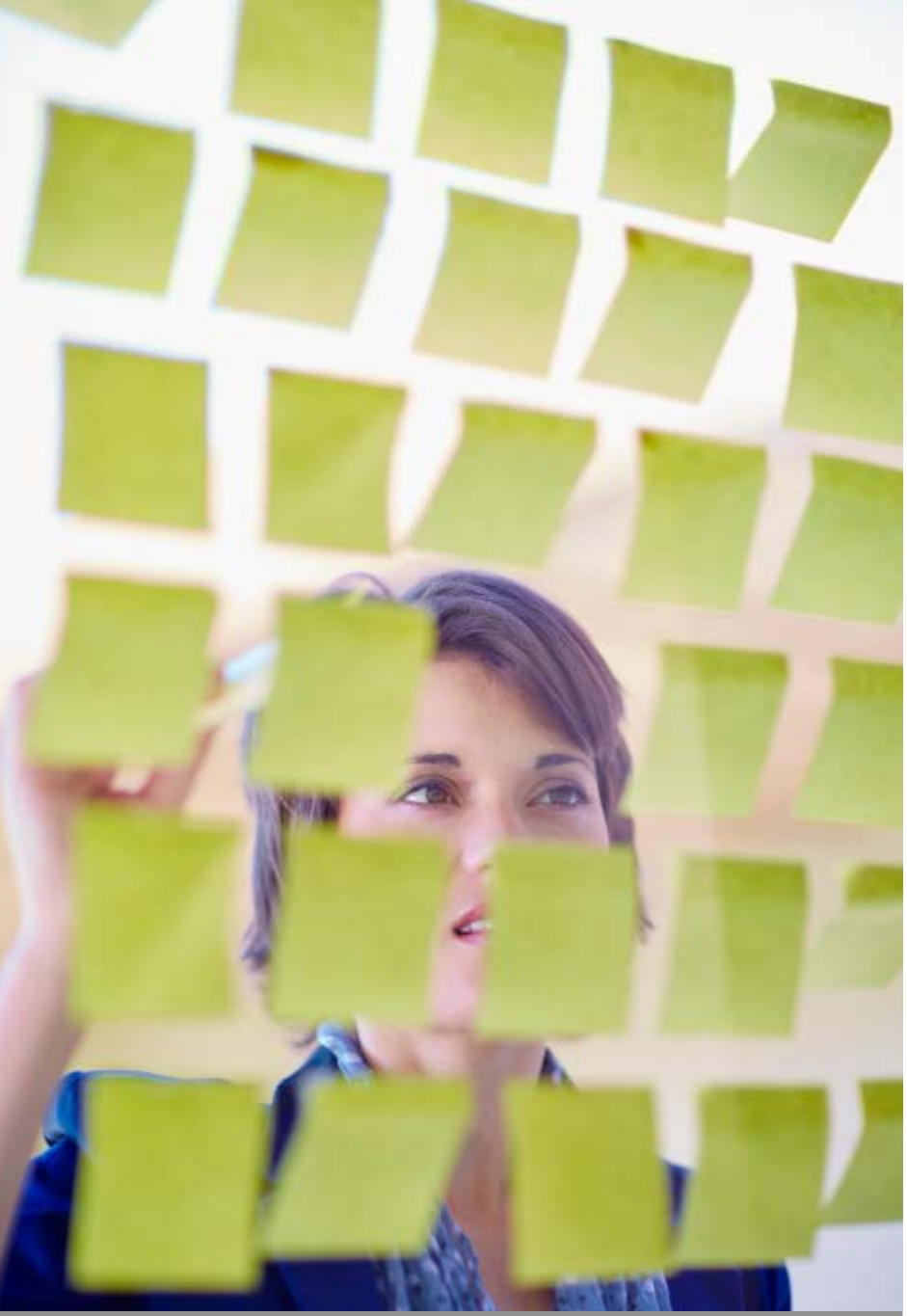
Energize Your Enterprise Risk Management

Presented By
Mark Caiazzo, CISA, CISM, CRISC
Tammy Michaud, CPA

May 15, 2017

BerryDunn

Reviewed:



Agenda

- Enterprise Risk Management Defined
- Benefits of ERM
- Key Components of the ERM Process
- 2017 ERM Survey Results
- Risks Facing NFP Organizations
- A Case Study

What is Risk?

