AGENDA

- What is Risk
- Why Manage Risk
- Traditional Risk Model
- Evolution of the Risk Model
- Strategic Risk Stewardship
- Implementation
- Benefits
- HHS – Program Support Center
- NASA
- DHS
WHAT IS RISK?

• Probability of an outcome other than what is expected
  o Generally recognized as an adverse outcome
  o Positive deviations from the outcome are considered risk too

• Types of Risk
  o Pure Risk – Only the chance of loss or no loss
  o Speculative Risk – Possibility of loss or gain

• Classifications of Risk
  o Quantitative Risk (tangible)
    • Loss
    • Gain
  o Qualitative Risk (intangible)
    • Reputational
WHY MANAGE RISK?

- Organizations and individuals are held to very high standards of care
- Organizations are being held liable for the actions of their employees
- Organizations are perceived as having a lot of assets (deep pockets)
- We live in a litigious society
- Taking the steps to prevent injury could help to defend in a legal action
- Courts are often sympathetic to injured claimants and give them benefit of the doubt
TRADITIONAL RISK MANAGEMENT 1.0

• Defensive measure to react to operational failures
• Historically is relegated to accounting and audit staff, related to financial reporting
• Has been legislated by Congress and regulated by OMB
• Back office function
• Not widely recognized at the strategic or program levels
• Perceived as an administrative burden rather than as a means of ensuring the objectives of the mission
Evolution of the Risk Model

Traditional Risk Management

Financial Reporting

Individual Program

Institutional Reputation

Evolution of the Risk Model

Transformation Beyond Financial Reporting Risk

- Culture Shift
- Retrain Employees
- Qualitative

- Adjust Metrics
- Target Resources to Risk
- Quantitative
**Risk Stewardship**

- Ensures that an organization identifies, understands, and measures the unanticipated or unexpected outcomes to which it is exposed.
- Requires that the organization creates and implements an effective strategic risk plan to address the impacts of unexpected outcomes.
- Includes:
  - Risk measurement
  - Risk management
  - Risk Exploitation
STRATEGIC RISK STEWARDSHIP

- Identify
- Measure Exposure
- Formulate Strategy
- Avoid Transfer Share Mitigate Accept
- Assess Impact of Exposure
- Evaluate Performance
- Transfer or Exploit
- Cost / Benefit

Risk Measurement

Risk Management
RISK MANAGEMENT v RISK MEASUREMENT

- The title risk management has frequently been appropriated to describe what **should be** called risk measurement.

- **Risk Measurement**
  - measuring and quantifying of risk and its associated costs
  - necessary to support the management of risk
  - requires specialized expertise and tools, and
  - should be organized as a standalone department separate from the operating departments.

- **Risk Management**
  - core competency of the organization
  - includes identifying, defining, and reporting out potential deviation from expectations
  - involves mitigating the downside risk and exploiting the upside risk
  - is everyone’s responsibility.
RISK EXPLOITATION

A GENERALLY NEGLECTED FACET OF RISK MANAGEMENT

• Establish the Risk Tolerance Zone
• Identify Opportunities Gained by Varying Degrees of Tolerance
• Compare the Tolerance to Potential Mission Gain
• Determine Alternatives for Adjusting
  o Tolerance Levels
  o Mission Outcomes
• Execute the Exploitation Strategy
• Continuously Monitor Tolerance Against Mission Outcomes via Reporting
Why Transform the Risk Model?

• An effective and operational risk stewardship practice demonstrates commitment to resource optimization and mission objectives
• Migrate to a proactive model that supports the creation of cost and operational efficiencies
• Reduces the likelihood of project failure: financial-, project-, or schedule-based
• Projects or programs with a sound risk strategy can expect a 15% higher success rate
• An effective strategic model should recover its cost
IMPLEMENTATION OF A RISK STEWARDSHIP STRUCTURE

• Determine risk appetite or tolerance
  o Understand the acceptable level of risk
  o The cost of avoiding risk beyond this level – tolerance

• Develop a risk language
  o All parties must understand the terminology

• Identify Risks and Mission Outcomes
  o Understand and validate the objectives of the organization

• Prioritize and Formulate Strategy
  o Develop an overall risk reduction strategy and approach
  o For each risk, determine whether to monitor, mitigate, accept or ignore

• Mitigate, Accept, or Exploit

• Report and Review
Where in the Organization?

