PRIMA'S 2016 RISK MANAGEMENT
WEBINAR SERIES

ERM: Risk Maps and Registers

Performing an ISO 31000 Risk Assessment

Agenda

- Following a Standard?
- Framework First
- Performing a Risk Assessment
- Assigning Risk Ownership
- Data Management
- Questions?

Following a Standard?

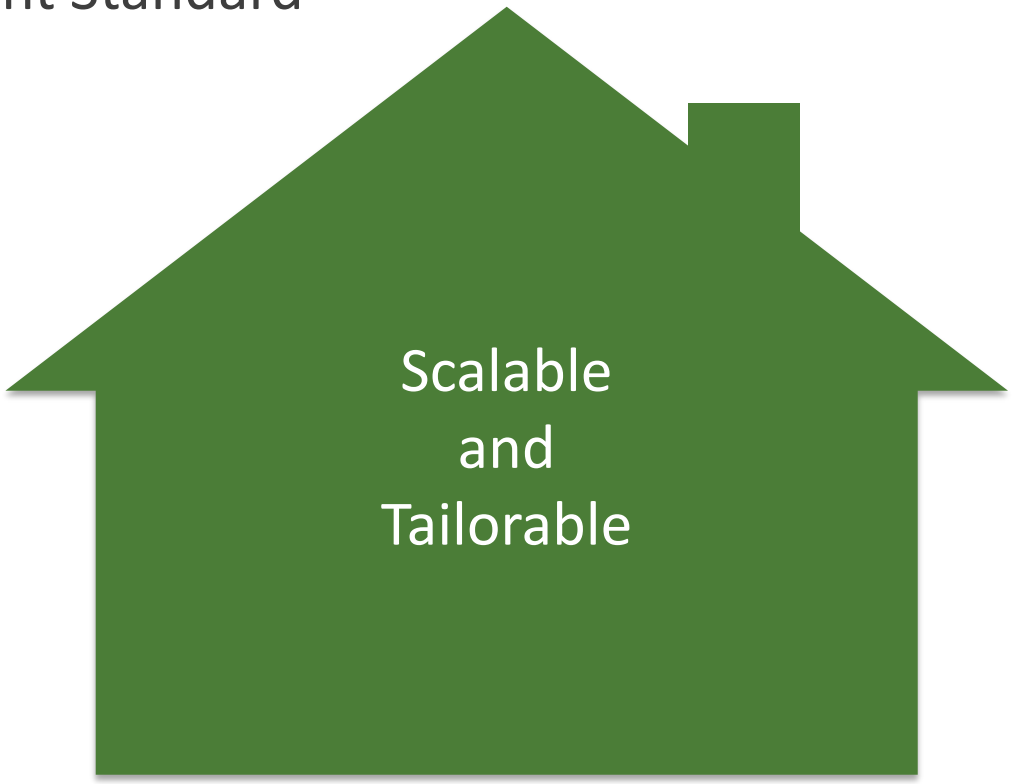
ISO 31000

The International Risk Management Standard



ISO 31000

The International Risk Management Standard

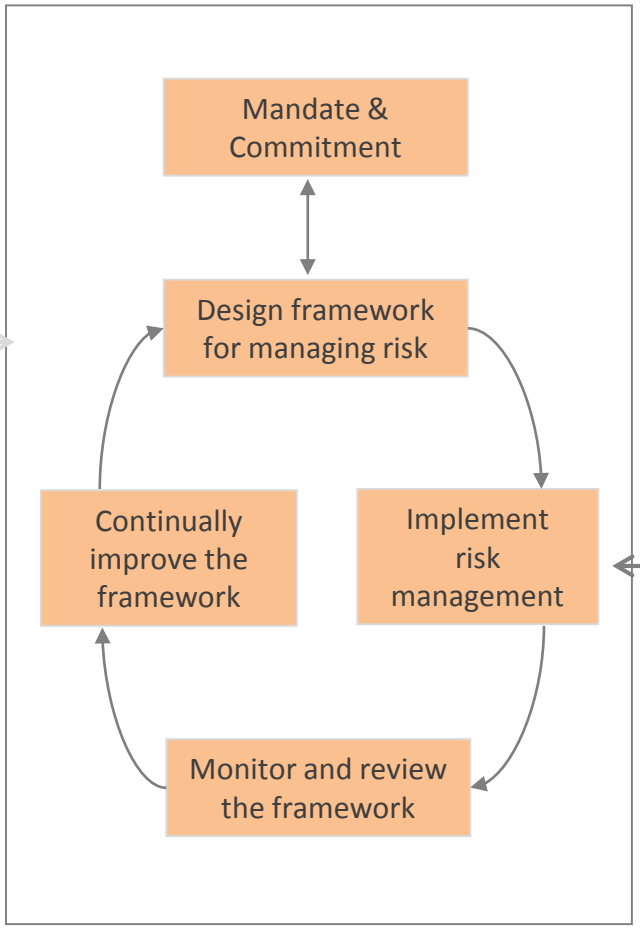


ISO 31000 Risk Management Model

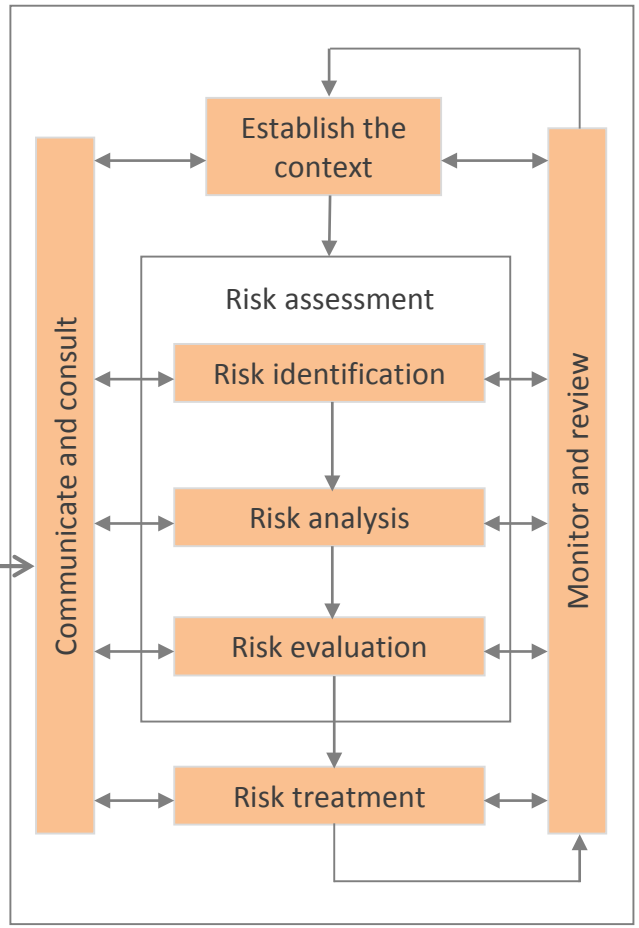
Principles

- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on best available information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement and enhancement of the organization

Framework



Process



Framework First