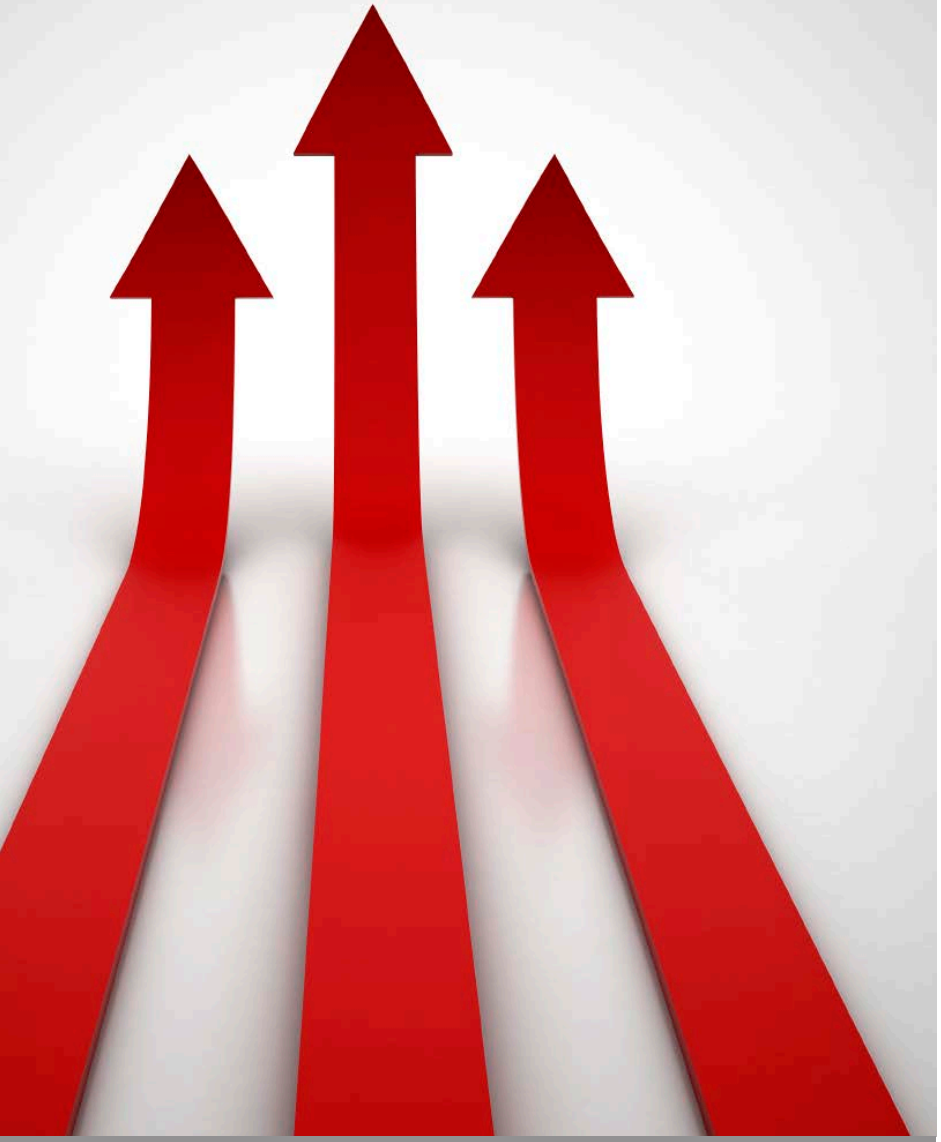
The possibility of an event occurring that may have either a positive or negative impact on the achievement of objectives.

- Harm, loss, danger, threat, and hazard
- Chance, uncertainty, and opportunity

What is Enterprise Risk Management (ERM)?

