PRIMA'S 2019 RISK MANAGEMENT
WEBINAR SERIES

Integrating ERM with the Strategic Planning Process

Tim Wiseman
Enterprise Risk Manager and PRIMA Faculty Member

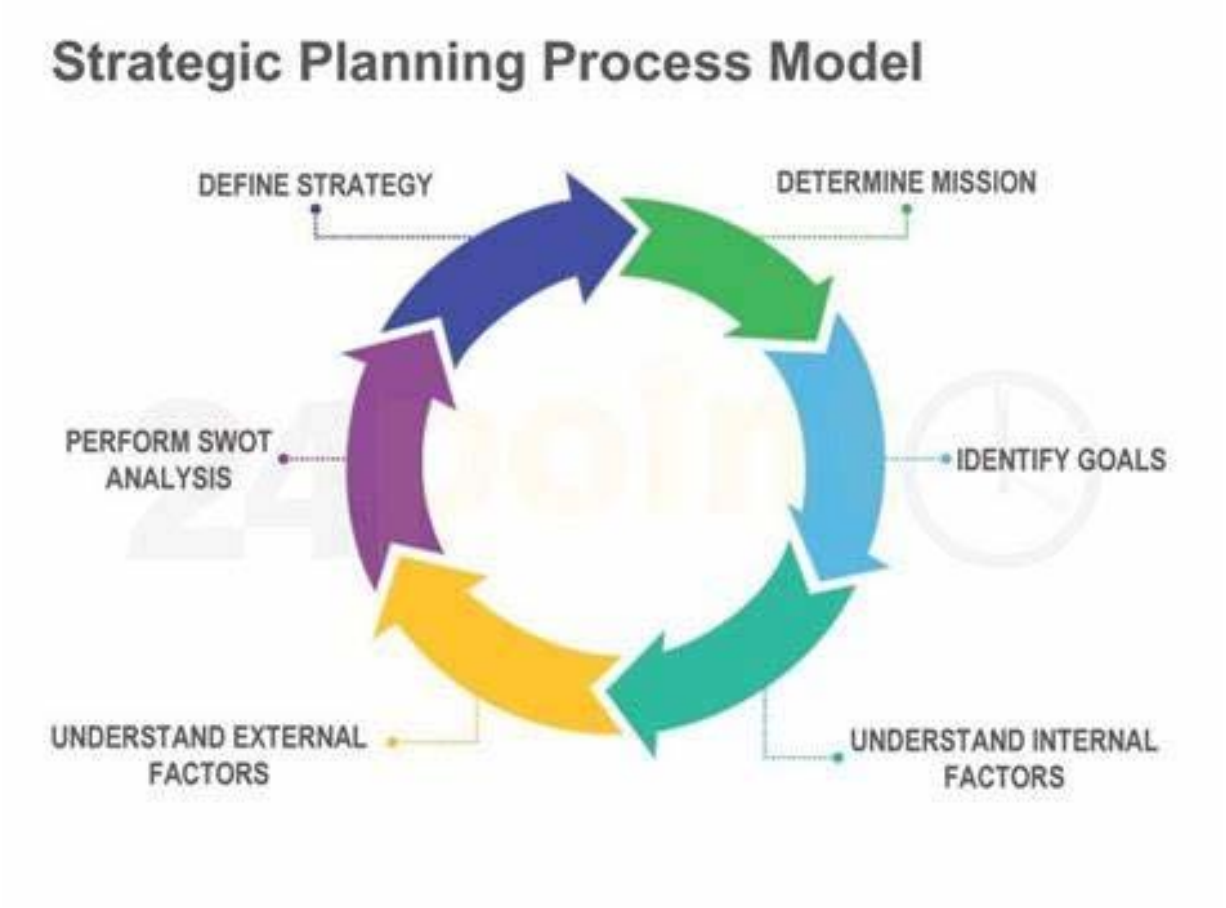
Ellen Shew Holland
President, Strategic Risk Frameworks, LLC
Higher Education Practice Leader - Hanover Stone Partners

October 16, 2019

Agenda

- Sources of Strategic Direction and Planning Guidance for Public Entities
- Including Modern ERM Concepts in the Strategy Setting
- Strategic Risk Management
- Questions and Answers

Sample Strategic Planning Process Model



What are some "peculiarities" to strategic planning in public entities?

