Enterprise Risk Management (ERM) and Cybersecurity

National Science Foundation
March 14, 2018

Agenda

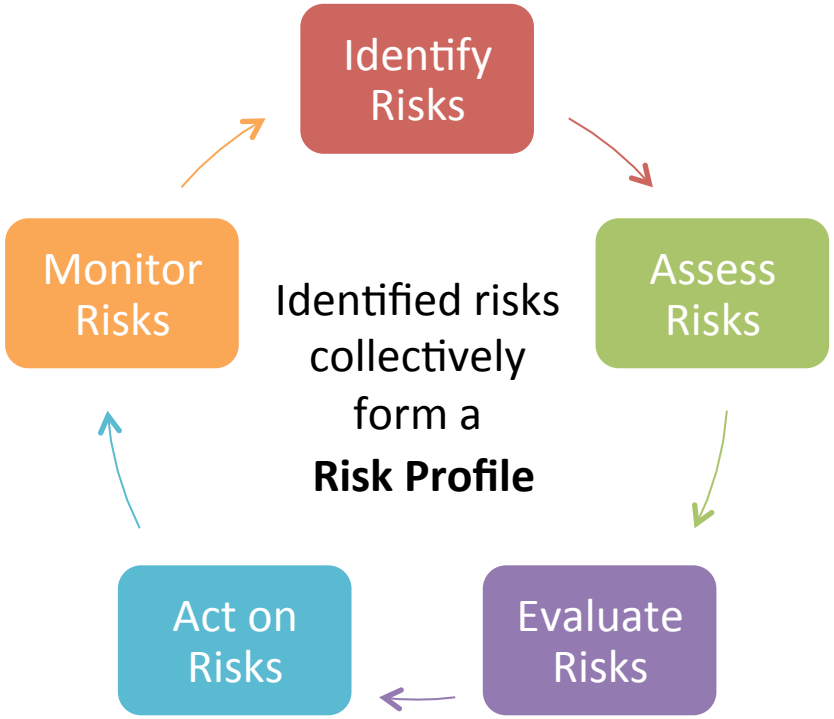
- Guiding Principles for Implementing ERM at NSF (Based on COSO)
- NSF's ERM Framework
- ERM Cybersecurity Risk Profile
- Cybersecurity Risk Management Philosophy
- Governance, Risk Management and Communication
- Risk Tolerance
- NIST Risk Frameworks
- IT Risk Management Documents

Guiding Principles for Implementing ERM at NSF (Based on COSO)

1. Support from the Top is a Necessity
2. Build ERM using Incremental Steps
3. Focus initially on a Small Number of Top Risks
4. Leverage Existing Resources
5. Build on Existing Risk Management Activities
6. Embed ERM into the Decision Making Practices of the Organization
7. Provide Ongoing ERM Updates and Continuing Education for Leadership and Senior Management

NSF's ERM Framework

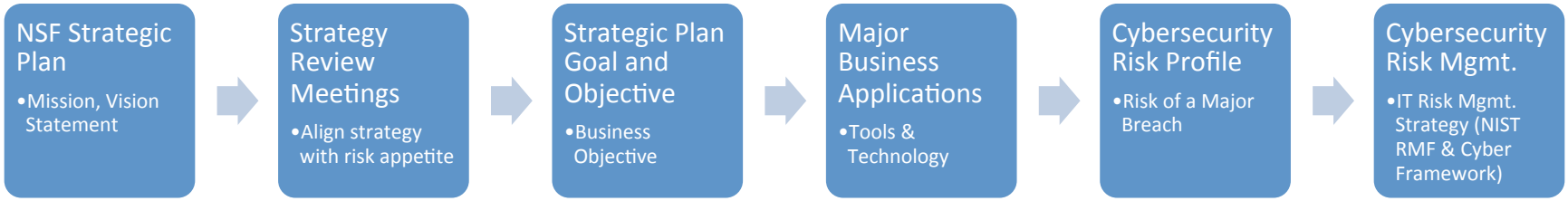
- **NSF's Strategic Plan** embraces enterprise risk management
  - Encourages use of methodical risk analysis for resilience
  - Maintain a risk profile of significant risks and opportunities
- NSF established an **Enterprise Risk Management** approach
  - Developed a "maturity based" ERM strategy and process
  - Developed an **"initial" risk profile**
  - Cybersecurity is a profile
  - About 12 agency level risks identified



ERM Cybersecurity Risk Profile

- **Risk appetite** is the type and amount of risk an organization is prepared to accept (on a broad level); statement reflects the culture
  - Qualitative statement – low, high appetite, e.g. low appetite for major cybersecurity breaches
  - Quantitative – measures, e.g. 10% of the budget is allocated to innovation
- **Risk tolerance -** Once the risk appetite has been defined, risk tolerance defines boundaries of acceptable variation
- **Risk profile** allows management to determine resource allocation