- Risk is pervasive at every level
- Impacts all normal business activities
- Should be managed at all levels
  - Corporate or Strategic
  - Project or Portfolio
  - Program
  - Department or Division
  - Operations
STRATEGIC FORMULATION

STRATEGY
- Which risks affect your enterprise
- How will you prioritize
- How will you address
- How will you monitor

TYPES OF RISK
- Strategic
- Regulatory
- Project or Program
- Reputational
- Operational
- Legal
- Credit
Benefits of Risk Stewardship

- Optimizing Resources: time, assets, income, property and people
- Protecting the reputation and image of the organization
- Increasing the stability of operations
- Protecting people from harm
- Protecting the environment
- Sustainable and repeatable processes
- Ensuring the mission and its objectives
- Preventing or reducing legal liability
- Improves business and strategic planning
- Increased ability to deliver on time – Scheduling Efficiency
- Ability to grasp new opportunities (exploiting risk)
- Ability for continuous improvement
PROPER RISK STEWARDSHIP

Does not have to be expensive or time consuming: It may be as uncomplicated as answering these questions:

1. What can go wrong? (WHAT)
2. What is the likelihood it will occur? (PROBABILITY)
3. What is the impact of the occurrence? (MAGNITUDE)
4. What will we do? (RESPONSE, MITIGATION OR ACCEPTANCE)

A PREMIERE RISK STEWARDSHIP PLAN INCLUDES STRATEGIES AND TECHNIQUES FOR RECOGNIZING AND CONFRONTING UNEXPECTED EVENTS
HHS
PROGRAM SUPPORT CENTER

• Established a Cross-Functional Committee – The Risk Management and Financial Oversight Board (RMFOB)
  o Increased Management Support – Reflects the Tone from the Top
  o Provides “C-Level” involvement in the mitigation of risk

• Secretary’s Program Integrity Initiative
  o Programmatic Risk Assessment
  o Develop Risk Response
  o Mitigation

FINANCIAL REPORTING  INDIVIDUAL PROGRAM  INSTITUTIONAL REPUTATION
HHS
Program Support Center

- Capabilities based on
  - Organizational Structure & Staffing
  - Communications
  - Systems Security
  - Contract Analysis & Negotiations
  - Disaster Plans
  - Financial & Managerial Accounting and Reporting

- Evolved Risk Management from Defensive Posture to Anticipatory
  - Identified and Developed Critical Management Skills
    - All managers must possess an intimate knowledge of the business
    - A strategic view of risk and risk management role
HHS Program Support Center

- PSC as Service Provider and Cost Reimbursable Entity Develops and Tracks Costs Related to Risk Management
- Primary Key Performance Indicator is Total Cost of Risk (TCOR)
TYPES OF RISK

Financial Risk
- Forecasting
- Rate Setting
- Cost Control
- Revenue
- Billing & A/R
- Cash Flow

Operational Risk
- Human Capital
- Contract Management
- Resource Management
- System Security
- IT Support

Strategic Risk
- Compliance
- Audit
- Growth
- Intellectual Capital

Hazard Risk
- Employee Satisfaction
- Property Damage
- Natural Disaster
- Employee Injury
- Legal Liabilities
PROGRAM SUPPORT CENTER

SPECIFIC PROGRAM INITIATIVES

• Do Not Pay Initiative
  o Pre-Payment
  o Move to Pre-Award

• Data Mining on Grants

• Business Intelligence Initiative

• Financial Reporting Improvements

• Program Performance Reviews
QUALITY ASSURANCE DIVISION (QAD)

