Chapter 15: Operational Risk Management (ORM)

15.0 Operational Risk Management (ORM)

15.1 Defining Risk and Risk Management

ORM is a decision-making tool to systematically help identify operational risks and benefits and determine the best courses of action for any given situation. In contrast to an Operational and Support Hazard Analysis (O&SHA), which is performed during development, ORM is performed during operational use. For example, an ORM might be performed before each flight. This risk management process, as other safety risk management processes is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare.

Risk management, as discussed throughout this handbook is pre-emptive, rather than reactive. The approach is based on the philosophy that it is irresponsible and wasteful to wait for an accident to happen, then figuring out how to prevent it from happening again. We manage risk whenever we modify the way we do something to make our chances of success as great as possible, while making our chances of failure, injury or loss as small as possible. It's a common-sense approach to balancing the risks against the benefits to be gained in a situation and then choosing the most effective course of action.

Often, the approach to risk management is highly dependent on individual methods and experience levels and is usually highly reactive. It is natural to focus on those hazards that have caused problems in the past. In the FAA's operational environment where there is a continual chance of something going wrong, it helps to have a well-defined process for looking at tasks to prevent problems. Operational Risk Management, or ORM, is a decision-making tool that helps to systematically identify risks and benefits and determine the best courses of action for any given situation. ORM is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare.

Risk is defined as the probability and severity of accident or loss from exposure to various hazards, including injury to people and loss of resources. All FAA operations in the United States, and indeed even our personal daily activities involve risk, and require decisions that include risk assessment and risk management. Operational Risk Management (ORM) is simply a formalized way of thinking about these things. ORM is a simple six-step process, which identifies operational hazards and takes reasonable measures to reduce risk to personnel, equipment and the mission.

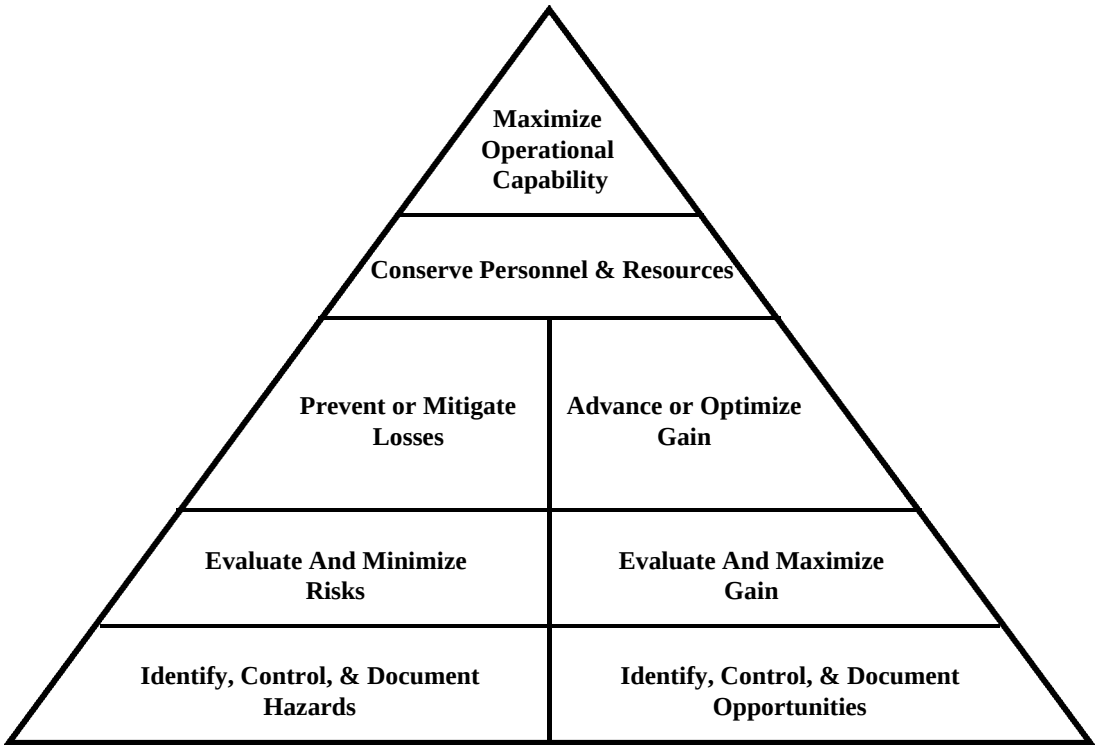
In FAA operations, decisions need to take into account the significance of the operation, the timeliness of the decision required, and what level of management is empowered to make the decision. Risk should be identified and managed using the same disciplined process that governs other aspects of the Agency's endeavors, with the aim of reducing risk to personnel and resources to the lowest practical level.

Risk management must be a fully integrated part of planning and executing any operation, routinely applied by management, not a way of reacting when some unforeseen problem occurs. Careful determination of risks, along with analysis and control of the hazards they create results in a plan of action that anticipates difficulties that might arise under varying conditions, and pre-

determines ways of dealing with these difficulties. Managers are responsible for the routine use of risk management at every level of activity, starting with the planning of that activity and continuing through its completion.

Figure 15-1 illustrates the objectives of the ORM process: protecting people, equipment and other resources, while making the most effective use of them. Preventing accidents, and in turn reducing losses, is an important aspect of meeting this objective. In turn, by minimizing the risk of injury and loss, we ultimately reduce costs and stay on schedule. Thus, the fundamental goal of risk management is to enhance the effectiveness of people and equipment by determining how they are most efficiently to be used.