Written Risk Management Framework

- Best way to get everyone on board
- Answers the questions:

  "Why do we manage risk at ABC?"

  "How do we manage risk at ABC?"

- Sections can cover:
  - Framework objective
  - Mandate & commitment
  - Risk appetite
  - Guiding principles
  - Roles & accountabilities
  - Applying the framework
  - Performance monitoring
  - Reporting
  - Quality & improvement
  - Committee charge

Incorporated Into Strategy, Operations & Decisions

- Three levels of risk to consider



Risk as Pillar of Governance

Governance

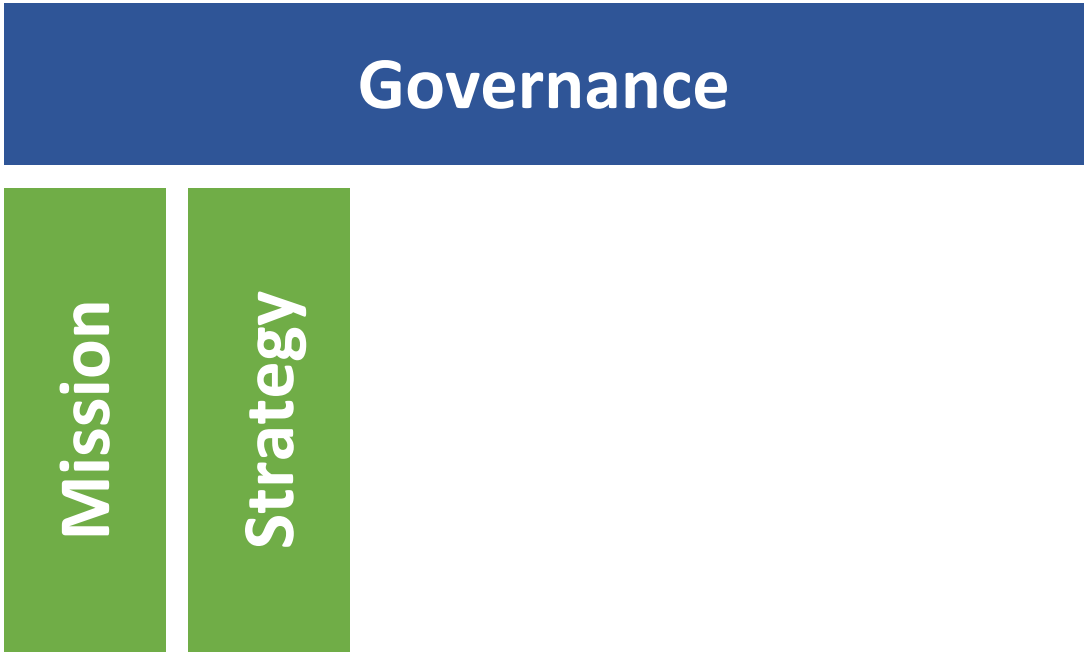
Risk as Pillar of Governance



Mission

The board sets the overall mission and objectives of the organization and insists that its culture and values are aligned with that mission.