Committee of Sponsoring Organizations (COSO) – key terms

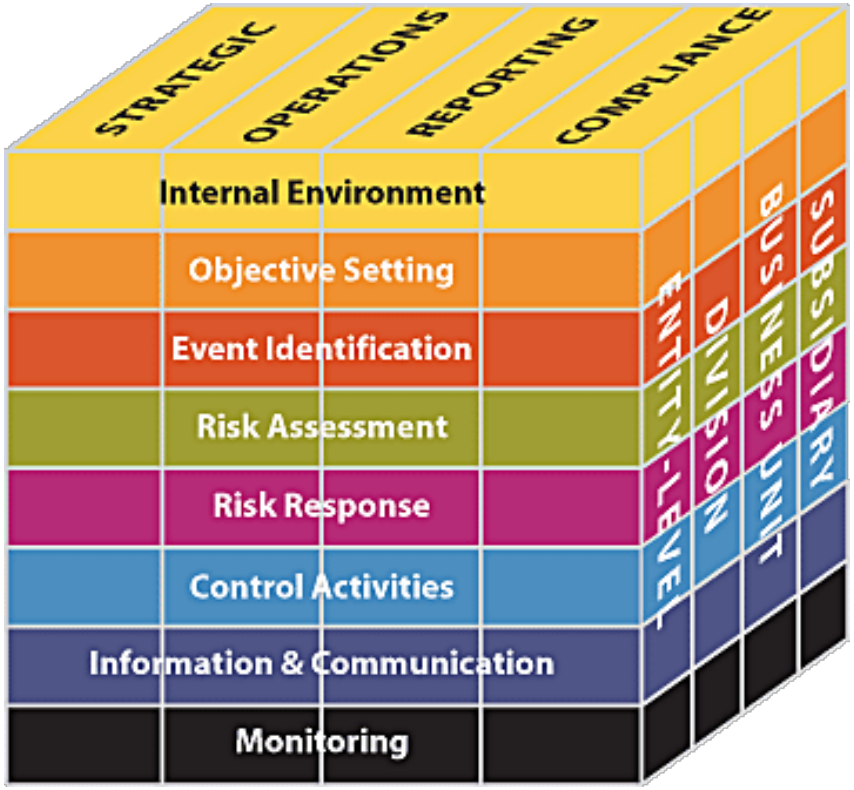
- Continuous process
- Effected by key stakeholders
- Strategically aligned
- Identification of possible events
- Implementation of reasonable measures
- Achievement of entity objectives



Benefits of ERM

- Foundation for many operational activities
- Emphasizes organization-wide accountability and transparency
- Establishes processes to identify risks in a timely manner
- Connects decision-making to risk assessment
- Builds effective audit and monitoring activities
- Helps coordinate regulatory and compliance matters
- Reduces surprises

THE COSO CUBE



Components of ERM

- Internal Environment
- Objective Setting
- Risk Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Measure & Monitor

Internal Environment

The general culture and environment in which an organization operates.

- ✓ Mission, vision, and core values
- ✓ Code of conduct
- ✓ Employment policies
- ✓ Communication - “tone at the top”
- ✓ Strategic plan
- ✓ Governance plan

Objective Setting

The process management uses to set its strategic goals and objectives and establish the organization's risk appetite and tolerance.

- ✓ Strategic risk
- ✓ Operational risk
- ✓ Financial risk
- ✓ Compliance risk
- ✓ Reputational risk