Figure 15-1: Risk management Goal



15.2 ORM Principles

Four principles govern all actions associated with operational risk management. These continuously employed principles are applicable before, during and after all tasks and operations, by individuals at all levels of responsibility.

Accept No Unnecessary Risk:

Unnecessary risk is that which carries no commensurate return in terms of benefits or opportunities. Everything involves risk. The most logical choices for accomplishing an operation are those that meet all requirements with the minimum acceptable risk. The corollary to this axiom is "accept necessary risk," required to successfully complete the operation or task.

Make Risk Decisions at the Appropriate Level:

Anyone can make a risk decision. However, the appropriate decision-maker is the person who can allocate the resources to reduce or eliminate the risk and implement controls. The decision-maker must be authorized to accept levels of risk typical of the planned operation (i.e., loss of operational effectiveness, normal wear and tear on materiel). He should elevate decisions to the next level in the chain of management upon determining that those controls available to him will not reduce residual risk to an acceptable level.

Accept Risk When Benefits Outweigh the Costs:

All identified benefits should be compared against all identified costs. Even high-risk endeavors may be undertaken when there is clear knowledge that the sum of the benefits exceeds the sum of the costs. Balancing costs and benefits is a subjective process, and ultimately the balance may have to be arbitrarily determined by the appropriate decision-maker.

Integrate ORM into Planning at all Levels:

Risks are more easily assessed and managed in the planning stages of an operation. The later changes are made in the process of planning and executing an operation, the more expensive and time-consuming they will become.

15.3 The ORM Process Summary

The ORM process comprises six steps, each of which is equally important. Figure 15-2 illustrates the process.

Figure 15-2: ORM's 6 Process Steps

Step 1: Identify the Hazard

A hazard is defined as any real or potential condition that can cause degradation, injury, illness, death or damage to or loss of equipment or property. Experience, common sense, and specific analytical tools help identify risks.

Step 2: Assess the Risk

The assessment step is the application of quantitative and qualitative measures to determine the level of risk associated with specific hazards. This process defines the probability and severity of an accident that could result from the hazards based upon the exposure of humans or assets to the hazards.

Step 3: Analyze Risk Control Measures

Investigate specific strategies and tools that reduce, mitigate, or eliminate the risk. All risks have three components: probability of occurrence, severity of the hazard, and the exposure of people and equipment to the risk. Effective control measures reduce or eliminate at least one of these. The analysis must take into account the overall costs and benefits of remedial actions, providing alternative choices if possible.

Step 4: Make Control Decisions

Identify the appropriate decision-maker. That decision-maker must choose the best control or combination of controls, based on the analysis of step 3.

Step 5: Implement Risk Controls

Management must formulate a plan for applying the controls that have been selected, then provide the time, materials and personnel needed to put these measures in place.

Step 6: Supervise and Review

Once controls are in place, the process must be periodically reevaluated to ensure their effectiveness. Workers and managers at every level must fulfill their respective roles to assure that the controls are maintained over time. The risk management process continues throughout the life cycle of the system, mission or activity.

15.4 Implementing the ORM Process

To derive maximum benefit from this powerful tool, it must be used properly. The following principles are essential.

Apply the steps in sequence

Each step is a building block for the next, and must be completed before proceeding to the next. If a hazard identification step is interrupted to focus upon the control of a particular hazard, other, more important hazards may be overlooked. Until all hazards are identified, the remainder of the process is not effective.

Maintain a balance in the process

All six steps are important. Allocate the time and resources to perform them all.

Apply the process in a cycle

The “supervise and review” step should include a brand-new look at the operation being analyzed, to see whether new hazards can be identified.

Involve people in the process

Be sure that the risk controls are mission supportive, and that the people who must do the work see them as positive actions. The people who are actually exposed to risks usually know best what works and what does not.

15.5 Risk versus Benefit

Risk management is the logical process of weighing the potential costs of risks against the possible benefits of allowing those risks to stand uncontrolled.

15.5.1 Types of Risk Defined

Identified risk: That risk that has been determined to exist using analytical tools. The time and costs of analysis efforts, the quality of the risk management program, and the state of the technology involved affect the amount of risk that can be identified.

Unidentified risk: That risk that has not yet been identified. Some risk is not identifiable or measurable, but is no less important for that. Mishap investigations may reveal some previously unidentified risks.

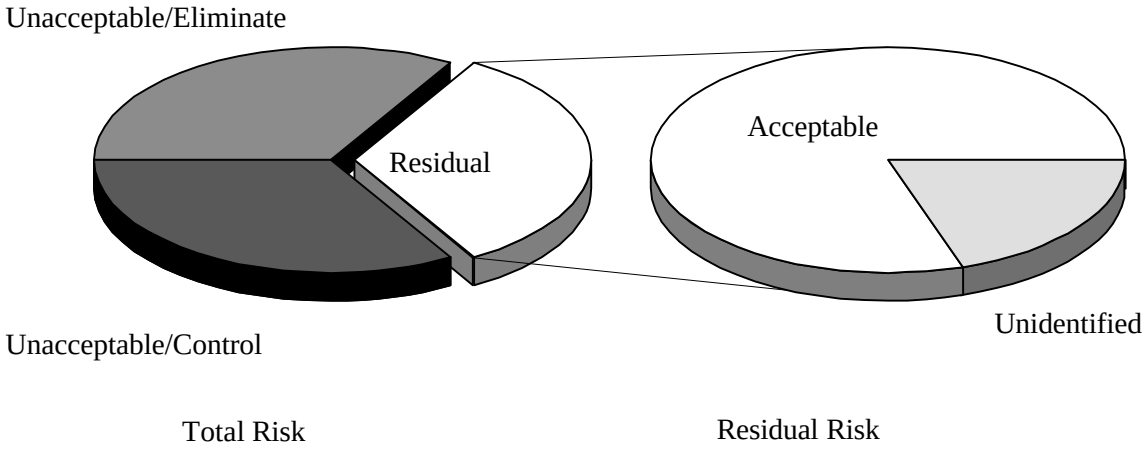
Total risk: The sum of identified and unidentified risk. Ideally, identified risk will comprise the larger proportion of the two.

