGRAM INTEGRATION

1. Accountability
2. Teaming
3. Partnership
4. Integrate in Training
5. Risk Decision Points
6. Organization & Policy Structure
7. Employee Activities
8. Process Integration
9. Direct Change
10. Gain a Champion
11. Integrate in Strategic Planning
12. Integrate into Measurement

THE IMPORTANCE OF PACE

- Don't use the shotgun
- Don't get out in front of the organization - too far
- Don't "inspect-in" ORM

- Do focus on "targets"
- Do expect crawl, walk, run
- Patience, patience, patience

USAF ORM MATURATION

- Vision
- USAF Approach
- Background
- Strategy

VISION

Macro: Every Leader, Member, & Employee Manages Risk in All They Do... *On- & Off-Duty*

Micro:

On-Duty - Every Organization Manages Normal Operational Risk Profile

- Unique Operations Identified & Assessed

Off-Duty - Every Individual Applies Risk Management Process to Activities

CAP APPROACH

- Top-Down Approach
- Strong Senior Leader Backing
- Decentralized Implementation
- Moderate Implementation Tempo
- Safety Lead Role for Cross-Functional Implementation

ORM STRATEGY
Miscellaneous Initiatives

- Automated “Tools”
- Doctrine Integration
- Crosstell
- NEWS Release(s)
- Video(s)

The leader's role will be a decisive factor in the success or failure of ORM

ORM Leadership Opportunities

1. Commit to Breakthrough Improvement

Objectives: Put improvement of risk performance (control-opportunity) on a competitive level with other important mission concerns.

2. Set Goals & Objectives

Objectives: Establish periodic ORM performance and programmatic goals.

ORM Leadership Opportunities Continued

3. Set a Personal Example

Objectives: To assure credibility of the ORM process through personal behavior.

4. Build an Aggressive Opportunity Mindset in the Organization

Objectives: Create an organization as conscious of the opportunity aspects of ORM as it is the risk reduction

ORM Leadership Opportunities Continued

5. Induce Loss Control Community Functional Integration

Objectives: Build increasing cooperation and integration of the loss control community

6. Establish an ORM Management Structure

Objectives: Provide the necessary leadership and staff resources to adequately guide the ORM process

ORM Leadership Opportunities Continued

7. Resource ORM Activities

Objectives: Allocate resources to ORM (control-opportunity) at a level it can competitively justify

8. Heat Shield Subordinates

Objectives: Protect subordinates who have taken prudent, mission supportive risks, but experienced severe losses, from negative consequences.

ORM Leadership Opportunities Continued

9. Detect & Correct Gambling

Objectives: Develop an organization in which risk "gambling" is deterred even when the gambler "wins".

10. Use the Power of Question

Objectives: Use pointed ORM questions to induce ORM activity and culture change.

ORM Leadership Opportunities Continued

11. Regularly Monitor ORM Progress

Objectives: Periodically assess a set of data that effectively monitors organization ORM status

12. Exploit the ORM Value of Major Mishap Reviews

Objectives: Consistently induce consideration of the ORM implications of mishaps

Definition

Basel II – *Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk, but excludes strategic and reputation risk*.

Definition

Who are these people?

What does this have to do with us?

Definition

Basel Committee on Banking Supervision – Committee of banking supervisory authorities that provides a forum for cooperation on bank supervisory matters and encourages convergence towards common approaches and standards. It also frames guidelines and standards for banks and bank supervisors.

Basel Accords – Recommendations on banking laws and regulation

Definition

Basel II was intended to create an international standard for banking regulators to control how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

Basel II lists three types of risk:

- Credit risk
- Market risk
- Operational risk

What about liquidity risk?

Definition

Market liquidity is the risk that a security can not be sold at all or quickly enough to prevent a loss.

Market liquidity risk is a type of market risk. It is addressed in Basel III.

Funding liquidity risk is the risk that liabilities can not be met when due.

Funding liquidity risk is an operational risk.

Definition

Solvency II codifies and harmonizes EU insurance regulation.

Solvency II definition - *Operational risk means the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events. [It] shall include legal risks, and exclude risks arising from strategic decisions, as well as reputation.*

Definition

Legal risk - risk of loss due to legal actions or uncertainty in the applicability or interpretation of contracts, laws, or regulations. Included.

Strategic risk – risk arising from decisions concerning a company's direction. Excluded.

Reputational risk - risk related to the trustworthiness of the company. Excluded.