Evolution of Risk Management

Transactional

Historic Risk Management

- Insurance
- Specific hazards
- No compliance input
- Separate safety & emergency management
- "Silo" approach
- Risk Manager = insurance buyer

Risk is bad – focus is on transferring risk

Integrated

Advanced Risk Management

- Alternative risk transfer techniques
- Proactive prevention & risk reduction
- Integrated approach to claims, contracts, insurance, etc.
- Increased education & accountability
- Collaboration across departments
- Risk Manager *may* be the risk owner

Risk is an expense – focus is on reducing cost-of-risk

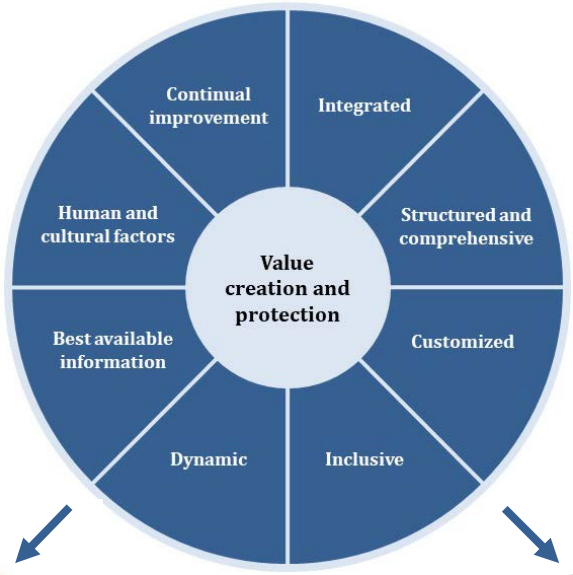
Strategic

Enterprise-Wide Risk Management

- Broad range of risks analyzed
- Combination of risk controls & opportunities
- ERM alignment with strategy
- Helps manage growth, allocate capital & resources
- Risks owned by subject matter experts
- Greater availability of risk mitigation and analytical tools
- Risk Manager = risk moderator, partner, leader; *not* the owner of every risk

Risk is uncertainty – focus is on optimizing risk to achieve goals

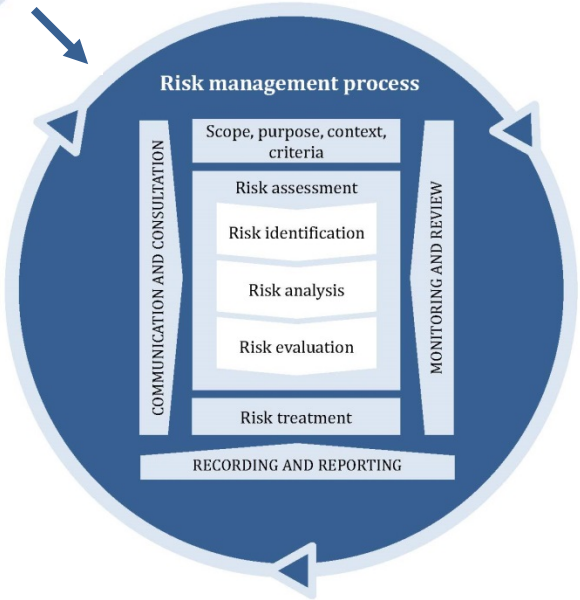
Purpose & Principles



The Framework



Risk Management Process



ISO 31000 – Figure 1

Framework



The **purpose** of the risk management framework is to integrate risk management into **all** activities and functions.

Leadership and commitment is at the core of all risk management activities and functions.

Leadership and Commitment

Senior leaders and governing boards, together:

Ensure RM is integrated into <u>all</u> organizational activities

Senior leaders:

Accountable for managing risk

Governing boards:

Accountable for overseeing RM

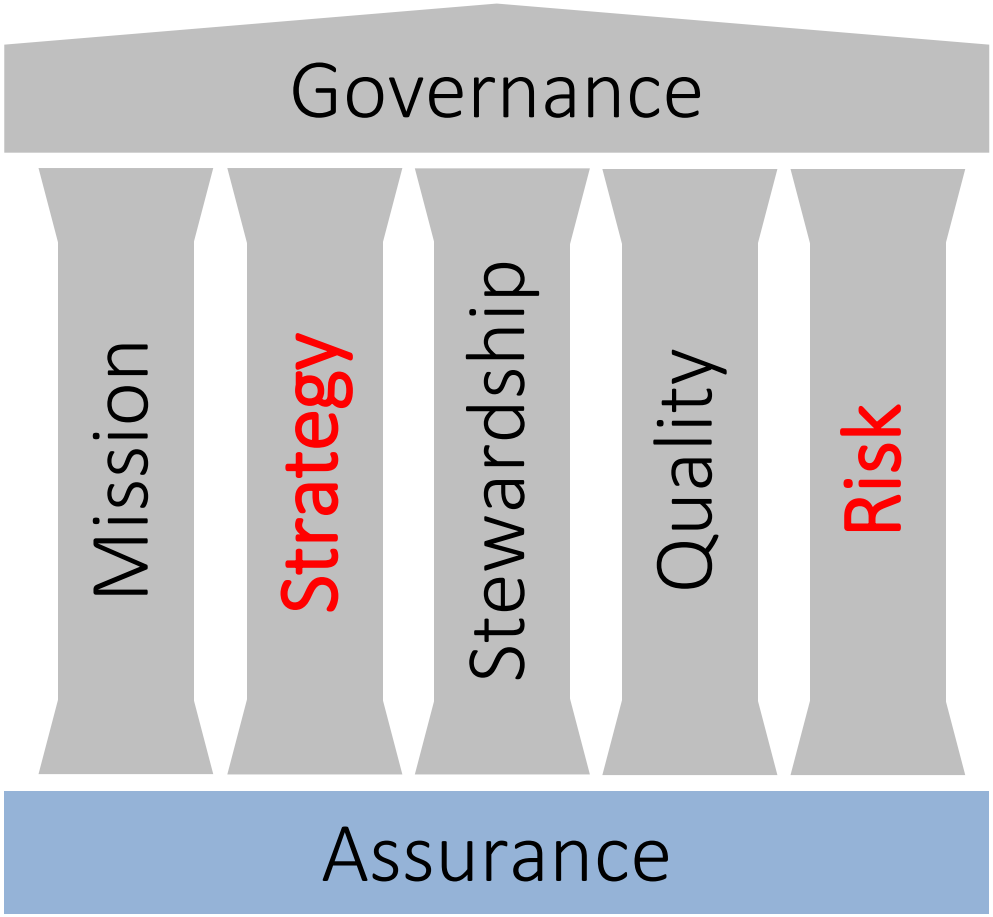
Leadership and Commitment

Role of Governing Board re Risk

- Fiduciary responsibilities
- **Strategic direction**
- Gives input re global uncertainties and trends
- Sets the tone and demonstrates commitment to the comprehensive management of risk
- Oversight of management's plans and execution

Does your organization's governing board understand its responsibilities regarding risk oversight? What about the Audit Committee? Are roles clearly delineated?

RM as a Pillar of Governance



Strategy

Senior leadership, in conjunction with the board, develops strategic plans to carry out the organization's mission. Determining and executing strategy requires and supports good governance.

Demonstration of Leadership and Commitment

- Aligning RM with **strategy**, objectives, and culture
- Issuing statement or policy establishing RM approach
- Ensuring necessary resources
- Assigning authority, responsibility, and accountability at appropriate levels
- Recognizing and addressing all obligations of the organization
- Establishing amount and type of risk that may or may not be taken
- Communicating the value of RM to organization and stakeholders
- Promoting systematic monitoring of risks
- Ensuring RM framework remains appropriate

Demonstration of Leadership and Commitment

- Aligning RM with **strategy**, objectives, and culture
- Issuing statement or policy establishing RM approach
- Ensuring necessary resources
- Assigning authority, responsibility, and accountability at appropriate levels
- Recognizing and addressing all obligations of the organization
- Establishing amount and type of risk that may or may not be taken
- Communicating the value of RM to organization and stakeholders
- Promoting systematic monitoring of risks
- Ensuring RM framework remains appropriate

Why is Culture Important?