Acceptable risk: The part of identified risk that is allowed to persist after controls are applied. Risk can be determined acceptable when further efforts to reduce it would cause degradation of the probability of success of the operation, or when a point of diminishing returns has been reached.

Unacceptable risk: That portion of identified risk that cannot be tolerated, but must be either eliminated or controlled.

Residual risk: The portion of total risk that remains after management efforts have been employed. Residual risk comprises acceptable risk and unidentified risk.

Figure 15-3: Types of Risk



15.5.2 Benefits Defined

Benefits are not limited to reduced mishap rates or decreased injuries, but may also be realized as increases in efficiency or mission effectiveness. Benefits are realized through prudent risk-taking. Risk management provides a reasoned and repeatable process that reduces the reliance on intuition.

15.6 Acceptability of Risk

Risk management requires a clear understanding of what constitutes unnecessary risk, i.e., when benefits actually outweigh costs. Accepting risk is a function of both risk assessment and risk management, and is not as simple a matter as it may first appear. Several principles apply:

- Some degree of risk is a fundamental reality
- Risk management is a process of tradeoffs
- Quantifying risk does not in itself ensure safety
- Risk is often a matter of perspective
- Realistically, some risk must be accepted. How much is accepted, or not accepted, is the prerogative of the defined decision authority. That decision is affected by many inputs. As tradeoffs are considered and operation planning progresses, it may become evident that some of the safety parameters are forcing higher risk to successful operation completion. When a manager decides to accept risk, the decision should be coordinated whenever practical with the affected personnel and organizations, and then documented so that in the future everyone will know and understand the elements of the decision and why it was made.

15.7 General Risk Management Guidelines

- All human activity involving technical devices or complex processes entails some element of risk.
- Hazards can be controlled; they are not a cause for panic.
- Problems should be kept in perspective.
- Judgments should be based upon knowledge, experience and mission requirements.
- Encouraging all participants in an operation to adopt risk management principles both reduces risk and makes the task of reducing it easier.
- Good analysis tilts the odds in favor of safe and successful operation.
- Hazard analysis and risk assessment do not replace good judgment: they improve it.
- Establishing clear objectives and parameters in risk management works better than using a cookbook approach.
- No one best solution may exist. Normally, there are a variety of alternatives, each of which may produce a different degree of risk reduction.
- Tact is essential. It is more productive to show a mission planner how he can better manage risk than to condemn his approach as unworkable, risky, unsafe or unsound.
- Seldom can complete safety be achieved.
- There are no “safety problems” in planning or design, only management problems that may cause accidents, if left unresolved.

15.8 Risk Management Responsibilities

15.8.1 Managers

- Are responsible for effective management of risk.
- Select from risk reduction options recommended by staff.
- Accept or reject risk based upon the benefit to be derived.
- Train and motivate personnel to use risk management techniques.
- Elevate decisions to a higher level when it is appropriate.

15.8.2 Staff

- Assess risks and develop risk reduction alternatives.
- Integrate risk controls into plans and orders.
- Identify unnecessary risk controls.

15.8.3 Supervisors

- Apply the risk management process
- Consistently apply effective risk management concepts and methods to operations and tasks.
- Elevate risk issues beyond their control or authority to superiors for resolution.

15.8.4 Individuals

- Understand, accept and implement risk management processes.
- Maintain a constant awareness of the changing risks associated with the operation or task.
- Make supervisors immediately aware of any unrealistic risk reduction measures or high-risk procedures.

15.9 Systematic Risk Management: The 5-M Model

Successful operations do not just happen; they are indicators of how well a system is functioning. The basic cause factors for accidents fall into the same categories as the contributors to successful operations—Human, Media, Machine, Mission, and Management.

Risk management is the systematic application of management and engineering principles, criteria and tools to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all operational phases. To apply the systematic risk management process, the composite of hardware, procedures, and people that accomplish the objective, must be viewed as a system.

The 5-M model, depicted in Figure 15-4, is adapted from military ORM. In this model, "Man" is used to indicate the human participation in the activity, irrespective of the gender of the human involved. "Mission" is the military term that corresponds to what we in civil aviation call "operation." This model provides a framework for analyzing systems and determining the relationships between the elements that work together to perform the task.

The 5-M's are Man, Machine, Media, Management, and Mission. Man, Machine, and Media interact to produce a successful Mission (or, sometimes, an unsuccessful one). The amount of overlap or interaction between the individual components is a characteristic of each system and evolves as the system develops. Management provides the procedures and rules governing the interactions between the other elements.

When an operation is unsuccessful or an accident occurs, the system must be analyzed; the inputs and interaction among the 5-Ms must be thoroughly reassessed. Management is often the controlling factor in operational success or failure. The National Safety Council cites the management processes in as many as 80 percent of reported accidents.

15.9.1 Man

The human factor is the area of greatest variability, and thus the source of the majority of risks.

