

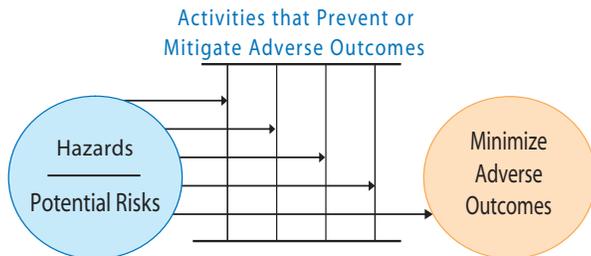
## RISK IS . . .

The potential for adverse outcomes that can happen when hazards go unchecked.

- Hazards and adverse outcomes are all around in every organization
- Without constant vigilance, hazards will hinder mission accomplishment by adversely affecting critical operational aspects, such as agency reputation, employee welfare, program performance, financial integrity, legal liability, and management performance
- Risks exist in all areas at NIH, including both extramural and intramural research, research information, IT, finance and administration
- Risks can cause small problems that become large if not managed, or risks can cause unexpected, large disruptions
- The importance of any given risk is a combination of the likelihood that it will cause an adverse outcome and the probable severity of related losses

## RISK MANAGEMENT IS . . .

Identifying and controlling hazards to **prevent** adverse outcomes or to mitigate those that, inevitably, do occur.



Risk management addresses three important questions:

- Have I identified the main hazards and risks in my environment?
- Do my prevention and mitigation activities address my risks?
- Are my prevention and mitigation activities working effectively to eliminate or minimize risks?

The extent (and cost) of prevention and mitigation activities should be proportional to the severity of the risk. The goal is to reduce risk in a cost effective manner, without compromising quality or doing harm to the mission.

## RISK MANAGEMENT OPERATES . . .

At the **agency level** and cascades down throughout NIH, addressing all major risk areas, such as:

- Extramural and/or Intramural—Grants management, scientific review and reporting, possible scientific misconduct, protection of human subjects in clinical trials, and observance of research protocols
- Research information—Privacy of research participants and records management
- Other—Accurate reporting of financial and performance information, information security, procurement, and property

## RISK MANAGEMENT ALSO OPERATES . . .

At the **project level**. Project risk is the probability that something may go wrong or at least not happen as planned. Risks are different for each project and change as the project progresses. Examples of project risks include lack of staff buy-in, loss of key employees, questionable vendor availability and skills, insufficient time, inadequate project budgets, funding cuts, and cost overruns.

## PROJECT RISK MANAGEMENT IS . . .

The systematic process of applying risk management principles and processes to identify, analyze, and respond to risk at the project level. It addresses the following kinds of questions:

- Are we losing sight of objectives as the project goes on?
- Are we ensuring that the results will improve NIH's ability to complete its mission?
- Are we ensuring sufficient funds are available, including funds to address risks?
- Are we tracking progress to ensure "quicker/better/cheaper" objectives are being met?
- Are we recognizing new risks along the way, such as new IT systems or staff changes?
- Are we taking corrective action to prevent or fix problems rather than simply allocating more money and time to them?



## RISK MANAGEMENT IS IMPORTANT

- Government-wide attention to managing risks of all kinds, not just financial or administrative, is increasing
- This increased attention is happening in the private sector also—it holds managers accountable for their decisions
- Sound and ethical program management is the foundation of success in accomplishing NIH's mission
- When properly implemented, risk management provides a sound defense against problems that detract from the agency's ability to carry out its mission

### Official Guidance

The Office of Management and Budget has set forth some specific new requirements for agencies to strengthen their risk management programs, beginning in FY 2006. The new guidance is set forth in OMB Circular A-123: *Management's Responsibility for Internal Control*. (The terms "internal control," "management control," and "risk management" sometimes are used interchangeably.)

OMB guidance emphasizes MANAGEMENT'S responsibility for taking adequate steps to reduce RISKS in programs. OMB specifies three risk management objectives:

- Efficiency and effectiveness of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

OMB also requires that management self-report annually that "controls" are in place and working. Any serious deficiencies in such controls must be reported as "material weaknesses" and must be corrected. The Circular is supported by GAO standards, and supplemented by guidelines from HHS. Details from all these sources are codified in NIH Policy Manual Chapter 1750.

## BENEFITS OF RISK MANAGEMENT

### NIH-wide

- Accomplish mission better (ensure economy, efficiency and compliance; avoid waste and mismanagement; avoid resource drain of responding to allegations of mismanagement, and of doing work over)
- Early warning of problems; fewer "gotchas" from outside
- Credibility with all stakeholders, including Congress, HHS, OMB, GAO

### Managers at various levels

- Confidence that functions under their responsibility are being properly managed; effective; and free from ethical lapses, waste, fraud, abuse, and threats to health and safety
- Confidence that they will be the first to know if things start going off track and will have time to fix them
- Credibility with supervisors; data and information to make a case for improvements and supporting resources