Definition

Better definition - *Operational risk is the risk arising from execution of a company's business function.*

This focuses on the risks arising from people, processes, and systems.

Note that it includes external events that affect a company's operations.

Definition

Operational risk does not include strategic risk – the risk that arises from decisions concerning a company's objectives.

Reputational risk may arise from operational risk but is not, in and of itself, an operational risk. It also can arise from credit risk, market risk, and strategic risk.

Operational risk is not used to generate profit, whereas market risk, credit risk, and strategic risk can do so.

Types of Operational Risk

Basel II List

Internal fraud – misappropriation of assets, tax evasion, intentional mismarking of positions, bribery

External fraud – theft of information, hacking damage, third party theft and forgery

Employment practices and workplace safety – discrimination, workers' compensation, employee health and safety

Clients, products, and business practice – market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning

Damage to physical assets – natural disasters, terrorism, vandalism

Business disruption and system failures – utility disruptions, software failures, hardware failures

Executive, delivery, and process management – data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

Legal risk is in several of these categories.

Types of Operational Risk

Operational risk losses usually are idiosyncratic to a particular institution.

Operational risk losses most commonly are from a failure of internal controls.

Internal operational risk losses arise from errors and ineffective operations.

Operational Risk Management Framework

Basel II

Risk organizational and governance structure

Policies, procedures and processes

Systems used by a bank in identifying, measuring, monitoring, controlling and mitigating operational risk

Operational risk measurement system (ORMS) – systems and data used to measure operational risk to estimate the operational risk charge

Operational Risk Management Framework

Enterprise Risk Management Steps

1. Identify risks
2. Describe and/or quantify risks
3. Decide how to mitigate risks
4. Implement decisions
5. Monitor results of decisions and make changes as needed

Communication is key.

Operational Risk Management Framework

Basel II differentiates between verification and validation.

Verification tests the effectiveness of the overall ORMF and tests ORMS validation processes to ensure they are independent and implemented consistent with bank policies.

Validation ensures that the ORMS is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes, and outputs.

Operational Risk Management Framework

Essential elements for verification and validation:

Independence

Capacity – adequately staffed with adequate resources

Professional competence and due diligence

Quantification

Basel Committee on Banking Supervision "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches" June 2011

Operational risk data categories for Advanced Measurement Approaches:

- Internal loss data (ILD)
- External data (ED)
- Scenario analysis (SA)
- Business environment and internal controls factors (BEICF)

Quantification

It all starts with scenarios.

Ask “What if…?”

Don’t know what internal and external data to collect unless you have some idea of what scenarios you need to look at.

Data includes qualitative as well as quantitative.

Qualitative data sometimes is more important than quantitative, particularly when there are recent changes.

Quantification

Internal Loss Data (ILD)

Internal to the organization

Used to estimate loss frequencies

Used to inform the severity distribution(s)

Serves as input into the scenario analysis

Quantification

External Data (ED)

External to the organization

Used to estimate loss severity, particularly for the tail

May be from a consortium of like members

(Association of British Insurers' Operational Risk Consortium – www.abioric.com)

Quantification

Scenario Analysis (SA)

Scenario outputs form part of the input into the Advanced Measurement Approach model

Qualitative

Produce range of results

Quantify uncertainty arising from scenario biases – This is a significant challenge.

Quantification

Business Environment and Internal Controls Factors (BEICF)

Highly subjective

Often used as indirect input into the quantification framework

Often used as an *ex post* adjustment to model output

Mitigation

Goals

Have business continuity

Mitigate financial loss

Reduce reputational risk

Mitigation

The size of loss a company is willing to accept compared to the cost of correcting errors or improving operations determines its operational risk appetite.

Most effective means of reducing operational risk are sound policies, practices, and procedures for internal events and insurance for external and some internal events.

Mitigation

Low frequency, low severity – may do nothing.

Low frequency, high severity – analyze by scenario testing. Handled by planning for these in advance and/or by financing risk such as by purchasing insurance.

High frequency, low severity – may do nothing. However these can accumulate to the point where the severity becomes larger, such as if it triggers a loss of reputation.

High frequency, high severity – take risk control measures. May finance risk such as by purchasing insurance.

Mitigation

Insurance companies sell products that mitigate others' operational risks.

Mitigation

Basel Committee on Banking Supervision - “Principles for the Sound Management of Operational Risk” June 2011

Internal controls embedded in day-to-day operations are designed to ensure to the extent possible that:

Activities are efficient and effective

Information is reliable, timely and complete

The entity is compliant with applicable laws and regulation.