Selection: The right person psychologically and physically, trained in event proficiency, procedures and habit patterns.
Performance: Awareness, perceptions, task saturation, distraction, channeled attention, stress, peer pressure, confidence, insight, adaptive skills, pressure/workload, fatigue (physical, motivational, sleep deprivation, circadian rhythm).
Personal Factors: Expectancies, job satisfaction, values, families/friends, command/control, perceived pressure (over tasking) and communication skills.

15.9.2 Media

Media are defined as external, and largely environmental and operational conditions. For example:

Climatic: Ceiling, visibility, temperature, humidity, wind, precipitation.
Operational: Terrain, wildlife, vegetation, human made obstructions, daylight, and darkness.
Hygienic: Ventilation/air quality, noise/vibration, dust, and contaminants.
Vehicular/Pedestrian: Pavement, gravel, dirt, ice, mud, dust, snow, sand, hills, curves.

15.9.3 Machine

Hardware and software used as intended, limitations interface with man.

Design: Engineering reliability and performance, ergonomics.
Maintenance: Availability of time, tools, and parts, ease of access.
Logistics: Supply, upkeep, and repair.
Technical data: Clear, accurate, useable, and available.

15.9.4 Management

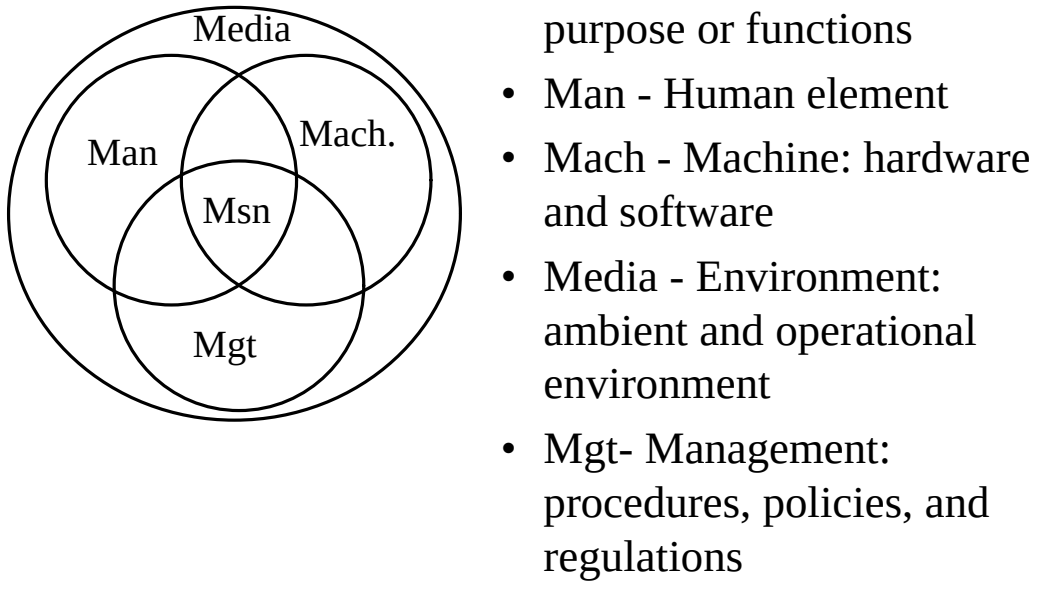
Directs the process by defining standards, procedures, and controls. Although management provides procedures and rules to govern interactions, it cannot completely control the system elements. For example: weather is not under management control and individual decisions affect personnel far more than management policies.

Standards: FAA Policy and Orders.
Procedures: Checklists, work cards, and manuals.
Controls: Crew rest, altitude/airspeed/speed limits, restrictions, training rules/limitations.
Operation. The desired outcome.

15.9.5 Mission (Operation)

Objectives: Complexity understood, well defined, obtainable. The results of the interactions of the other -M's (Man, Media, Machine, and Management).

Figure 15-4: The 5-M Model



15.10 Levels of Risk Management

The risk management process operates on three levels. Although it would be preferable to perform an in-depth application of risk management for every operation or task, the time and resources may not always be available. The three levels are as follow:

15.10.1 Time-Critical

Time-critical risk management is an "on the run" mental or verbal review of the situation using the basic risk management process without necessarily recording the information. This time-critical process of risk management is employed by personnel to consider risk while making decisions in a time-compressed situation. This level of risk management is used during the execution phase of training or operations as well as in planning and execution during crisis responses. It is also the most easily applied level of risk management in off-duty situations. It is particularly helpful for choosing the appropriate course of action when an unplanned event occurs during execution of a planned operation or daily routine.

15.10.2 Deliberate

Deliberate Risk Management is the application of the complete process. It primarily uses experience and brainstorming to identify risks, hazards and develops controls and is therefore most effective when done in a group. Examples of deliberate applications include the planning of upcoming operations, review of standard operating, maintenance, or training procedures, and damage control or disaster response planning.

15.10.3 Strategic

This is the deliberate process with more thorough hazard identification and risk assessment involving research of available data, use of diagram and analysis tools, formal testing, or long term tracking of the risks associated with the system or operation (normally with assistance from technical experts). It is used to study the hazards and their associated risks in a complex operation or system, or one in which the hazards are not well understood. Examples of strategic applications include the long-term planning of complex operations, introduction of new equipment, materials and operational, development of tactics and training curricula, high risk facility construction, and major system overhaul or repair. Strategic risk management should be used on high priority or high visibility risks.

15.11 ORM Process Expansion

Many aspects of the ORM process utilize the same risk management tools described throughout this handbook. There are some unique contributions and issues in the ORM process which are expanded in this section.