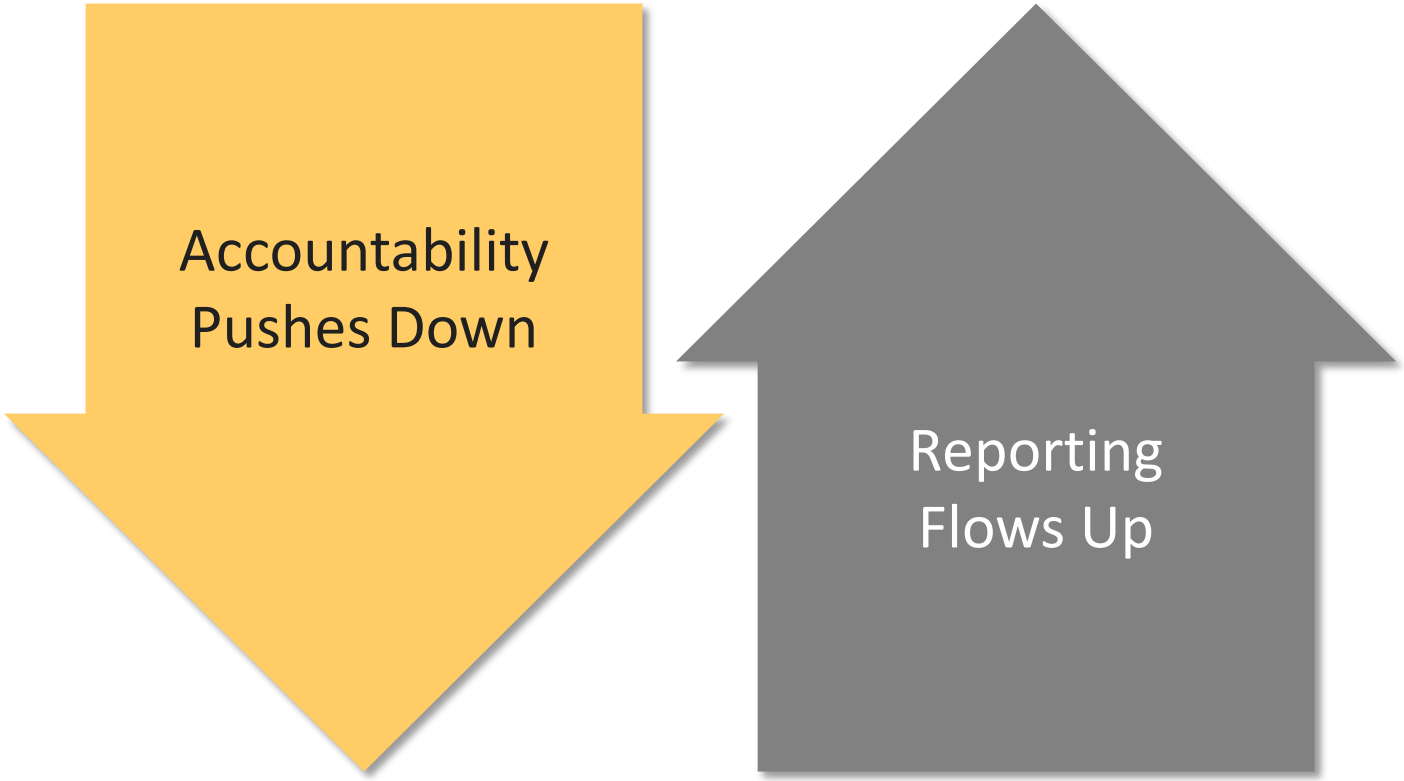
- Culture is very stable and slow to change – it is embedded in organizational processes and actions
- Culture drives attitudes and beliefs
- Culture can have drastic consequences for overall performance – and can kill organizational initiatives



The Ideal Scenario!

- Objectives and governance structures are clear, agreed to and aligned across your entity
- Organizational performance is measured and tracked
- Your culture accepts uncertainty and supports risk taking
- The executive's preference for risk taking is understood and reflected in risk rating/reporting

Accountability



Framework



The purpose is to integrate risk management into organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

Integrating RM

Integrating risk management relies on an ***understanding of organizational structures and context***. Structures differ depending on the organization's purpose, goals and complexity.

Risk is ***managed in every part*** of the organization's structure. Everyone in the organization has responsibility for managing risk.

Section 5.2.2 of ISO 31000

Integrating RM

Governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices to achieve its purpose. ***Management structures translate*** governance direction into the **strategy** and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining the ***accountability and oversight roles*** within an organization are ***integral parts of the organization's governance***.

Section 5.2.2 of ISO 31000

Integrating RM

Integrating risk management into an organization is a dynamic and iterative process, and should be ***customized to the organization's needs and culture***.

Risk management should be a ***part of, and not separate from***, the organizational purpose, governance, leadership and commitment, **strategy**, objectives and operations.