Risk Identification

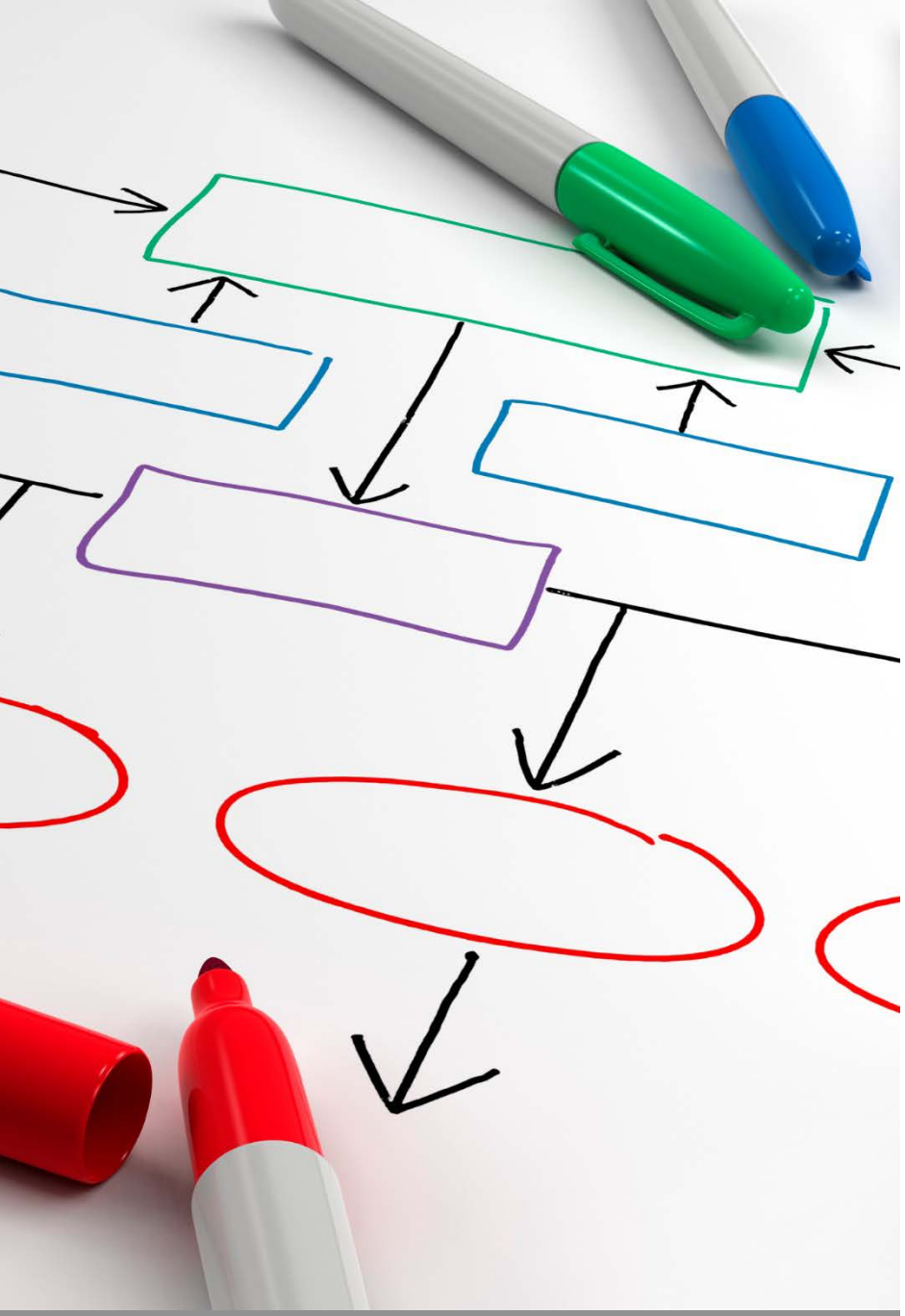
The process used by an organization to identify events that influence strategy and objectives, or could affect an organization's ability to achieve its objectives.

- Facilitated group discussions
- Questionnaires
- Industry benchmarking
- Historic trend analysis
- Understanding regulatory requirements
- Third-party arrangements (down-stream risks)

Risk Assessment

The organization’s process of evaluating the impact and likelihood of events, and prioritizing related risks.