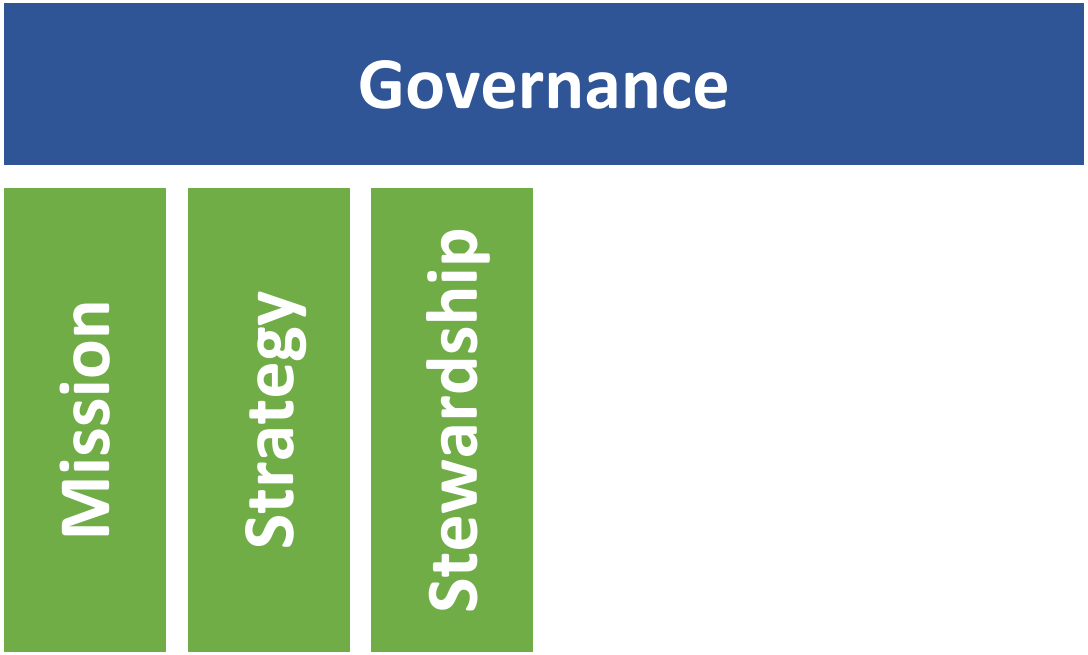
Risk as Pillar of Governance



Strategy

Senior leadership, in conjunction with the board, develop strategic plans to carry out the organization's mission and objectives.

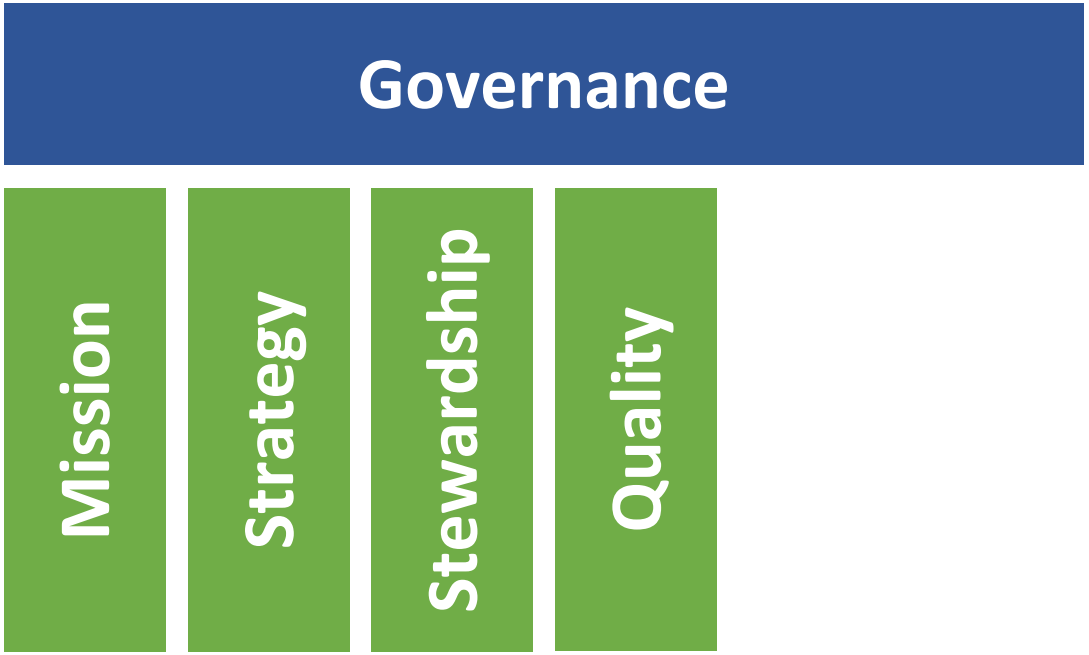
Risk as Pillar of Governance



Stewardship

Financial resources are developed and maintained to ensure the mission and strategic plans are adequately funded.