Section 5.2.2 of ISO 31000

Articulating RM Commitment

- Reasons for managing risk and links to organization's objectives and other policies
- Reinforcing the need to integrate risk management into overall culture of the organization
- Leading integration of risk management into core business activities and decision-making
- Authorities, responsibilities and accountabilities
- Making necessary resources available
- Way in which conflicting objectives are dealt with
- Measurement and reporting within the organization’s performance indicators
- Review and improvement
- **Creating VALUE!!!**

Section 5.3.2 of ISO 31000

Articulating RM Commitment

Articulation of commitment can be through:

- Policies
- Statements and addresses
- Committees
- Employee evaluations
- Newsletters and other regular communications
- Everyday interactions
- Training – RM and incorporated into other

Sample Governance Model

Name of Group	Role	Overview
Governing Board	Oversight	Big picture, strategy, holds management accountable
Audit Committee	Assurance	Reports to the Board on key risks, integrates key risks into audit plan
ERM Advisory Committee	Management	Provides authority and oversight, responsible for progress
ERM Working Group	Implementers	Responsible for program development and implementation
Risk Owners	Responsible for managing individual risks	Control and management of individual risks, coordination and reporting


Good tactics can save even the worst strategy. Bad tactics will destroy even the best strategy.
— George S. Patton —
AZ QUOTES

Strategic Risk Management
ISO 31000:2018

Integrating Strategic Risk Management (SRM) with Strategic Planning

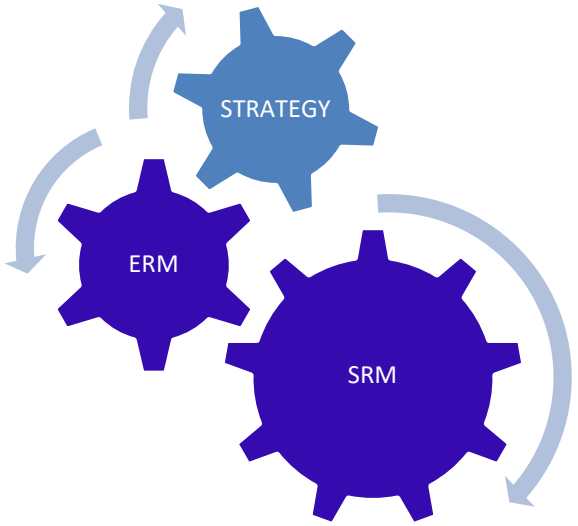
Objectives

1. Identify the differences between:
   - Enterprise Risk Management (ERM)
   - Strategic Risk Management (SRM)

2. How to integrate SRM into your strategic planning

3. Useful tools

Overview and Definitions



STRATEGIC RISK MANAGEMENT (SRM)

- ISO 31000:2018 for Risk Management |
- COSO ERM FRAMEWORK 2017
- Other REFERENCES : COSO* 404-Sarbanes-Oxley and ISO 27000-Cyber
- SRM aligns risk & decision-making to external and strategic risks
- Cyber Security and Privacy risk is noted in 5 of the Top 10 Risks*

*COSO-Committee on Sponsoring Organizations
*COSO 2017 is ERM Framework
*Corporate Compliance Insights 2019-Top 10 Risks

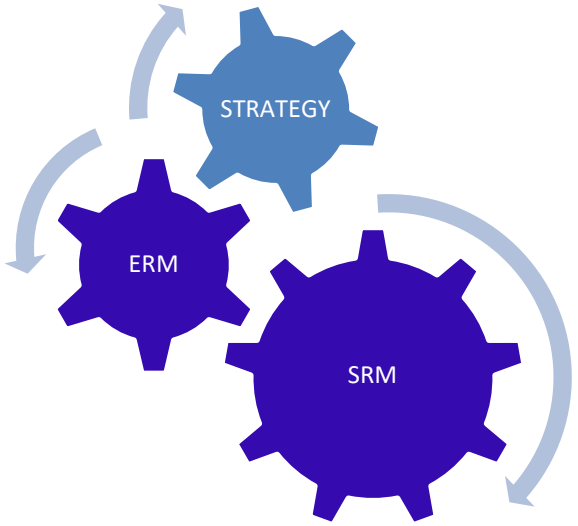
Enterprise Risk Management (ERM)

- Integrated framework focused on *internal* risks-ISO 31000-2009
- Embeds risk mitigation within critical decision-making processes
- Interdisciplinary team/FTE's with high levels of accountability
- Risk Manager manages the process and is accountable for detail
- Originated through COSO 404-Sarbanes-Oxley;
- Similar to ISO 27000, Cyber Security
- ROI perception is low depending upon results desired

Strategic Risk Management (SRM)