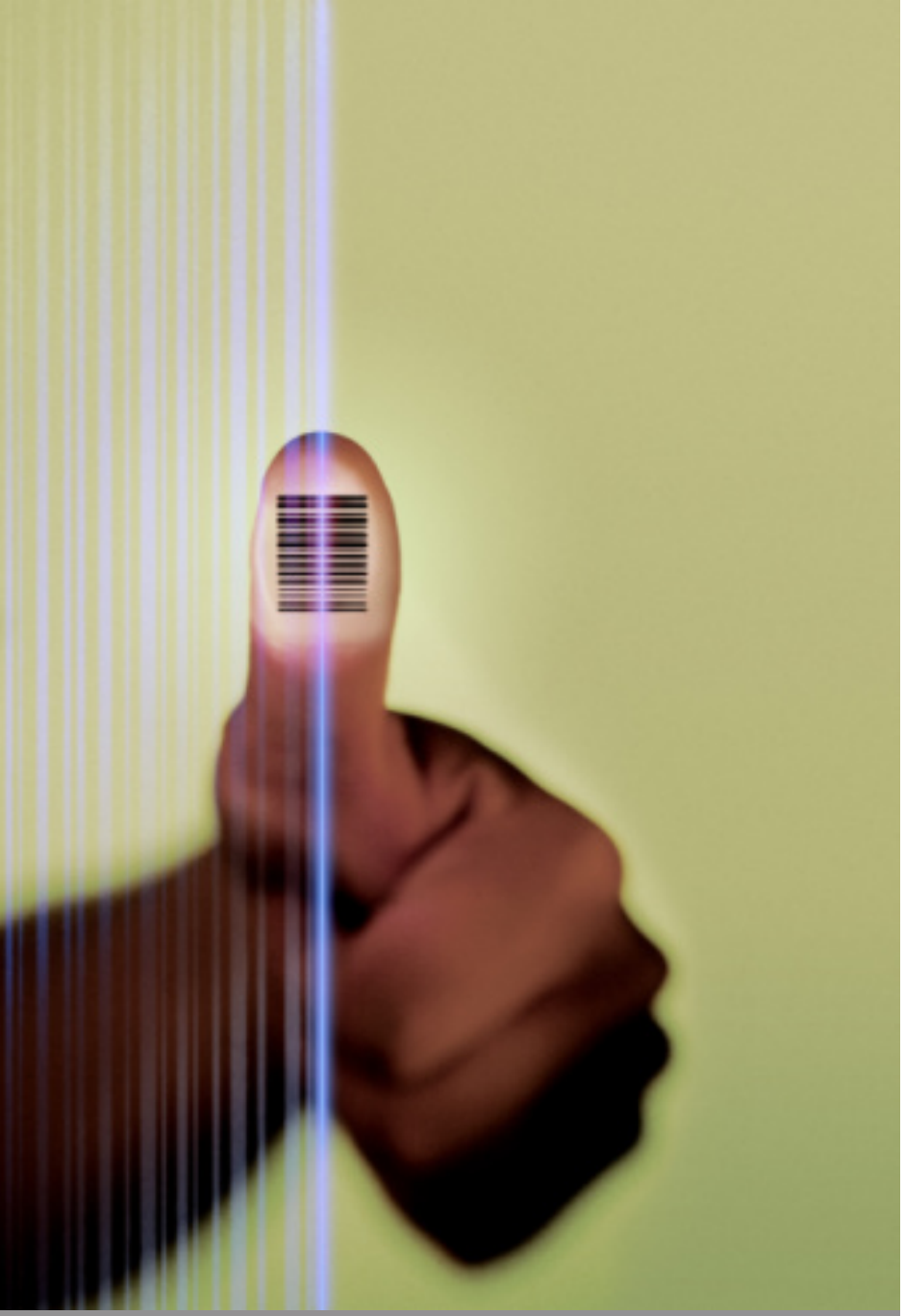
- ✓ Probability of risk occurring
- ✓ Potential impact if it occurs
- ✓ Qualitative vs quantitative analysis
- ✓ Consideration of risk appetite
- ✓ Consideration of third-parties
- ✓ Consideration of controls, processes, and systems already in place



Risk Response

Determining how management will respond to the risks an organization faces.