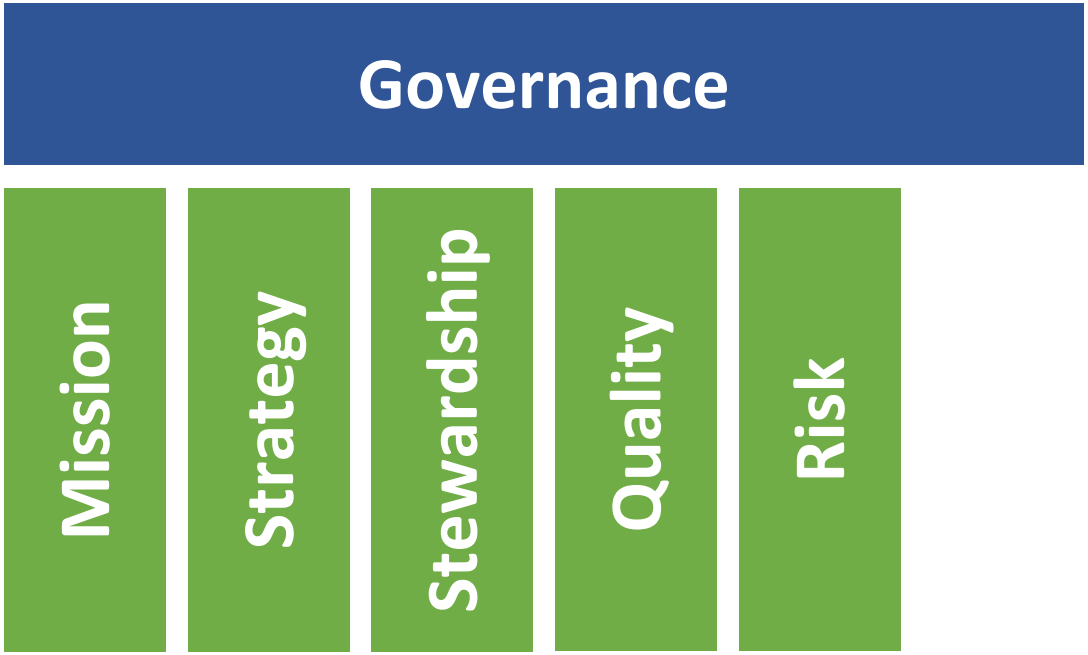
Risk as Pillar of Governance



Quality

The quality of the organization's programs are planned for and tested in order to maintain demand for the "product" in the long-term.

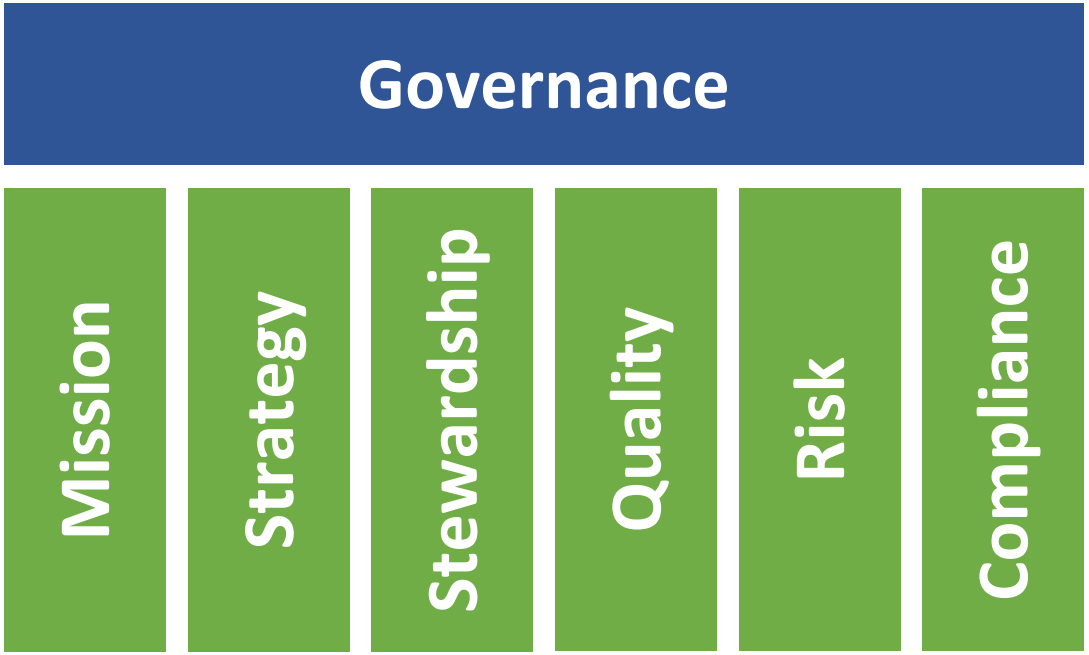
Risk as Pillar of Governance



Risk

Risks to the organization in meeting its organizational objectives, including threats and opportunities, are identified, assessed, and treated.