- Integrates and aligns risk mitigation into strategic considerations
- Focuses on external and strategic risks-ISO 31000:2018
- Risk Manager consults with process owner to mitigate risk
- Can be used as a compliment to an ERM program
- The board sees an efficient and effective program with results

Steps in Starting Your Program

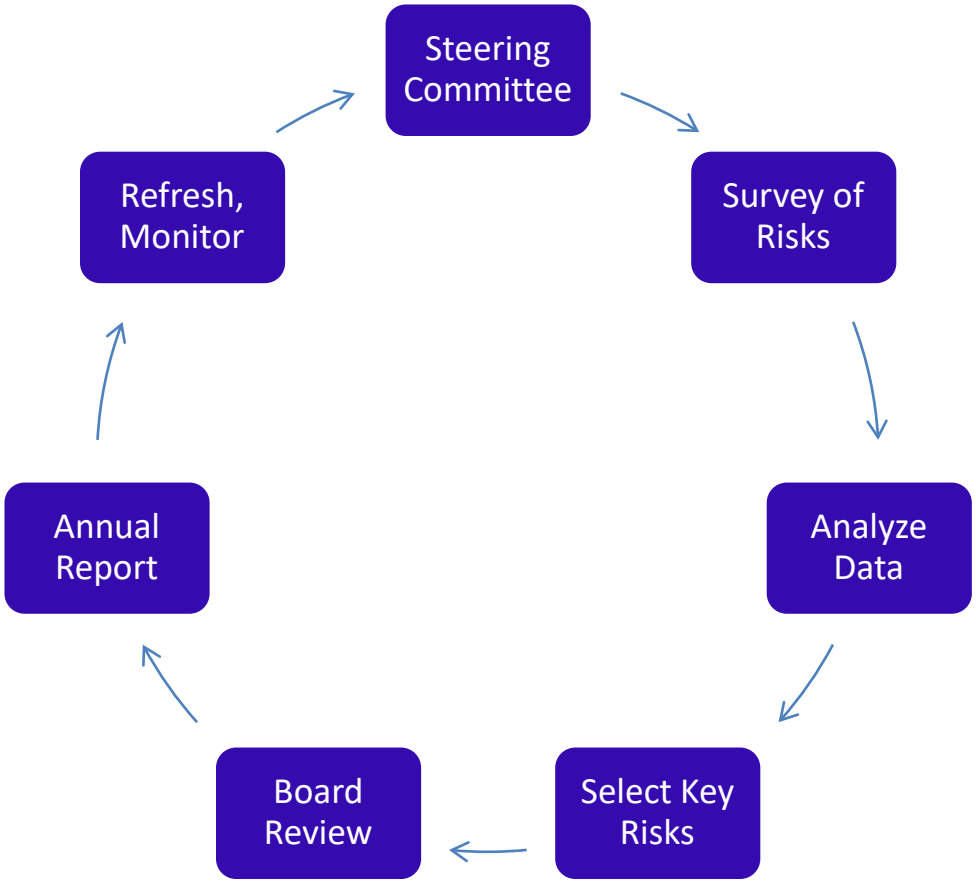


Strategic Risk Management vs. Enterprise Risk Management

Items of Interest	SRM: ISO 31000-2018	ERM: ISO 31000-2009
Outcome	▪ Focuses on 3 strategic or "Key Risks" ▪ Strategically and externally focused ▪ Implemented in 4-6 months	▪ Identifies 10-20 "Key Risks" from 100 risks ▪ Internally focused-good for Hospitals, etc. ▪ Implemented in 1-3 years
Resources Used	▪ Steering committee of 4-6 persons ▪ ROI is effective	▪ Team of 10-12 persons plus 1-2 FTE's; ▪ Low *ROI perception ▪ Effective for hospitals, research emphasis
Reporting	▪ Results of 3 Key Risks within 1 year ▪ Customized "Scorecard" or report for monitoring current/prior risks	▪ Reporting results may take 2-3 years ▪ Report includes: risk register, heat map, or scorecard-reviewed annually
Board Engagement	▪ Aligns with Strategy ▪ Risk Manager likely perceived effective ▪ Can be supplemental to ERM	▪ Internal process focus with 10-20 key items ▪ Risk of too much information at the Board level; minimizing Risk Manager effectiveness
Risk Owner Engagement	▪ Process owners own the risk mitigation and monitoring ▪ SRM Team/CRO consult risk mitigation	▪ CRO and ERM Team "own" the responsibility with burden on their shoulders