• The NASA Office of the Chief Financial Officer (OCFO) established the Quality Assurance Division (QAD) in FY 2005. QAD is responsible for internal controls and compliance reviews, and performs quality assurance reviews.
  o **Vision** - Empowering NASA to move beyond compliance and toward achieving financial management excellence
  
  o **Mission** - Ensure compliance with financial reporting requirements and applicable laws and regulations, through continuous monitoring, evaluation, assessment; and making recommendations for improvement

FINANCIAL REPORTING  INDIVIDUAL PROGRAM  INSTITUTIONAL REPUTATION
Quality Assurance Division

Structure

Quality Assurance Division Director
Frank E. Petersen, III

Deputy Director
Mustapha Wai

Audit Planning and Coordination
- Coordinate all OCFO audit activities (OIG, GAO, and other external audits)
- Coordinate all entrance & exit conferences and other required meetings
- Ensure all audit requests are fulfilled
- Coordinate site visits

Audit Resolution
- Coordinate with responsible parties to develop corrective action plans to address audit recommendations
- Monitor and report progress made on the execution of corrective actions
- Request closure of audit recommendations

IPIA and Recovery Audits
- Prepare contractor requirements and review contractor proposals
- Prepare necessary guidance
- Conduct risk assessment, testing and reporting for IPIA
- Liaison between contractors, Centers and Comp. Ctr.

Internal Controls and A-123 Compliance
- Establish and maintain internal control framework
- Execute internal control testing
- Coordinate with OICMS to support preparation of the Agency Stmt of Assurance
- Prepare necessary documentation for AFR Reporting

Assessment, Assurance, and Advisory
- Monitor compliance with policies, procedures, regulations, laws, etc.
- Monitor high risk/sensitive areas such as segregation of duties, contract closeout, employee receivables, etc.
- Document and provide recommendations to affected parties

Risk Assessment
INHERENT RISKS

Business Processes

CONTROL OBJECTIVES & ACTIVITIES

Activities

FEDERAL REQUIREMENTS & STANDARDS

Transactions

Accounts

MANAGEMENT DECISIONS

Reports

Risk

Assess

Mitigate

Monitor/Report

RESULTS = Relevant, Reliable, Consistent, and Timely Financial Information for Management Decision Making
FINANCIAL RISK MITIGATION
TOOLS AND TECHNIQUES

- Developed a Comprehensive Compliance Strategy (CCS) that focuses on ensuring compliance with Generally Accepted Accounting Principles (GAAP) and other financial reporting requirements.
- Continuous Monitoring Program detects control risks that may adversely impact financial data used in reporting and management.
- NASA implemented “Approva” in FY 2007 to monitor user roles in the core financial system to ensure that proper segregation of duties mitigates financial control and reporting risk.
- NASA’s performs Improper Payment Information Act IPIA Program risk assessments.
RISK ASSESSMENT AT NASA

• Risk assessment is a key component of NASA’s internal control program.

• OCFO employs a risk-based approach to OMB Circular A-123, Appendix A.
  o Assess key business process qualitative and quantitative risk factors.
  o Informs management decision making on processes assessed

• NASA’s OMB Circular Appendix-C IPIA risk assessment methodology has been considered as a best practice by other Agencies
RISK ASSESSMENT MATRIX

- At the summary level the risk matrix ties out the pre-defined risk conditions with the NASA programs.
- The defined risk conditions are weighted to determine the likelihood and impact if the risk condition was to occur.
- Once the matrix is populated with the risk conditions and weightings it is a matter of plugging in the numbers and the spreadsheet calculates an overall risk score.
- A predetermined threshold is used to identify which programs are low, medium or high risk.
- The tool can be modified for any program or process.
- In FY 2011 NASA plans to use the matrix for the A-123, Appendix A assessment.
# FY 20XX Risk Assessment