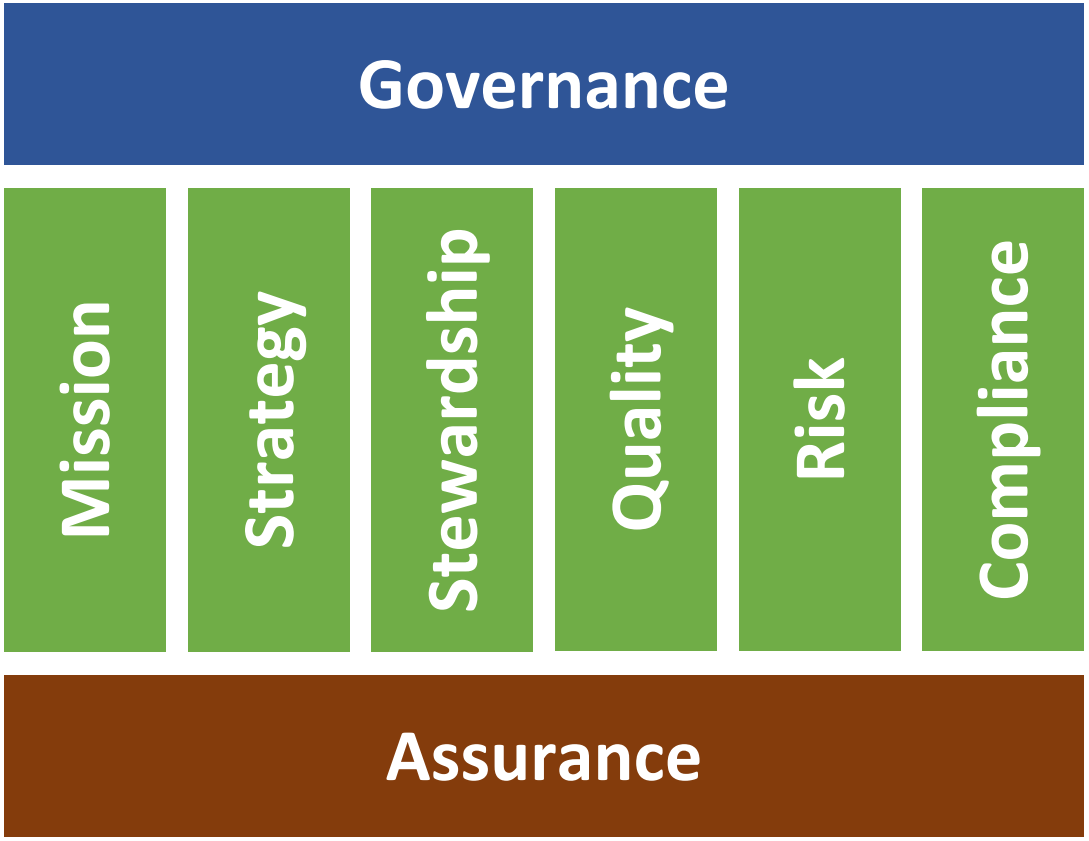
Risk as Pillar of Governance



Compliance

Risks to the organization for failing to comply with its legal, regulatory, industry, and internal standards are identified, assessed, and managed.

Risk as Pillar of Governance

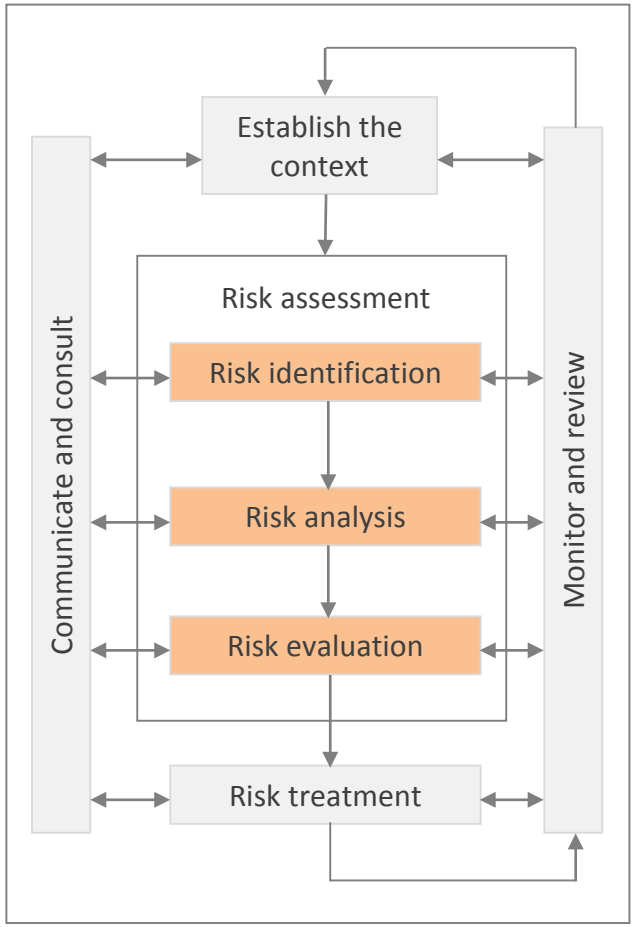


Assurance

A strong management structure and culture is maintained to ensure proper reporting and accountability, and internal and external audits are utilized to bring board assurance.