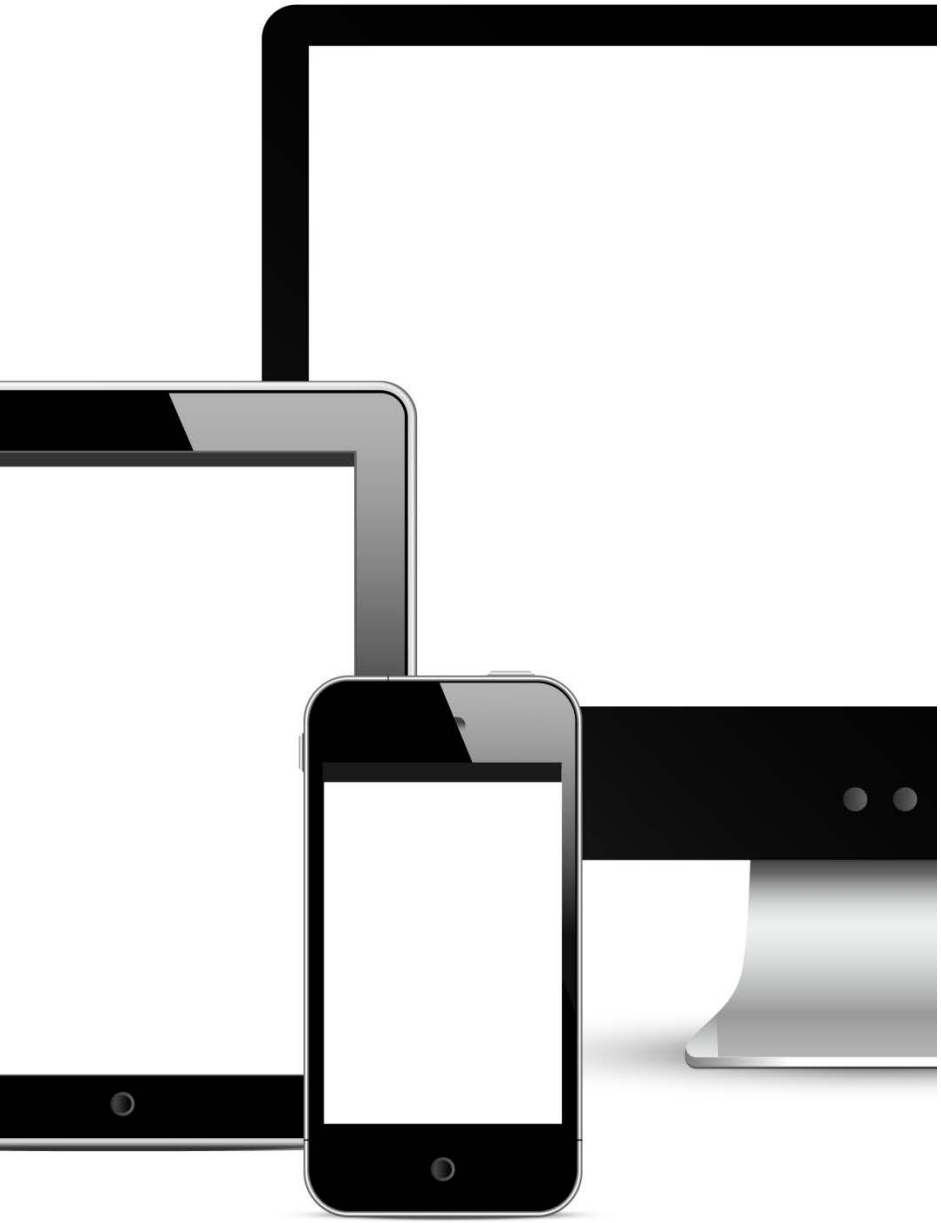
- ✓ Risk mitigation – fix or reduce the risk to a cost-effective level
- ✓ Risk acceptance – deal with it
- ✓ Risk avoidance – decision not to proceed
- ✓ Risk transfer – let a third-party deal with it
- ✓ Risk financing – cover with insurance



Control Activities

Policies, procedures, and systems that an organization implements to address the risks the organization chooses to mitigate.

- ✓ Business resumption plans
- ✓ Incident response plans
- ✓ Training programs
- ✓ Communications plans
- ✓ Vendor due diligence program



Information and Communication

The practices that ensure that the right information is communicated to the right people, at the right time.

- ✓ Staff education
- ✓ Board education and reporting
- ✓ Customer communication
- ✓ Incident response
- ✓ Compliance reporting

Measure and Monitor

Ongoing evaluations to ensure controls are functioning as designed, and taking corrective action to enhance control activities if needed.