*Return on Investment (ROI)

Starting Your SRM or ERM Program



How To Implement: Plan, Survey, Analyze

Plan

- Get a “Champion” such as a VP for Finance or Chief Academic Officer
- Create a project plan with timeline and task deadlines
- Meet with Steering Committee regularly to keep on track

Conduct a Survey

- Include select leadership at varying levels
- Create questionnaire so that it can be analyzed with reliability

How To Implement: Plan, Survey, Analyze

Analyze

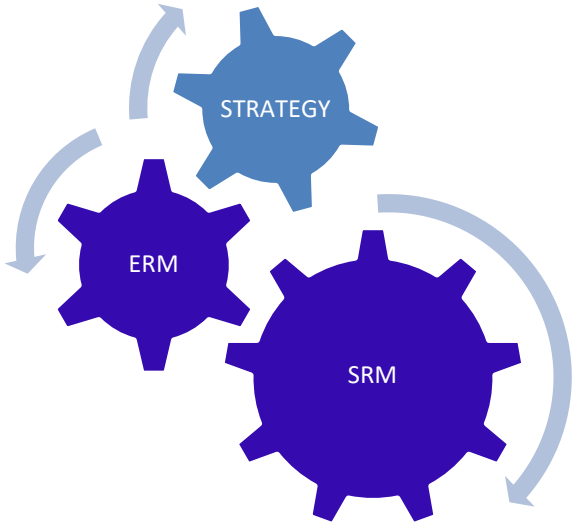
- Open-ended questions regarding risk can be categorized by “type”
- Sub-level questions must have multiple choice options with a numbering system to weight and rank answers in order to analyze
- From the pivot analysis and weighting and ranking, create color-coded charts

How To Implement: Reporting

Reporting

- Annual report showing methodology, results, narrowing of current key risks
- Monitoring key risks once completed to continue risk mitigation
- Allows flexibility to include urgent risks or opportunities as needed

Tools for Your Program



SRM Program – Sample Timeline

Strategic Risk Management Program (SRM)
by Strategic Risk Frameworks, LLC.

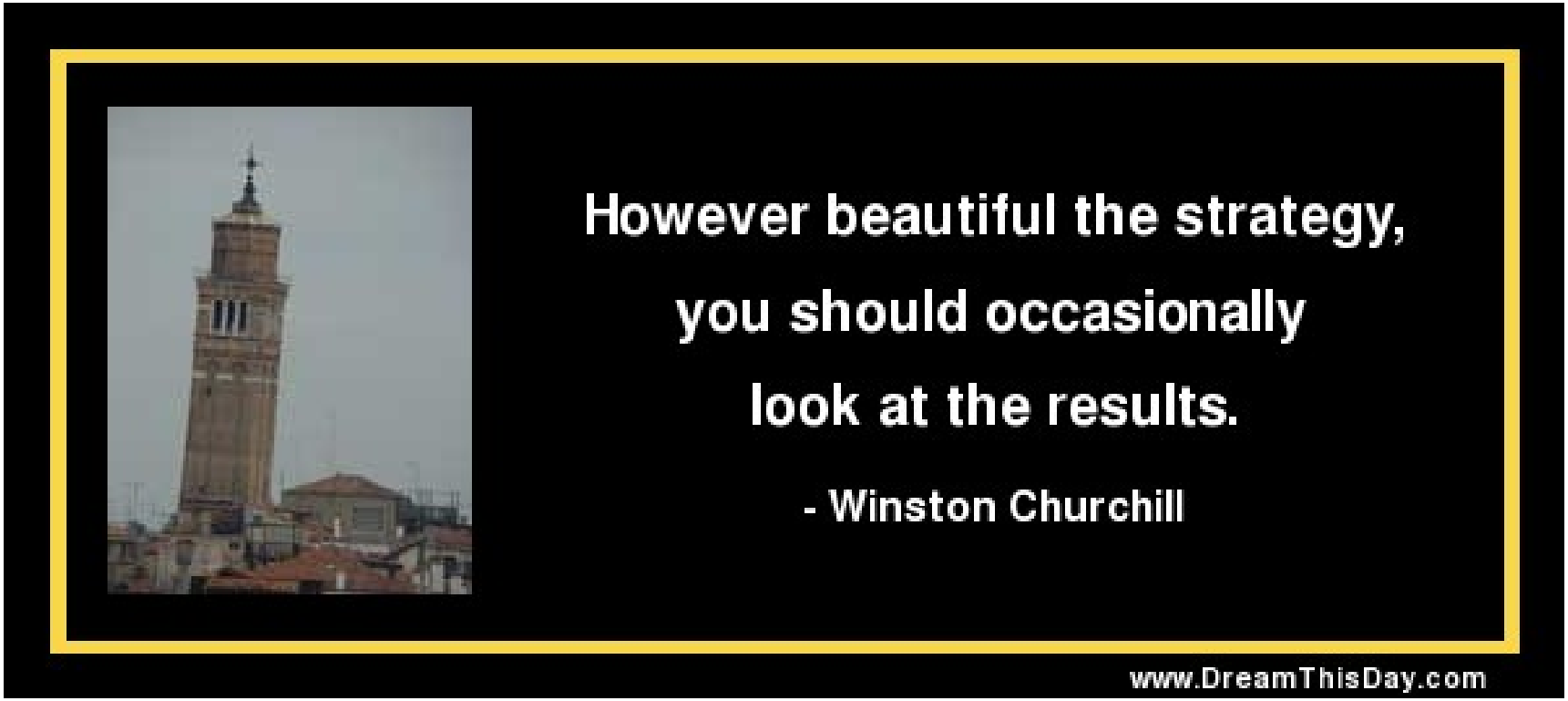
ABC University
Facilitator: Ellen Shew Holland, ARM; Hanover Stone Partners (HSP), LLC and Strategic Risk Frameworks (SRF), LLC
Dates: February 2019 - September 2019