Performing a Risk Assessment

ISO 31000 RM Process



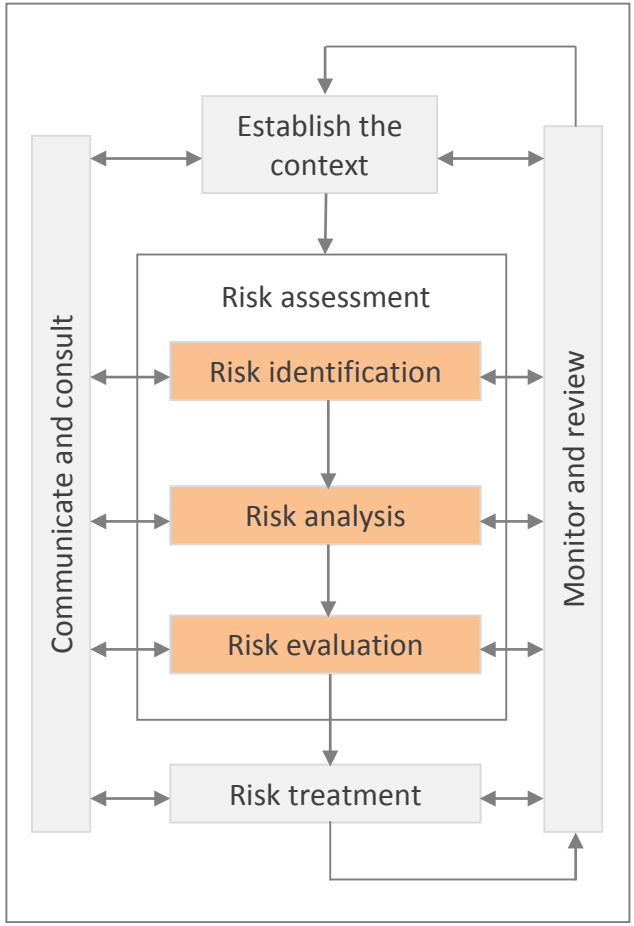
Risk Assessment Considerations

- What is the context of this risk assessment?
- Who should be there?
  - Senior leadership
  - Risk committee
  - Ad hoc team
  - Risk management
- Identification of internal and external stakeholders
- How precise to be
  - ISO 31000 details 31 risk assessment methods
  - But normally looking for reasonable consensus and “gut feel”
- Agree on risk criteria

