



Enterprise Risk Management at NSF



Mike Wetklow
Rafael Cotto
Charisse Carney-Nunes
Office of Budget, Finance, and Award Management
June 14, 2018

Introduction

Purpose:

- To summarize Enterprise Risk Management (ERM) efforts to date and elicit Business Operations Advisory Committee (BOAC) perspectives on maturing ERM at NSF

Outcome:

- Guidance on strategies and best practices that will assist NSF to continue developing ERM



Background

- On July 15, 2017, Office of Management and Budget released an update to Circular A-123, [Management's Responsibility for Enterprise Risk Management and Internal Control](#)
- NSF implemented ERM to:
 - Determine what risk areas could negatively affect the ability of NSF to carry out its mission
 - Identify resources, processes, policies, and procedures for proactively managing risk
 - Create greater risk management awareness at all levels of the organization
 - Provide a coordinated and common framework for capturing and reporting risk information and getting the right people around the table to discuss risk and incorporate into decision making
- NSF is in its second year of implementing ERM



Top Accomplishments

- Leadership: Director, Chief Operating Officer (COO), and Assistant Directors support ERM
- Director's Watch List and National Science Board (NSB) risk discussions
- Maturity based ERM strategy and process
- OMB concurred with NSF's plan; met first major milestone by developing an initial risk profile in June 2017
- Office of Inspector General (OIG): discussed road rules on collaboration
- NSF's Strategic Plan: Incorporated ERM into Strategic Plan
- NSF's Internal Controls Program: Integrated ERM with internal controls program



Features [View All Features »](#)

A woman, Dr. France Cordova, is speaking at a podium during a staff briefing. The text "DR. FRANCE CORDOVA NSF Director" is overlaid on the image.	The Director is presenting the FY18 budget request to a group of people seated at a table.	A group of NSF staff members are standing together, participating in a public service recognition event.
Staff Briefing on NSF's 10 Big Ideas	Director Presents the FY18 Budget Request	NSF Staff Contribute to Grateful Tree for PSRW
A collage of images related to proposal and award processes, including a globe and documents.	The text "ERM" is prominently displayed over a green, abstract background.	A blue and white graphic with the NSF logo and the text "Information Technology".
Revised Proposal & Award Policies & Procedures	COO Message on Enterprise Risk	Renewing NSF - Information Technology



NSF ERM Maturity Level



Level 1 Nascent

- Lacks formal ERM process; no basic communication or monitoring; risks addressed as they arise; fails to anticipate potential risks

Level 2 Emerging

- ERM roles and responsibilities defined; governance established; risks are identified and assessed; rarely well prepared for unanticipated events

Level 3 Integrated

- ERM program is endorsed by leadership; policies and processes are in place for some activities; risks are shared across silos; occasionally well prepared for unanticipated events

Level 4 Predictive

- ERM program is recognized by whole organization; policies and processes are in place for all activities; risks are identified and qualitatively assessed; periodically well prepared for unanticipated events

Level 5 Advanced

- Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. An early warning system is in place to notify management of risks above established thresholds; regularly well prepared for unanticipated events and have learned from past events to improve processes