Major Task	Responsible Party	February	March	April	May	June	July	August	September	October	Year 2 Review	Year 2 Updates	Year 3 Review & Updates
Present Program	IMA/HSP												
Approval of Program	School												
Kick-Off Meeting w/Team	School/HSP	February											
Prepare Survey for Committee	Team /HSP	February	March.										
Conduct Survey	Team / HSP		March/April										
Analyze Survey	HSP			April									
ID Key Risks and Risk Owners	Committee			April/May									
Prepare First Draft of Report	Team/HSP					June/July							
Final Board Report	Team/HSP								September				
Debrief	Committee									October			
END of INITIAL PROJECT IMPLEMENTATION													
Ongoing Monitoring (Internal or through IMA/HSP-SRF)													
Review prior year report											January		January
Identify Key Risks or conduct survey												March	March
Maintain "Legacy" Key Risk Balance Scorecard Monitor Report												May	May

Monitoring: Sample Scorecard for a Risk

Sub 2	Increasing Competition - specifically Company A. New competition being seen from Company B in South America.				Natural disaster damages Plants 1 and 2 and we are down for 3 -4 months.				Looking to consolidate operations of 3 plants into 2. Potential loss of key talent because people will not be willing to move.			
UNMITIGATED RISK EVALUATION	Probability	Impact	Velocity	Total Risk Value	Probability	Impact	Velocity	Total Risk Value	Probability	Impact	Velocity	Total Risk Value
	4	4	4	64	3	3	4	36	3	4	5	60
MITIGATING FACTORS	New multi lingual customer srvice teams are still working effectively. Efforts continue to improve quality & delivery. Owning facilities locally is proving to be very beneficial for sales and good will.				There is new equipment being installed and there are new tests being performed that can be outsourced more easily. We note that the impact of Plant 1 being down a 3-6 month period would have no immediate business impact thus allowing us to reduce the mitigated risk score. Both plants work can be outsourced and/or picked up by plants 3, 4 and 5.				Work closely with HR to identify key resources that will consider and not consider moving. Develop requisitions for the key positions that will not moving and begin searches immediately.			
MITIGATED RISK EVALUATION	Probability	Impact	Velocity	Total Risk Value	Probability	Impact	Velocity	Total Risk Value	Probability	Impact	Velocity	Total Risk Value
	3	3	3	27	3	3	3	27	3	2	4	24
ADDITIONAL RISK RESPONSE	6 customers have moved to Sub 2 due to Company A faltering. We continue to fix customer service issues. Plant upgrades are in process to better service all customers. We plan to be able to hold onto 4 of the 6 customers we converted this year.				Continue to look for outsourcing partners as backup. Most of this work is completed.				Provide excellent relocation and house finding benefit. See if remote working conditions is a possibility with one week travel to plant site per month.			

Questions?


However beautiful the strategy,
you should occasionally
look at the results.
- Winston Churchill
www.DreamThisDay.com