## Business Cycle

<table>
<thead>
<tr>
<th>Entity-Level</th>
<th>Weight</th>
<th>4</th>
<th>3</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>3</th>
<th>2</th>
<th>3</th>
<th>3</th>
<th>3</th>
<th>2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Blended Cycle Risk Ratio</td>
<td>2.57</td>
<td>5.0</td>
<td>2.6</td>
<td>1.0</td>
<td>5.0</td>
<td>1.0</td>
<td>3.4</td>
<td>1.0</td>
<td>1.0</td>
<td>3.0</td>
<td>1.0</td>
<td>2.2</td>
<td>1.0</td>
</tr>
<tr>
<td>Financial Statement Materiality</td>
<td>5.0</td>
<td>3.0</td>
<td>3.0</td>
<td>2.0</td>
<td>3.0</td>
<td>2.5</td>
<td>5.0</td>
<td>1.5</td>
<td>3.0</td>
<td>3.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>Compliance</td>
<td>4.8</td>
<td>4.2</td>
<td>2.9</td>
<td>2.7</td>
<td>2.5</td>
<td>3.7</td>
<td>5.0</td>
<td>4.0</td>
<td>4.6</td>
<td>2.4</td>
<td>4.0</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Centralized/Decentralized Processes</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
<td>3.0</td>
<td>4.0</td>
<td>3.0</td>
<td>1.0</td>
<td>5.0</td>
<td>5.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Recent Process Changes</td>
<td>3.7</td>
<td>3.9</td>
<td>2.8</td>
<td>5.0</td>
<td>2.3</td>
<td>3.9</td>
<td>1.0</td>
<td>2.6</td>
<td>4.1</td>
<td>4.6</td>
<td>2.6</td>
<td>2.6</td>
<td>1.3</td>
</tr>
<tr>
<td>Complexity</td>
<td>3.3</td>
<td>3.8</td>
<td>1.8</td>
<td>2.0</td>
<td>1.8</td>
<td>2.2</td>
<td>1.0</td>
<td>1.6</td>
<td>3.0</td>
<td>3.2</td>
<td>3.0</td>
<td>3.0</td>
<td>2.2</td>
</tr>
<tr>
<td>Planned IT Systems Implementation/Upgrade</td>
<td>3.2</td>
<td>3.9</td>
<td>1.8</td>
<td>3.2</td>
<td>1.8</td>
<td>2.8</td>
<td>1.0</td>
<td>2.4</td>
<td>3.0</td>
<td>3.4</td>
<td>2.4</td>
<td>3.0</td>
<td>1.3</td>
</tr>
<tr>
<td>Inherent IT Risk</td>
<td>3.1</td>
<td>3.9</td>
<td>2.4</td>
<td>3.6</td>
<td>2.3</td>
<td>2.6</td>
<td>3.0</td>
<td>1.7</td>
<td>3.2</td>
<td>3.9</td>
<td>2.3</td>
<td>2.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Multiple Systems and/or Interfaces</td>
<td>2.7</td>
<td>3.8</td>
<td>1.8</td>
<td>3.2</td>
<td>1.8</td>
<td>2.8</td>
<td>1.0</td>
<td>2.4</td>
<td>3.0</td>
<td>3.4</td>
<td>2.4</td>
<td>3.0</td>
<td>1.3</td>
</tr>
<tr>
<td>Fraud/Theft</td>
<td>2.6</td>
<td>3.8</td>
<td>1.5</td>
<td>1.9</td>
<td>4.3</td>
<td>1.6</td>
<td>2.8</td>
<td>3.0</td>
<td>2.1</td>
<td>3.9</td>
<td>3.8</td>
<td>2.1</td>
<td>2.1</td>
</tr>
<tr>
<td>Known Deficiencies</td>
<td>2.9</td>
<td>3.8</td>
<td>1.8</td>
<td>3.2</td>
<td>1.8</td>
<td>2.8</td>
<td>1.0</td>
<td>2.4</td>
<td>3.0</td>
<td>3.4</td>
<td>2.4</td>
<td>3.0</td>
<td>1.3</td>
</tr>
<tr>
<td>Continuous Monitoring Program (CMP)</td>
<td>2.6</td>
<td>3.8</td>
<td>1.8</td>
<td>3.2</td>
<td>1.8</td>
<td>2.8</td>
<td>1.0</td>
<td>2.4</td>
<td>3.0</td>
<td>3.4</td>
<td>2.4</td>
<td>3.0</td>
<td>1.3</td>
</tr>
</tbody>
</table>