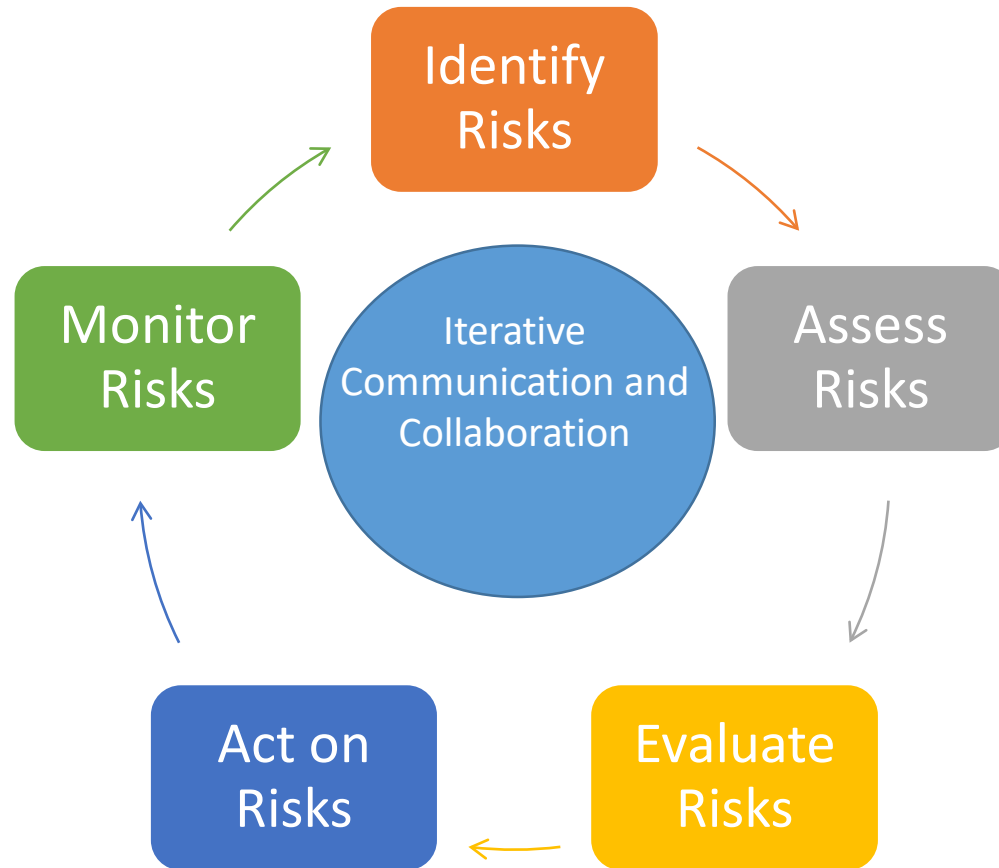


Top Lessons Learned

- Exploring dedicated ERM Accountable Official and/or formal Risk Management Council
- Improving governance and clarifying NSF wide roles and responsibilities for ERM to guard against “compliance exercise” risks and maximize “value” to NSF
- Moving NSF risk management from good to great
- Moving from annual reporting to regular ongoing discussions about risks
- Developing clearer linkages with strategic opportunity initiatives
- Considering governmentwide trends and lessons learned, “where do we go from here?”



NSF's ERM Framework*



Appreciating different meanings of risk, illustrative examples:**

- external
- strategy
- preventable

* Consistent with authoritative guidance from Committee on Sponsoring Organizations of the Treadway Commission (COSO) and Chief Financial Officer (CFO) and Performance Improvement Officer (PIO) Council Playbook

** Based on a Harvard Business Review Article, [Managing Risks: A New Framework](https://hbr.org/2012/06/managing-risks-a-new-framework) (available at <https://hbr.org/2012/06/managing-risks-a-new-framework>)





Harvard Business Review Framework


- External Risks: Risks that arise from outside and are beyond an organization's influence and control
- Strategy Risks: Risks that an organization voluntarily accepts to generate superior returns from its strategy
- Preventable Risks: Internal risks, arising from within the organization, that are controllable and ought to be eliminated or avoided