15.11.1 Hazard identification expansion

Hazard identification, the foundation of the entire ORM process, and ans analysis of control measures require further expansion. Figure 15-3 depicts the actions necessary to identify hazards. Specifically, identify hazards associated with these three categories:

Operational or System Degradation.
Injury or Death.
Property Damage.

Action 1—Task Analysis

The 5-M's are examined. This is accomplished by reviewing current and planned operations. Management defines requirements and conditions to accomplish the tasks. Construct a list or chart depicting the major phases of the operation or steps in the job process, normally in time sequence. Break the operation down into 'bite size' chunks.

Some tools that will help perform operation/task analysis are:

Operations Analysis/Flow Diagram
Preliminary Hazard Analysis (PHA)
Multi-linear Events Sequence (MES)

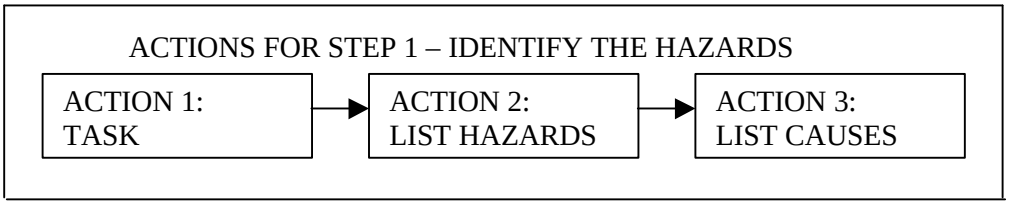
Action 2—List Hazards

Hazards are identified based on the deficiency to be corrected and the definition of the operation and system requirements. The output of the identification phase is a listing of inherent hazards or adverse conditions and the accidents, which could result. Examples of inherent hazards in any one of the elements include fire, explosion, and collision with ground, wind, or electrocution. The analysis must also search for factors that can lead to hazards such as alertness, ambiguity, or escape route. In addition to a hazard list for the elements above, interfaces between or among these elements should be investigated for hazards. Make a list of the hazards associated with each phase of the operation or step in the job process. Stay focused on the specific steps in the operation being analyzed. Try to limit your list to "big picture" hazards. Hazards should be tracked on paper or in a computer spreadsheet/database system to organize ideas and serve as a record of the analysis for future use. Tools that help list hazards are:

Preliminary Hazard Analysis
"What if" Tool
Scenario Process Tool

Logic Diagram
Change Analysis Tool
Opportunity Assessment
Training Realism Assessment.

Figure 15-3. Identify Hazards Actions



Action 3—List Causes

Make a list of the causes associated with each hazard identified in the hazard list. A hazard may have multiple causes related to each of the 5-M's. In each case, try to identify the root cause (the first link in the chain of events leading to operational degradation, personnel injury, death, or property damage). Risk controls can be effectively applied to root causes. Causes should be annotated with the associated hazards in the same paper or computer record mentioned in the previous action. The same tools for Action 2 can be used here.

Strategic Tools

If time and resources permit, and additional hazard information is required, use strategic hazard analysis tools. These are normally used for medium and long term planning, complex operations, or operations in which the hazards are not well understood.

The first step of in-depth analysis should be to examine existing databases or available historical and hazard information regarding the operation. Suggested tools are:

Accident analysis
Cause and effect diagrams

The following tools are particularly useful for complex, coordinated operations in which multiple units, participants, and system components and simultaneous events are involved:

Multi-linear event sequence (MES).
Interface analysis.
Failure mode and effect analysis.

The following tools are particularly useful for analyzing the hazards associated with physical position and movement of assets:

Mapping tool.
Energy trace and barrier analysis.
Interface analysis.

SEVEN PRIMARY HAZARD IDENTIFICATION TOOLS

- **THE OPERATIONS ANALISIS**
- **THE PRELIMINARY HAZARD ANALYSIS**
- **THE WHAT IF TOOL**
- **THE SENARIO PROCESS TOOL**
- **THE LOGIC DIAGRAM**
- **THE CHANGE ANALYSIS**
- **THE CAUSE AND EFFECT TOOL**

Figure 15-4: The Primary Family of Hazard Identification Tools

There are many additional tools that can help identify hazards. One of the best is through a group process involving representatives directly from the workplace. Most people want to talk about their jobs, therefore a simple brainstorming process with a facilitator is often very productive. The following is a partial list of other sources of hazard identification information:

Accident/Incident Reports: These can come from within the organization, for it represents memory applicable to the local workplace, cockpit, flight, etc. Other sources might be NTSB reports, medical reports, maintenance records, and fire and police reports.

Operational Personnel: Relevant experience is arguably the best source of hazard identification. Reinventing the wheel each time an operation is proposed is neither desired nor efficient. Seek out those with whom you work who have participated in similar operations and solicit their input.

Outside Experts: Look to those outside your organization for expert opinions or advice.

Current Guidance: A wealth of relevant direction can always be found in the guidance that governs our operations. Consider regulations, operating instructions, checklists, briefing guides, SOPs, NOTAMs, and policy letters.