Mitigation

Three lines of defense:

- Business line management
- An independent corporate operational risk management function
- An independent review

Monitoring

Key Performance Indicator (KPI) – Are we achieving our desired level of performance?

Key Risk Indicators (KRI) – How is our risk profile changing and is it within our desired tolerance levels?

Key Control Indicators (KCI) – Are our organization's internal controls effective?

Risk Identification and Mitigation Examples

Fine Dining Restaurant

Family owned
Open only for dinner Monday through Saturday
Seats 80 at a time for two seatings a night
Private party room upstairs
Owner is one of the managers on duty but is also a chef
Has a general manager and one other manager on duty
Has two part-time office staff and one cleaner
Has an Executive Chef, two Line Chefs, one Dessert Chef
Has two expediters and two dishwashers
Has three captains, six waiters, six bussers, and one bartender
Has one hostess and one coat checker
Subcontracts car parking

Risk Identification and Mitigation Examples

Fine Dining Restaurant

Internal policies, practices, and procedures

- What can go wrong in the front of the house?
- What can go wrong in the kitchen?
- What can go wrong in the office?
- What can go wrong elsewhere?
- What communication problems can there be?

External events

- What could negatively affect the restaurant?

Risk Identification and Mitigation Examples

Large Taxi Company

In major city
Owned by one private investor
No Board of Directors
One garage location
Owns 500 cabs
Has 1,000 drivers
Has 20 mechanics in own repair shop
Has own gas station and car wash
Has 5 dispatchers
Has 10 office staff including CEO, COO, and CFO positions

Risk Identification and Mitigation Examples

Large Taxi Company

Internal policies, practices, and procedures

- What can go wrong on the streets?
- What can go wrong in the repair shop?
- What can go wrong with the gas station and car wash?
- What can go wrong with dispatching?
- What can go wrong in the office?
- What can go wrong elsewhere?
- What communication problems can there be?

External events

- What could negatively affect the company?

Risk Identification and Mitigation Examples

Insurance Company

Privately held
Much of board is family members
Writes automobile liability and physical damage for taxis in large city
Recently had large business expansion
Is moving from low-tech to high-tech back office
Uses independent agents to write business

Risk Identification and Mitigation Examples

Insurance Company

- Internal policies, practices, and procedures
  - What can go wrong with the agents?
  - What can go wrong with customer service?
  - What can go wrong with underwriting?
  - What can go wrong with claim handling?
  - What can go wrong with data processing?
    - Increased inefficiency due to data overload
    - Compliance risk if data not protected
    - Privacy risk
    - Security risk

Risk Identification and Mitigation Examples

Insurance Company

- Internal policies, practices, and procedures (continued)
  - What can go wrong with accounting?
  - What can go wrong with investing?
  - What can go wrong with reinsurance?
  - What can go wrong with the Board of Directors?
  - What can to wrong with the owners?
  - What can go wrong elsewhere?
  - What communication problems can there be?
- External events
  - What could negatively affect the company?

Risk Identification and Mitigation Examples

Insurance Company

Operational risk losses usually are idiosyncratic to a particular institution.

Very highly automated back-office systems – exposure to IT operational risks

Low tech back office – exposure to people and process operational risks

Words of Wisdom

Strategic decisions affect operations.

Have an “open door” policy.

Manage by walking around.

“Good reason” versus “real reasons.”

When someone presents a problem, they must also present a possible solution or be willing to participate in finding a solution.

Words of Wisdom

Some processes need to be “hard-wired” in: no exceptions.

Manage by exception. Use those to improve processes and systems.

Allow people to make exceptions that are in the company’s long-term best interest.

Cross train.

Words of Wisdom

Be aware of what is going on outside the company:

- Clients/customers
- Service providers
- Competitors
- Related industries
- General population – demographics, work environments, socially
- Technology innovation
- Accounting standards
- Politically
- Judicially
- Legislatively
- With the country in general
- With the world in general

Words of Wisdom

Be more proactive than reactive.

Keep an open mind.

See what is really there.

Be prepared.

Be flexible.

Communicate, communicate, communicate.

Operational Risk – An ERM Presentation

Definition - *Operational risk is the risk arising from execution of a company's business function.*

Types of Operational Risk

Operational Risk Management Framework

Quantification

Mitigation

Monitoring

Risk Identification and Mitigation Examples

Words of Wisdom