**Harvard
Business
Review**



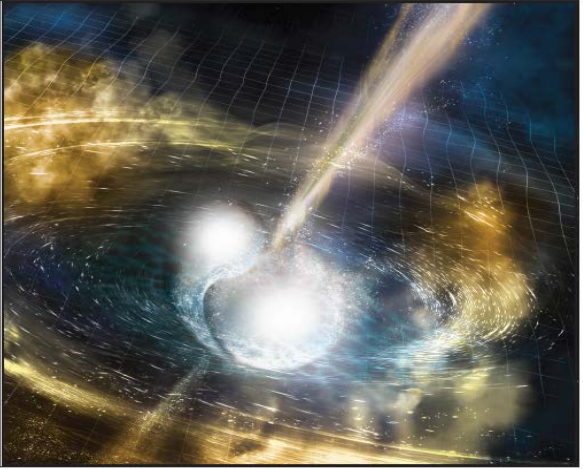
2018 Risk Reporting





National Science Foundation

BUILDING THE FUTURE INVESTING IN DISCOVERY AND INNOVATION

NSF Strategic Plan for Fiscal Years (FY) 2018-2022



	External Risk Risks that arise from outside and are beyond the organization's influence and control	Strategy Risk Risks that an organization voluntarily accepts to generate superior returns from its strategy	Preventable Risk Internal risks, arising from within the organization, that are controllable and ought to be eliminated or avoided
NSF Strategic Goal			

Expand knowledge in science, engineering, and learning	STRATEGIC OBJECTIVE – Improve Program Outcomes								
	Risk	Inherent Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response Category
Advance the capability of the Nation to meet current and future challenges	Agency X may fail to achieve program targets due to lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program	High	Medium	Agency X will monitor capacity of program partners	Primary – Program	Primary – Strategic
	Enhance NSF's performance of its mission								
Contract and Grant fraud.	OPERATIONS OBJECTIVE								
	Encouraging the Ethical Conduct of Research (Low Risk Appetite)								
	Impact	5 Very High		Severe Impact/Very Rarely Happens	Severe Impact/Unlikely to Happen	Severe Impact/Will Possibly Happen	Severe Impact/Highly Likely to Happen	Severe Impact/Almost Certain to Happen	
	4 High	Significant Impact/Very Rarely Happens		Significant Impact/Unlikely to Happen	Significant Impact/Will Possibly Happen	Significant Impact/Highly Likely to Happen	Significant Impact/Almost Certain to Happen		
	3 Moderate	Material Impact/Very Rarely Happens		Material Impact/Unlikely to Happen	Material Impact/Will Possibly Happen	Material Impact/Highly Likely to Happen	Material Impact/Almost Certain to Happen		
	2 Low	Noticable Impact/Very Rarely Happens		Noticable Impact/Unlikely to Happen	Noticable Impact/Will Possibly Happen	Noticable Impact/Highly Likely to Happen	Noticable Impact/Almost Certain to Happen		
	1 Very Low	Negligible Impact/Very Rarely Happens		Negligible Impact/Unlikely to Happen	Negligible Impact/Will Possibly Happen	Negligible Impact/Highly Likely to Happen	Negligible Impact/Almost Certain to Happen		
Likelihood	1 Very Low	2 Low	3 Medium	4 High	5 Very High				
 Risk 1: Awards made to scientific projects based on proposals that are, in part, products of research misconduct.									
 Risk 2: Awards result in purported results, findings, or publications that are, in part, based on research misconduct									



ERM and Management Challenges

NSF is using ERM to assist Agency leadership in responding to strategic challenges by:

- Identifying Opportunities
- Making decisions about risks
- Building consensus with stakeholders



BOAC Discussion Questions

- What are the strategies and best practices that can help us mature ERM and move it from an Office of the Chief Financial Officer mindset to an NSF mindset?
- What actions can we take to continue to develop NSF's ERM governance structure?
- How have you changed your organizational culture to create an ERM community of practice?