NSF aligned cybersecurity with the NSF Strategic Plan, goal and objective



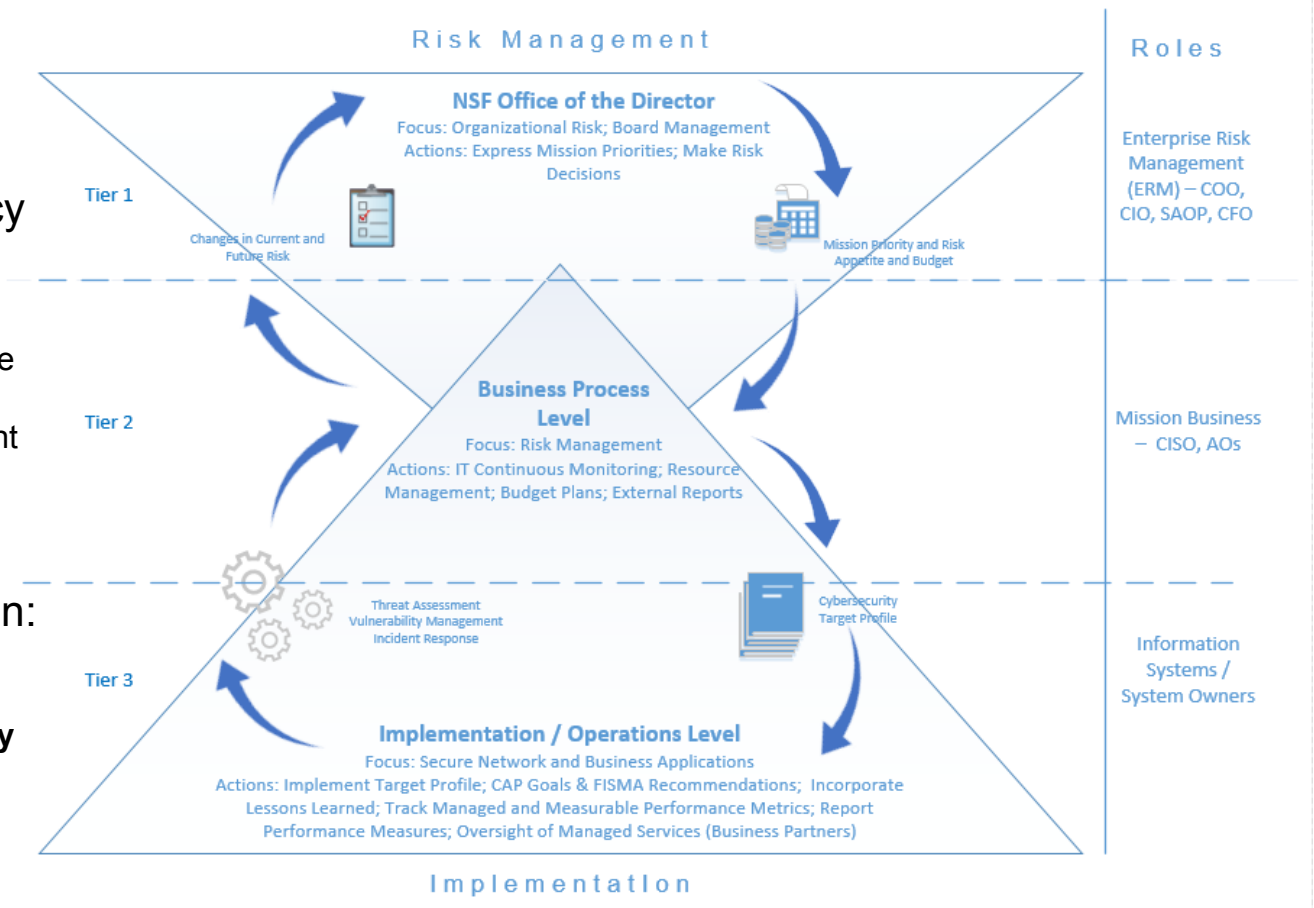
NSF Strategic Plan sets forth long term goals and objective per the Government Performance and Results Act (GPRA).