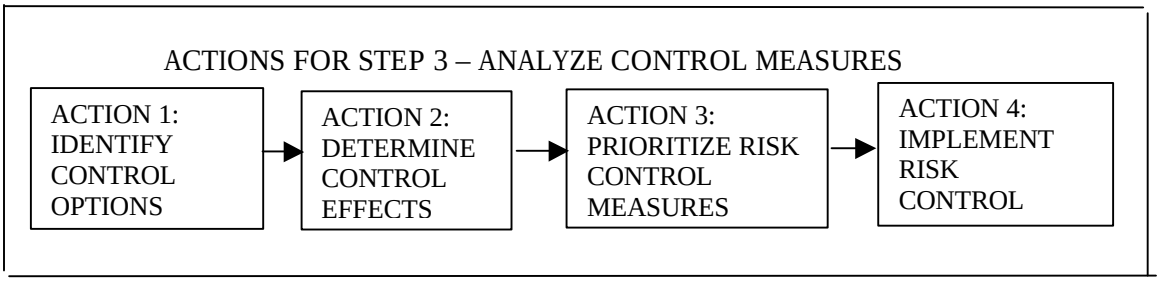
Surveys: The survey can be a powerful tool because it pinpoints people in the operation with first hand knowledge. Often, first line supervisors in the same facility do not have as good an understanding of risk as those who confront it every day.

Inspections: Inspections can consist of spot checks, walk-through, checklist inspections, site surveys, and mandatory inspections. Utilize staff personnel to provide input beyond the standard third-party inspection.

15.11.2 Analyze Control Measures

Hazard control is accomplished in several ways. Figure 15-5 depicts the actions necessary to analyze the alternatives.

Figure 15-5. Analyze Control Measures Actions



Action 1—Identify Control Options

Starting with the highest-risk assessed, identify as many risk control options as possible for all hazards. Refer to the list of possible causes from Step 1 for control ideas. The Control Options Matrix and "What-If" analyses are excellent tools to identify control options. Risk control options include: ***rejection, avoidance, delay, transference, spreading, compensation,*** and ***reduction***.

Action 2—Determine Control Effects

Determine the effect of each control on the risk associated with the hazards. A computer spread sheet or data form may be used to list control ideas and indicate control effects. The estimated value(s) for severity and/or probability after implementation of control measures and the change in overall risk assessed from the Risk Assessment Matrix should be recorded. Scenario building and next accident assessment provides the greatest ability to determine control effects.

Action 3—Prioritize Risk Controls/ Measures

For each risk, prioritize those risk controls that will reduce the risk to an acceptable level. The best controls will be consistent with objectives and optimize use of available resources (manpower, material, and equipment, money, time). Priorities should be recorded in some standardized format for future reference. Opportunity assessment, cost versus benefit analysis and computer modeling provide excellent aids to prioritize risk controls. If the control is already implemented in an established instruction, document, or procedure, that too should be documented.

The "standard order of precedence" indicates that the ideal action is to “plan or design for minimum risk” with less desirable options being, in order, to add safety devices, add warning devices, or change procedures and training. This order of preference makes perfect sense while the system is still being designed, but once the system is fielded this approach is frequently not cost effective. Redesigning to eliminate a risk or add safety or warning devices is both expensive and time consuming and, until the retrofit is completes, the risk remains unabated.

Normally, revising operational or support procedures may be the lowest cost alternative. While this does not eliminate the risk, it may significantly reduce the likelihood of an accident or the severity of the outcome (risk) and the change can usually be implemented quickly. Even when a redesign is planned, interim changes in procedures or maintenance requirements are usually required. In general, these changes may be as simple as improving training, posting warnings, or improving operator or technician qualifications. Other options include preferred parts substitutes, instituting or changing time change requirements, or increased inspections.

The feasible alternatives must be evaluated, balancing their costs and expected benefits in terms of operational performance, dollars and continued risk exposure during implementation. A completed risk assessment should clearly define these tradeoffs for the decision-maker.

Some Special Considerations in Risk Control. The following factors should be considered when applying the third step of ORM.

Try to apply risk controls only in those activities and to those who are actually at risk. Too often risk controls are applied indiscriminately across an organization leading to wasted resources and unnecessary irritation of busy operational personnel.
Apply redundant risk controls when practical and cost effective. If the first line of defense fails, the back up risk control(s) may prevent loss.
Involve operational personnel, especially those likely to be directly impacted by a risk control, in the selection and development of risk controls whenever possible. This involvement will result in better risk controls and in general a more positive risk control process.
Benchmark (find best practices in other organizations) as extensively as possible to reduce the cost associated with the development of risk controls. Why expend the time and resources necessary to develop a risk control and then have to test it in application when you may be able to find an already complete, validated approach in another organization?
Establish a timeline to guide the integration of the risk control into operational processes.

Action 4 — Implement Risk Controls

Once the risk control decision is made, assets must be made available to implement the specific controls. Part of implementing control measures is informing the personnel in the system of the risk management process results and subsequent decisions. If there is a disagreement, then the decision-makers should provide a rational explanation. Careful documentation of each step in the risk management process facilitates risk communication and the rational processes behind risk management decisions. Figure 15-6 depicts the actions necessary to complete this step.

Figure 15-6: Actions to Implement Risk Controls

ACTIONS FOR STEP 4—IMPLEMENT RISK CONTROLS

Step 1—Make Implementation Clear

To make the implementation directive clear, consider using examples, providing pictures or charts, including job aids, etc. Provide a roadmap for implementation, a vision of the end-state, and describe successful implementation. The control measure must be deployed in a method that insures it will be received positively by the intended audience. This can best be achieved by designing in user ownership.

Step 2—Establish Accountability

Accountability is an important area of ORM. The accountable person is the one who makes the decision (approves the control measures), and hence, the right person (appropriate level) must make the decision. Also, be clear on who is responsible at the unit level for implementation of the risk control.