Risk Assessment Process

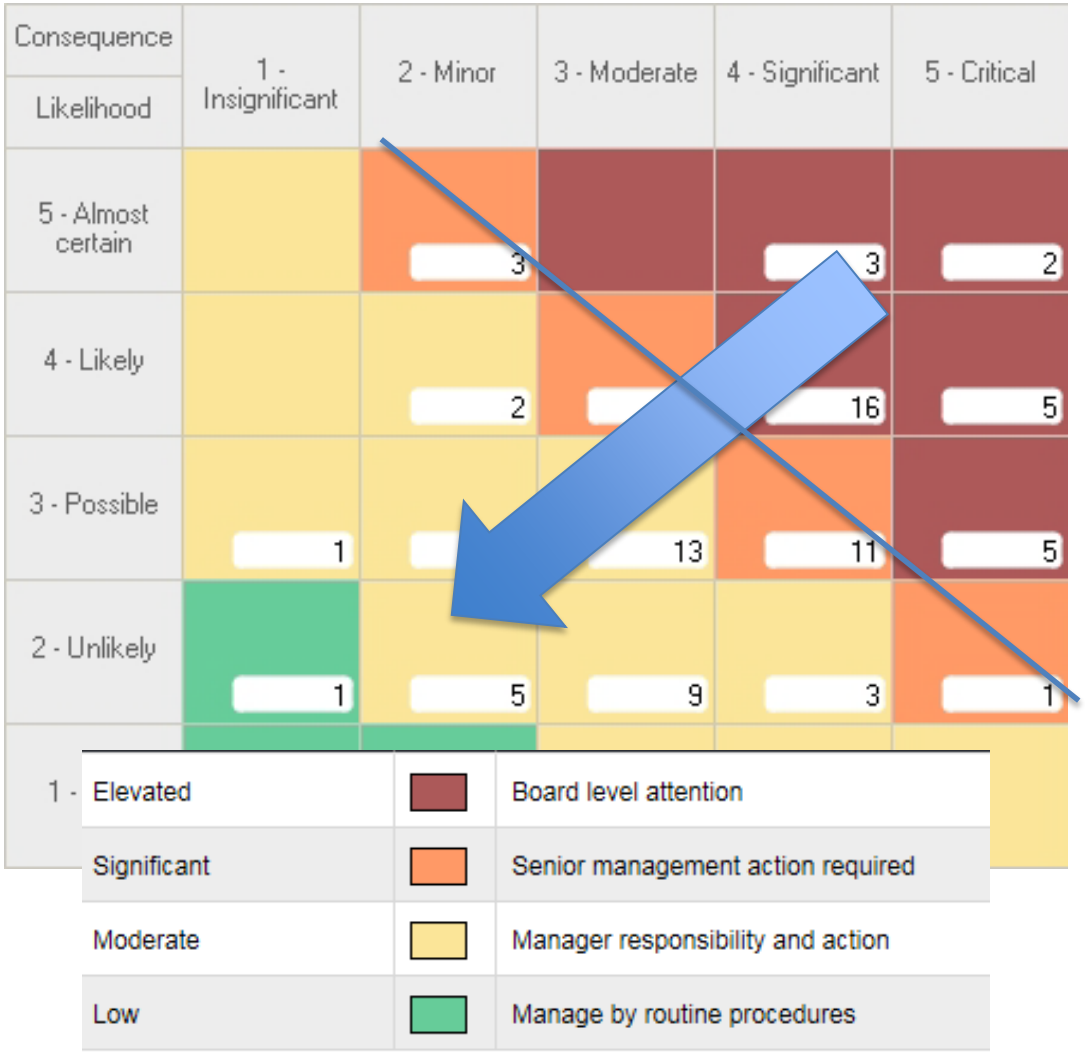
- Risk Identification
  - Risk register
  - Developed through:
    - Brainstorming
    - Interviews
    - Surveys
    - Other institutions
    - Associations
- Risk Analysis
  - Ranking based on likelihood and consequence (impact)
  - Use of heat maps
- Risk Evaluation
  - Prioritization

ISO 31000 RM Process



Risk (Heat) Maps

- Visual tool to plot likelihood and impact scores
  - Let's the viewer easily identify top risks
  - Highlights need for risk treatment and to drive risks from top right to bottom left
- A risk tolerance line can easily be drawn
- Excellent for senior leadership and Board presentations



Risk Assessments – Day Of

- Use of technology
  - Survey tools
  - Spreadsheet
- Have “placemat” ready
- Usually start with subject matter expert
  - Then rest of group agrees or challenges
- Can also agree on risk ownership at same time

Framework for Enterprise Risk Assessment

1. Risk management is a very important component of organizational governance alongside mission, strategy, stewardship, quality, and compliance.
2. Risks should always be tied to organizational mission and objectives
3. Rankings should be done from an organizational perspective and not just how it impacts a particular department or function
4. Keep the discussion at the strategic level
   - Operational risk assessments will normally follow
5. Rankings should be done considering the current state of controls and mitigation strategies in place
   - The next step will be to assign risk owners and develop risk treatment plans to reduce threats and increase opportunities, with reporting and accountability as key components
6. Likelihood is ranked first and then impact/consequence
   - The first question is, “What is the likelihood of the risk occurring?”
   - The second question is, “If the risk does occur, what is the impact to the organization?”
7. The ranking of risks will then flow into a discussion of prioritization
   - With the allocation of any needed resources being a key discussion point

Risk Criteria for Rankings

LIKELIHOOD

5–Almost certain	Event will normally occur at least on an annual basis (once a year or more frequently)
4–Likely	Event is likely to occur on a reasonably regular basis (once every 3 years)
3–Possible	Event may occur on occasion (once every 10 years)
2–Unlikely	Event is unlikely to occur in the foreseeable future (once every 30 years)
1–Rare	Event has occurred in the public sector, but is rare (once every 50 years)

IMPACT

5–Critical	Impact to the overall organization is at a critical stage and may last for years
4–Significant	Impact on the overall organization is significant and may last for several months
3–Moderate	Impact on the overall organization is moderate, but creates more serious disruption at depts
2–Minor	Impact on the overall organization is minor, but creates some disruption at depts
1–Insignificant	No measurable impact on the organization

What Happens After the Risk Assessment?