# KEY COMPONENTS OF EFFECTIVE RISK MANAGEMENT

## Five Standards

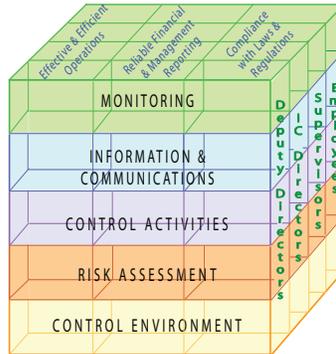
To meet the objectives of effectiveness and efficiency, reliable financial and management reporting, and compliance with laws and regulations, risk management must meet five important standards:

- 1. Control environment**—Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward managing well and reducing risks
- 2. Risk assessment**—The risks that the agency faces from both external and internal sources must be analyzed and evaluated
- 3. Control activities**—Management must take specific actions to effectively and efficiently prevent, reduce, and manage risks
- 4. Information and communication**—Specific and timely information should be recorded and communicated to help management and employees, up, down, and across the organization prevent, reduce, and manage risks
- 5. Monitoring**—Measuring and tracking of risk management activities over time helps to assess the quality of performance and ensure that the findings of audits and other reviews of risks and controls are promptly resolved

## Fundamental Concepts

Effective risk management executes and documents our accountability by:

- Preventing and reducing risks that could dampen mission-critical program objectives
- Providing reasonable assurance that risks are being well managed, not absolute assurance
- Building into operations, to the extent possible, quantitative data and other systematic information to monitor and correct problems



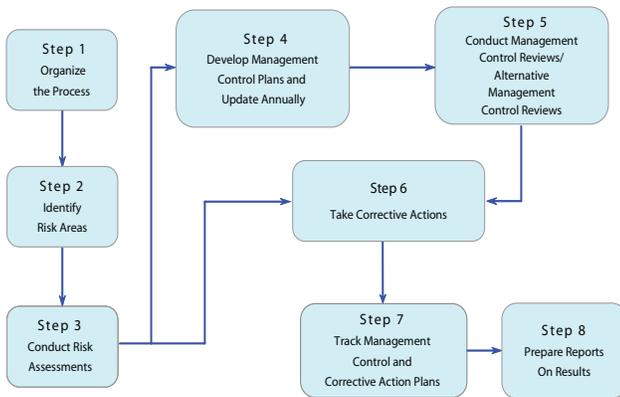
Risk management is most effective when:

- Actively supported by the agency's leadership
- Kept up-to-date and integrated into daily operations
- Designed and executed with common sense and good judgment

Risks are avoided most effectively in organizations that are constantly alert to them and prepared to quickly limit their consequences.

## Basic Process

Risk management programs generally include these 8 basic steps.



## RISK MANAGEMENT RESPONSIBILITIES

**Organizationally**, risk management is a shared responsibility of the central offices and the ICs

OMA supports program operation at all levels

**Employees at all levels** are responsible for complying with rules, regulations, and policies, and for avoiding/mitigating risk both in daily activities and in making program and management decisions

Dir. IC 1	Dir. IC 2	Dir. IC ...27	OD CS
			DDIR
			DDER
			DDM
			CIO

Deputy Directors and IC Directors sign assurances and ensure effective risk management, including a supportive environment, sufficient resources, and on-going monitoring

Supervisors ensure a supportive risk management environment; provide employees with necessary skills and knowledge to identify and mitigate risks and hold them accountable for doing so; monitor risk indicators and ensure necessary corrective actions are taken

Staff members work toward zero defects in daily activities, alert supervisors to possible problems, and help take corrective actions

## THE NIH PROGRAM WORKS LIKE THIS

All members of the NIH community are expected to work to avoid risk and mitigate possible adverse outcomes whenever they make management and program decisions.

The NIH supports you with a formal risk management program. Core principles guiding this program are:

- The program reinforces NIH's culture of outstanding management
- The Steering Committee provides leadership and oversight
- All managers have responsibility to develop and maintain risk management processes for the programs under them
- Risk management applies to intramural, extramural, and IT activities as well as to financial and administrative activities
- A successful program requires proactive management to prevent and mitigate adverse outcomes, not just to audit results afterward
- The program will be given sufficient resources to ensure its success
- It is essential to develop information and reporting systems that enable managers to systematically monitor programs, identify problems early, and take corrective actions in a timely fashion

Key aspects of the program in both NIH-wide offices and individual ICs include:

- **Governance:** The Risk Management Plan is overseen by the NIH Steering Committee
- **Risk assessment:** Risk areas are identified (defined) and ranked in priority order according to the probability and severity of potential adverse outcomes
- **Risk management plans:** Management sets forth key policies and procedures to prevent and mitigate important risks; to the maximum extent possible, these prevention-mitigation activities include systematic and quantifiable data that allow potential problems to be identified and addressed before they negatively impact mission in significant ways
- **Detailed reviews:** Areas of highest risk are reviewed in detail to determine if adequate prevention and mitigation steps are in place and effective
- **Corrective action plans:** These plans are developed on the basis of risk assessments or detailed reviews
- **Follow-up:** Corrective action plans are followed up to ensure that effective actions are taken

## ARE YOU READY TO MANAGE YOUR RISK?

For further information on how you can strengthen or establish a risk management program:

- Check out the website at: <http://oma.od.nih.gov>
- Contact OMA/DQM at 301-496-2461
- Contact the risk management officer in your Institute, Center, or Office (identified on website)