Step 3—Provide Support

To be successful, management must be behind the control measures put in place. Prior to implementing a control measure, get approval at the appropriate level. Then, explore appropriate ways to demonstrate commitment Provide the personnel and resources necessary to implement the control measures. Design in sustainability from the beginning and be sure to deploy the control measure along with a feedback mechanism that will provide information on whether the control measure is achieving the intended purpose.

Common Problems in Implementing Risk Controls

A review of the historical record of risk controls indicates that many never achieve their full potential. The primary reason for shortfalls is failure to effectively involve the personnel who are actually impacted by a risk control. Note that virtually all these factors are driven by the failure to properly involve personnel impacted by risk controls in the development and implementation of the risk controls. Shortfalls include:

- The control is inappropriate for the problem.
- Operators dislike it.
- Managers dislike it.
- It turns out to be too costly (unsustainable).
- It is overmatched by other priorities.
- It is misunderstood.

- Nobody measures progress until it is too late.

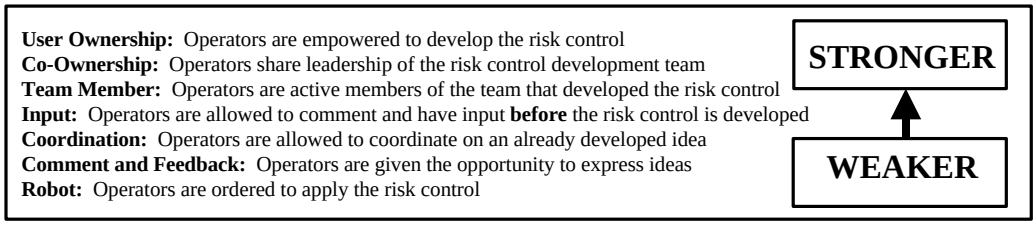
Procedures for Implementing Risk Controls within an Organizational Culture

The following procedures provide useful guidance for shaping a risk control within an organizational culture. Followed carefully they will significantly improve the impact and duration of the effectiveness of risk controls.

Develop the risk control within the organization's culture. Every organization has a style or a culture. While the culture changes over time due to the impact of managers and other modifications, the personnel in the organization know the culture at any given time. It is important to develop risk controls, which are consistent with this culture. For example, a rigid, centrally directed risk control would be incompatible with an organizational culture that emphasizes decentralized flexibility. Conversely, a decentralized risk control may not be effective in an organization accustomed to top down direction and control. If you have any doubts about the compatibility of a risk control within your organization, ask some personnel in the organization what they think. People are the culture and their reactions will tell you what you need to know.

Generate maximum possible involvement of personnel impacted by a risk control in the implementation of the risk control. Figure 15-7 provides a tool to assist in assessing this "involvement factor." The key to making ORM a fully integrated part of the organization culture, is to achieve user ownership in a significant percentage of all risk controls that are developed and implemented by the personnel directly impacted by the risk..

Figure 15-7: Levels of User Involvement in Risk Controls



Develop the best possible supporting tools and guides (infrastructure) to aid operating personnel in implementing the risk control. Examples include standard operating procedures (SOPs), model applications, job aids, checklists, training materials, decision guides, help lines, and similar items. The more support that is provided, the easier the task for the affected personnel. The easier the task, the greater the chances for success.

Develop a time line for implementing the risk control. Identify major milestones, being careful to allow reasonable timeframes and assuring that plans are compatible with the realities of organizational resource constraints.

Procedures for Generating Management Involvement in Implementing Risk Controls

Manager and supervisor's influence behind a risk control can greatly increase its chances of success. It is usually a good idea to signal clearly to an organization that there is interest in a risk control if the manager in fact has some interest. Figure 15-8 illustrates actions in order of priority that can be taken to signal leader support. Most managers are interested in risk control and are willing to do anything reasonable to support the process. Take the time as you develop a risk control to visualize a role for organization leaders.

Figure 15-8. Levels of Command Involvement

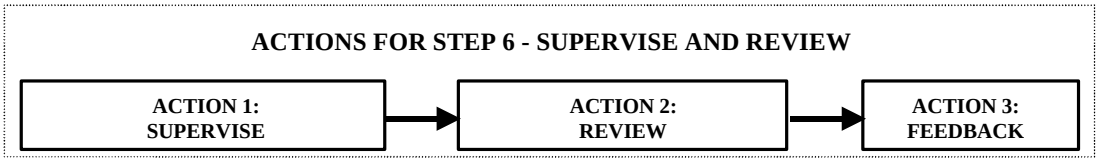
Procedures for Sustaining Risk Control Effectiveness

To be fully effective, risk controls must be sustained. This means maintaining the responsibility and accountability for the long haul. If the risk control has been well designed for compatibility with the organization operation and culture this should not be difficult. Managers must maintain accountability and yet provide a reasonable level of positive reinforcement as appropriate.

Supervise and Review

The sixth step of ORM, Supervise and Review, involves the determination of the effectiveness of risk controls throughout the operation. This step involves three aspects. The first is monitoring the effectiveness of risk controls. The second is determining the need for further assessment of either all or a portion of the operation due to an unanticipated change as an example. The last is the need to capture lessons-learned, both positive and negative, so that they may be a part of future activities of the same or similar type. Figure 15-9 depicts the actions necessary to complete this step.

Figure 15-9: Supervise and Review Actions



Action 1—Supervise

Monitor the operation to ensure:

- The controls are effective and remain in place.
- Changes, which require further risk management, are identified.
- Action is taken when necessary to correct ineffective risk controls and reinitiate the
- Risk management steps in response to new hazards.

Any time the personnel, equipment, or tasking change or new operations are anticipated in an environment not covered in the initial risk management analysis, the risks and control measures should be reevaluated. The best tool for accomplishing this is change analysis.