- ✓ Internal audit program
- ✓ GRC program
- ✓ Balanced scorecard
- ✓ Maturity modeling
- ✓ Customer and stakeholder feedback

2017 AICPA ERM Survey

Survey Results

- 58% of NFP respondents believe the volume and complexity of risks have increased significantly in the last 5 years
- 56% of NFP respondents indicate their organizations are risk averse or strongly risk averse
- 26% of NFP respondents have no formal ERM program in place or planned
- 59% of NFP respondents indicate they have provided no or only minimal RM training in the past 2 years
- 45% of NFP respondents indicate they feel pressure (somewhat or mostly) from outside parties to provide increased risk management information

2017 AICPA ERM Survey
REPORT ON ERM BARRIERS

- Competing priorities – 45%
- Insufficient resources – 44%
- Lack of perceived value – 37%
- Perception that ERM adds overhead – 28%
- Lack of executive leadership – 27%
- Legal or regulatory barriers – 5%

Evolving Risks

- Operational
- Financial
- Compliance

- Cash management
- Customer retention
- Human capital, culture
- Information technology
- Industry or economic changes
- Fraud
- Reputation, brand, image
- Privacy

Specific NFP Risks

- Economy
- Funding sources
- Donor retention
- Excess compensation and benefits
- Transparency / Transactions with related parties
- Compliance

Case Study – A Hypothetical

A not-for-profit recently found itself with an opportunity for rapid growth. A grant was given, significantly increasing the organization's funding and possibilities. This growth resulted in expansion for a couple of years, but as business grew, the organization's knowledge of proper infrastructure management and how to foresee and address risk did not keep pace.

The organization's first step to solving this problem was to identify the major risks they faced, plan an approach to address these risks, and a then developing a plan to monitor the major risks.

Case Study – Approach to Risk

- Educate management and key decision-makers in risk management practices and strategies. Ensure there is sponsorship.
- Assemble a working Committee comprised of management and staff with appropriate skill sets
- Clearly identify and document roles and responsibilities of those on the Committee
- Facilitate risk management meetings and provide open discussions and brainstorming to identify risks throughout the organization
- Rate the identified risks (impact, likelihood, and timeline), identify the controls that mitigate these risks, and establish risk event response plans
- Establish a communication plan
- Develop a monitoring and reporting program for risk, including regular updates from the Risk Committee to the Board

Roles and Responsibilities

Case Study – The Risks

Once management was educated, and roles and responsibilities were defined and understood, they were ready to begin working with the Risk Committee. With work sessions, they identified the risks.

Some risks addressed by the committee:

- Contract Negotiation
- Cash flow management
- Inadequate payroll control
- Client service
- Licensing/Service authorization providers

Case Study – Risk, A Deeper Dive

After the risks were identified, the Risk Committee was confident enough in its assessment to discuss risks further through the next step, which was to facilitate interactive sessions.

These sessions shed light on risks that were related to:

- Funding sources
- Human capital
- Legislative
- IT
- Social media
- Financial
- Conflicts of interest
- Reputation

Risk Rating Matrix

	Risk Event	Severity	Likelihood	Timeframe	Controls	Rating
1	Cash flow impairment	High	Moderate	Moderate	Weak	High
2	Contract negotiation failure	High	Moderate	Moderate	Weak	High
3	Pre-authorized failure	Low	High	Rapid	Weak	High
4	Loss of funding source	High	Low	Slow	Weal	Moderate
5	Disaster recovery / Business continuity failure	High	Moderate	Rapid	Adequate	Moderate
6	Client billing failure	Low	High	Rapid	Adequate	Moderate
7	Key employee departure	High	Low	Moderate	Adequate	Moderate
8	Payroll fraud	Moderate	Low	Moderate	Strong	Low