**THANK
YOU!**



Attachments

- Guiding Principles for Implementing ERM at NSF
- National Science Board Philosophy and Principles
- NSF Governance Structure



National Science Board (NSB)

Philosophy

- Integral to NSB's role
- Recognizes that effective risk management must be an enterprise-wide activity
- Efforts are undertaken in conjunction with NSF's ERM

Principles

- Risk management is fundamental to effective oversight
- Board must be attuned to its own risk profile
- Strategic and holistic approach to the larger enterprise
- Applying the Harvard Business Review Risk Framework

NSB-2018-16

National Science Board Risk Philosophy

Risk management, mitigation, and (when warranted) informed acceptance of risk are integral to the National Science Board's (Board, NSB) role to further the National Science Foundation's (NSF, Foundation) mission and fulfill NSB's dual roles to set policy for NSF and serve as an advisor to Congress and the White House on science and engineering policy and education.

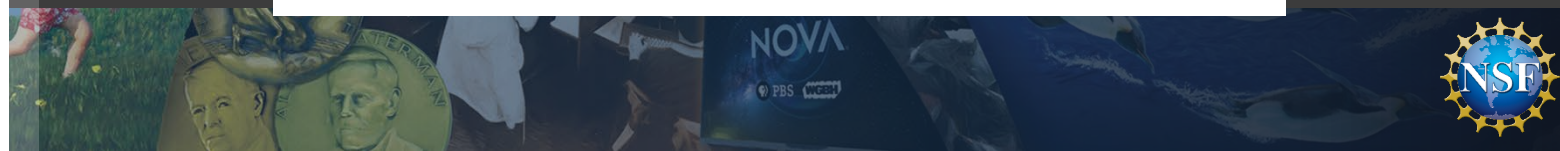
The Board recognizes that effective risk management must be an enterprise-wide activity. NSB's efforts are undertaken in conjunction with the NSF's enterprise risk management activities as well as directorate and facilities-specific risk monitoring, and are designed to complement those efforts. Through sustained risk-informed dialogue and consistent evaluation of risk factors, the Board, the NSF Director, and NSF Senior Management can arrive at a mutual understanding of the agency's risk appetite relative to the mission of promoting the progress of science, pursue opportunities, navigate challenges, and position NSF for maximal success. Internally, NSB also recognizes its responsibility to mitigate risks associated with its own work and processes.

As the governing body for the Foundation, the Board's primary interest is not to micro-manage NSF, but rather to have sufficient and timely insight and information on matters over which the Board has a decisional role, oversight responsibility, or about which the Board may be asked to respond by a wide range of stakeholders. The Board also recognizes that risk analyses are integral to its ability to engage strategically and generatively with NSF to meet future challenges, seize future opportunities, and fulfill the public trust.

National Science Board Risk Principles

- Risk management is fundamental to effective oversight; evaluation of risk will be incorporated into all Board activities
- The Board must be attuned to its own risk profile to avoid unintended consequences of its decisions or involvement in Foundation decisions
- The Board must be clear in its information needs to ensure it has sufficient information to understand the potential risks associated with matters presented to the Board for consideration.
- With a focus on the Foundation, writ large, the Board must include in its risk analysis of a particular action, a strategic and holistic approach to the larger enterprise.
- In applying the Harvard Business Review Risk Framework¹, the Board will be sensitive to the Foundation's equities in the various preventable, external, and strategy risks in any given matter before the Board.

¹ Robert Kaplan and Anette Mikes. *Managing Risks: A New Framework*, Harvard Business Review, June 2012, accessed online at: <https://hbr.org/2012/06/managing-risks-a-new-framework>



NSF Governance Structure

- Ultimate accountability and responsibility for ERM rests with NSF's COO
- Senior Management Round Table (SMaRT) supports the COO to ensure ERM is integrated into the NSF culture and that responsibilities have been appropriately delegated throughout agency
- SMaRT provides value by having different points of view all together in the same room (e.g., All Programs with Office of General Counsel, Office of Legislative & Public Affairs, Office of Diversity and Inclusion, etc.)
- SMaRT can provide governance and guidance on which risks to filter or share
- NSF will leverage its CXO Council for integrating ERM with mission support functions
- NSF's Deputy Chief Financial Officer provides senior staffing support to the Director, COO, and SMaRT