Cybersecurity Risk Management Philosophy

- **Risk-Based** - Risks are assessed, analyzed, understood and appropriately mitigated
  - Balance of operational and economic costs of protective measures with the gains in mission capability
  - Considers cost/benefit, risk analysis, assessment, oversight
- **Defense in Depth** - Layered approach to cybersecurity
  - Layers of security controls assure major systems and assets are protected with the most extensive controls
  - Implement management, operational, technical controls
- Risk management philosophy documented in the **NSF Information Security (InfoSec) Handbook**

Governance, Risk Management and Communication

- Risk management is a **coordinated activity** to communicate, direct and control challenges to agency goals and objectives
- ERM risk profiles capture
  - A-123 risk and control objective assessments
  - FISMA and Financial Statement audit evaluations
  - IG management challenges
- Cybersecurity risk management documented in:
  - **Framework Implementation Summary**
  - **IT Risk Management Strategy**
  - **InfoSec Handbook**



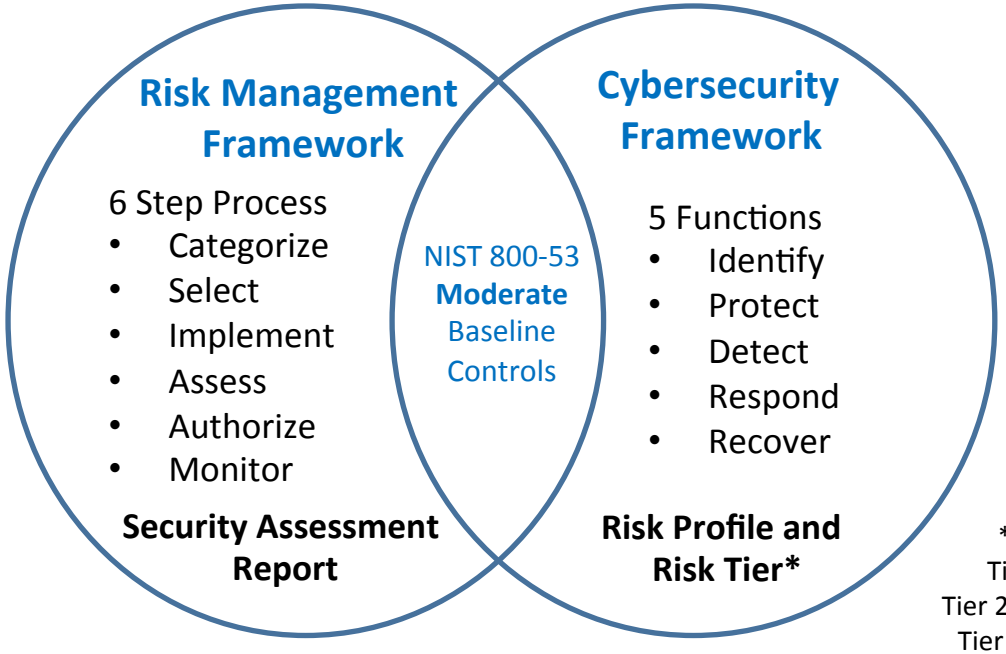
Risk Tolerance

- NSF's risk tolerance, e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable *depend on the type of event* and its *impact on the organization*
- *Priorities and trade-offs*, e.g., the relative importance of missions/business functions, trade-offs among different types of risk, time frames to address risk, and any factors of uncertainty to consider in risk responses *form NSF's tolerance for risk*
- NSF considers *reputational risk, business disruption, financial loss, and loss of privacy* as a few of the factors that affect risk tolerance
- Risk tolerance is articulated in NSF policies, procedures and **InfoSec Handbook** and **IT Security Risk Management Strategy**

NIST Risk Frameworks

NIST Frameworks are linked through the NIST controls

Risk Mgmt. Framework
Supports an informed risk-based decision to authorize a system to operate



Cybersecurity Framework
Risk tiers provide context on an organization's view of cybersecurity risk and the processes to manage risk

*Risk Tiers
Tier 1 Partial
Tier 2 Risk Informed
Tier 3 Repeatable
Tier 4 Adaptive

NIST 800-137 Guide for Applying the Risk Management Framework to Federal Information Systems

E.O. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017

IT Risk Management Documents

- **NSF Strategic Plan**
  - Describes NSF's long-term goals and objectives and performance goals
- **Cybersecurity Profile for Enterprise Risk Management**
  - Compliance objective for cybersecurity
- **NSF Information Security Handbook**
  - Supports moderate baseline NIST controls
- **IT Security Risk Management Strategy**
  - Addresses NIST Risk Management Framework and Cybersecurity Framework
- **NSF Cybersecurity Framework Implementation Summary**
  - Describes how NSF's IT security program aligns with the Cybersecurity Framework
- **Information Security Continuous Monitoring**
  - Describes the program and operational monitoring activities
- **Ongoing Authorization Plan**
  - Describes NSF's ongoing authorization approach