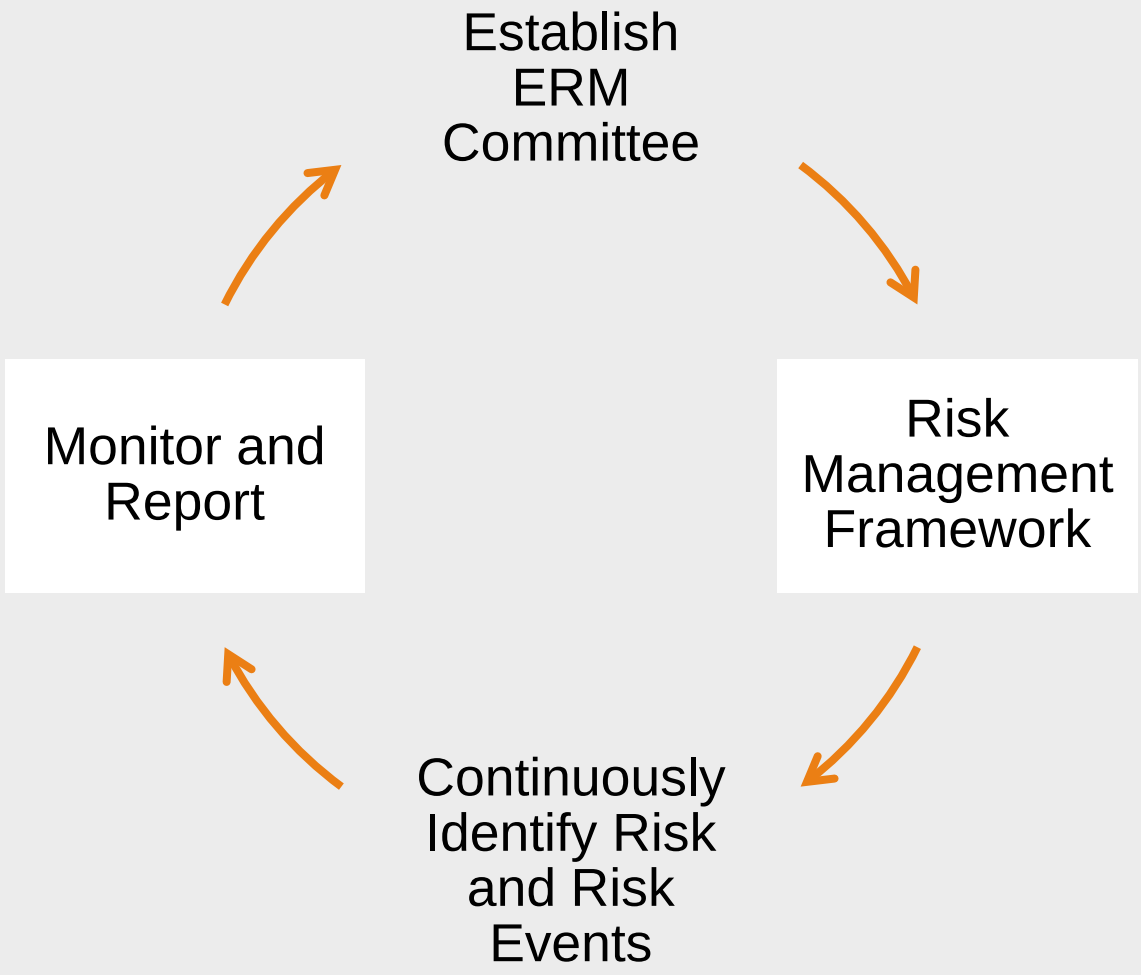
Risk Mitigation

	Risk Event	Mitigation Analysis
1	Cash flow impairment	• Implement cash flow reporting • Possible line of credit for short term aid • Review current accounts receivable for collectability • Develop authorized credit approval procedures for future counter-parties. • Designate representatives for major accounts • Streamline and enhance control of billing and collection processes
2	Contract negotiation failure	• Identify consulting partner to provide assistance with negotiations • Establish a Deal Review Board to authorize material agreements • Develop proper training programs for vital resources • Analyze in-force agreements for improvement opportunities

Risk Monitoring and Reporting

- A Risk Management Committee to perform on-going reviews and alignments for the organization’s operation strategies
- Risk monitoring responsibilities to senior resources
- Monthly reporting protocols for key resources
- Key risk indicators to be addressed at Board Meetings
- Periodic risk education updates throughout the organization on all levels
- An environment of employee buy-in, continual process, and control improvement

The Never Ending Story



Maturity Model: Where are You?

Interested in more?

Mark Caiazzo, CISA, CISM, CRISC
Principal
mcaiazzo@berrydunn.com

Tammy Michaud, CPA
Principal
tmichaud@berrydunn.com