## Risks

1 - Very Low, 2 - Low, 3 - Medium, 4 - High, 5 - Very High

- **Entity-Level**: 2.57
- **Fund Balance with Treasury**: 2.90
- **Financial Reporting**: 3.77
- **Budget Management**: 3.97
- **Property Management**: 3.32
- **Grants Management**: 2.97
- **Procurement and Payment Management**: 3.14
- **Revenue and Receivables Management**: 2.77
- **HR and Payroll Management**: 2.69
- **Investment Management**: 1.45
- **Information Technology**: 4.17
- **Cost Management**: 2.71

### Notes
- The table above represents the FY 20XX Risk Assessment for NASA. It includes various categories such as Business Cycle, Weight, Blended Cycle Risk Ratio, and risks rated from 1 to 5 (Very Low to Very High).
- The table provides a structured view of how different business cycles are rated based on various factors.
- This analysis helps in identifying areas requiring attention and resources for effective risk management.
NASA OCFO’s Agency MBAR is a business tool and financial management mechanism used to facilitate the tracking, monitoring, and reporting of financial management performance indicators both within NASA and externally.

- Stakeholder Community goes well beyond Accounting and Finance, to include Procurement and Systems.
- Makes leaders accountable and focus on business processes, not just financial operations.
- Communication tool for alerting management of potential risk areas so action can be taken to address the issues.
- Ensure monitoring of remedial actions for exceptions reported.
Engage Stakeholders and Process Owners

- Stakeholder Community goes well beyond Accounting and Finance to include:
  - Purchase and Travel Card issuers and users
  - Payment process users and servicers
  - Procurement and acquisition users and servicers
  - Financial Systems users and servicers
  - Financial Information users servicers, and generators of accounting events

- Describe and discuss senior management’s vision with respect to the purpose and objective of MBAR

- Meet with stakeholders to mutually understand related data elements

- Brainstorm with center, NASA HQ, and contract support personnel to obtain ideas for improving MBAR
**Mission**

- We will lead efforts to achieve a safe, secure, and resilient homeland.
- We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure resilience from disasters.

**What is Homeland Security’s Risk Tolerance?**

-- ZERO Failures --

- FY2007 – Created Internal Control Division under CFO
- FY2012 – Transition to Internal Control & Risk Management
DHS

- Department formed in 2003
  - 22 Components brought together/created
    - Different cultures, different missions, different business processes
    - Law Enforcement, 1st Responders, Military, Scientists
    - Mandatory spending, fees, insurance, pensions, grants, loans
      - Inherited Multiple Legacy Financial Systems
- Inherited 30 Significant Deficiencies, 18 Material Weaknesses
  - 15 Components preparing Financial Statements
  - Disclaimer of Opinion FY04-FY10
- Success in FY2011 – Earned Qualified Opinion on Consolidated Balance Sheet and Statement of Custodial Activity
DHS

CFO Desired State
To provide timely, accurate, reliable reporting in support of decision-makers and external stakeholders

Additional Consequences
• Unqualified Opinion on All Statements
• No Material Weaknesses
• Unqualified Opinion on Internal Control
• Removal from the GAO High Risk List
DHS

HOW WE WILL ACHIEVE DESIRED STATE

• Establish strategic risk stewardship plan
• Improve communication
• Involve risk management process in all stages of strategic planning
• Improve capability and tools to measure risk
• Senior management support
• Dedicated resources to strategic risk stewardship
QUESTIONS?