Successful performance is achieved by shifting the cost versus benefit balance more in favor of benefit through controlling risks. By using ORM whenever anything changes, we consistently control risks, those known before an operation and those that develop during an operation. Being proactive and addressing the risks before they get in the way of operation accomplishment saves resources, enhances operational performance, and prevents the accident chain from ever forming.

Action 2—Review

The process review must be systematic. After assets are expended to control risks, then a cost benefit review must be accomplished to see if risk and cost are in balance. Any changes in the system (the 5-M model, and the flow charts from the earlier steps provide convenient benchmarks to compare the present system to the original) are recognized and appropriate risk management controls are applied.

To accomplish an effective review, supervisors need to identify whether the actual cost is in line with expectations. Also the supervisor will need to see what effect the control measure has had on operational performance. It will be difficult to evaluate the control measure by itself so focus on the aspect of operational performance the control measure was designed to improve.

A review by itself is not enough, a feedback system must be established to ensure that the corrective or preventative action taken was effective and that any newly discovered hazards identified during the operation are analyzed and corrective action taken. When a decision is made to assume risk, the factors (cost versus benefit information) involved in this decision should be recorded. When an accident or negative consequences occur, proper documentation allows for the review of the risk decision process to see where errors might have occurred or if changes in the procedures and tools lead to the consequences. Secondly, it is unlikely that every risk analysis will be perfect the first time. When risk analyses contain errors of omission or commission, it is important that those errors be identified and corrected. Without this feedback loop, we lack the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

Measurements are necessary to ensure accurate evaluations of how effectively controls eliminated hazards or reduced risks. After action reports, surveys, and in progress reviews provide great starting places for measurements. To be meaningful, measurements must quantitatively or qualitatively identify reductions of risk, improvements in operational success, or enhancement of capabilities.

Action 3—Feedback

A review by itself is not enough: a feedback system must be established to ensure that the corrective or preventative action taken was effective and that any newly discovered hazards identified during the operation are analyzed and corrective action taken. Feedback informs all involved as to how the implementation process is working, and whether or not the controls were effective. Whenever a control process is changed without providing the reasons, co-ownership at the lower levels is lost. The overall effectiveness of these implemented controls must also be shared with other organizations that might have similar risks to ensure the greatest possible number of people benefit. Feedback can be in the form of briefings, lessons learned, cross-tell reports, benchmarking, database reports, etc. Without this feedback loop, we lack the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

Monitoring the Effectiveness of Implementation

This aspect of the supervise and review step should be routine. Periodically monitor the progress of implementation against the planned implementation schedule that should have been developed during the third and fifth ORM steps. Take action as necessary to maintain the planned implementation schedule or make adjustments as necessary.

Monitoring the Effectiveness of Risk Controls

If the risk control has been well designed, it will favorably change either physical conditions or personnel behavior during the conduct of an operation. The challenge is to determine the extent to which this change is taking place. If there has been no change or only minor change, the risk control is possibly not worth the resources expended on it. It may be necessary to modify it or even rescind it. At first thought it may seem obvious that we need only determine if the number of accidents or other losses has decreased. This is only practical at higher levels of management. Even at those levels of management where we have sufficient exposure to validly assess actual losses, it may be a year or more before significant changes actually occur. This is too long to wait to assess the effectiveness of risk controls. Too much effort may have been invested before we can determine the impact of our proposals. We need to know how we are doing much sooner. If we can't efficiently measure effectiveness using accident rates, how can we do it? The answer is to directly measure the degree of risk present in the system.

Direct Measures of Behavior. When the target of a risk control is behavior, it is possible to actually sample behavior changes in the target group. Making a number of observations of the use of restraints before initiating the seat belt program and a similar sample after, for example, can assess the results of an effort to get personnel to wear seat belts. The change, if any, is a direct measure of the effectiveness of the risk control. The sample would establish the percent of personnel using belts as a percentage of total observations. Subsequent samples would indicate our success in sustaining the impact of the risk control.

Direct Measures of Conditions. It is possible to assess the changes in physical conditions in the workplace. For example, the amount of foreign objects found on the flight line can be assessed before and after a risk control initiative aimed at reducing foreign object damage.

Measures of Attitudes. Surveys can also assess the attitudes of personnel toward risk-related issues. While constructing survey questions is technical and must be done right, the FAA often conducts surveys and it may be possible to integrate questions in these surveys, taking advantage of the experts who manage these survey processes. Nevertheless, even informal surveys taken verbally in very small organizations will quickly indicate the views of personnel.

Measures of Knowledge. Some risk controls are designed to increase knowledge of some hazard or of hazard control procedures. A short quiz, perhaps administered during a safety meeting before and after a training risk control is initiated.

Safety and Other Loss Control Reviews Procedures. Programmatic and procedural risk control initiatives (such as revisions to standard operating procedures) can be assessed through various kinds of reviews. The typical review involves a standard set of questions or statements reflecting desirable standards of performance against which actual operating situations are compared.

15.12 Conclusion

Operational risk management provides a logical and systematic means of identifying and controlling risk. Operational risk management is not a complex process, but does require individuals to support and implement the basic principles on a continuing basis. Operational risk management offers individuals and organizations a powerful tool for increasing effectiveness and reducing accidents. The ORM process is accessible to and usable by everyone in every conceivable setting or scenario. It ensures that all FAA personnel will have a voice in the critical decisions that determine success or failure in all our operations and activities. Properly implemented, ORM will always enhance performance.