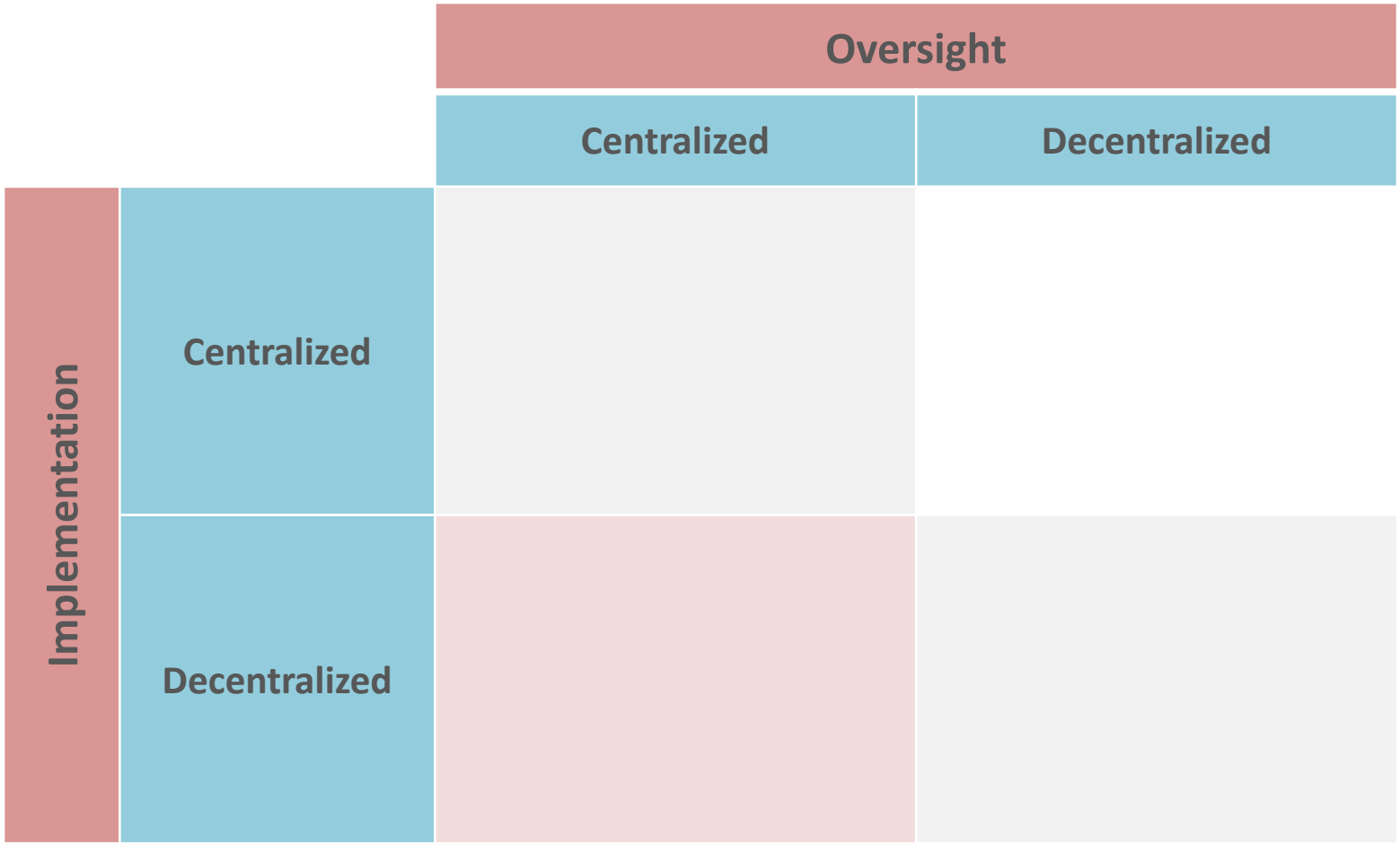
- Each risk turned over to owner
  - To draft risk treatment plan
  - To determine team needed
- Risk owners report back to leadership for approval of plan
  - Through committee
  - Through management structure
- Risk owners work their plans with accountability to central oversight
- Rerank risks as treatment plans are implemented
- Report to senior leadership, audit committee, and/or full board

Assigning Risk Ownership

Employment of “Ownership” Model is Critical

- Pushing work out to subject matter experts is essential to success
- Risk owners:
  - Develop risk treatment plans
  - Assemble work teams
  - Communicate and report
  - Monitor and evaluate
- At what level of the organization should ownership reside?

Central Oversight/Decentralized Implementation



Central Oversight/Decentralized Implementation

		Oversight	
		Centralized	**Decentralized**
Implementation	**Centralized**	Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise	
	Decentralized		

Central Oversight/Decentralized Implementation

		Oversight	
		Centralized	**Decentralized**
Implementation	**Centralized**	Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise	
	Decentralized		Where most organizations have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability

Central Oversight/Decentralized Implementation

		Oversight	
		Centralized	**Decentralized**
Implementation	**Centralized**	Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise	
	Decentralized	Oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk "ownership"	Where most organizations have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability

Reporting & Accountability Clearly Addressed



Data Management

Administrative Tools

- Spreadsheets
- Enterprise software
- Governance, Risk & Compliance (GRC) software
  - As part of RMIS
  - As stand-alone cloud system

Functions to look for:

- Detailed risk and compliance obligation registers with multiple data points
- Dashboards for each risk and obligation with the ability to rank risks and catalogue treatment plans
- Risk rankings that flow into interactive, institutional heat maps
- Ability to manage delegations using email assignments and workflow through calendars
- Reporting tools for use at all levels of the organization

Questions?