

# MABE

The logo graphic consists of two overlapping parallelograms. The top one is red and the bottom one is yellow, both pointing towards the right.

MARYLAND ASSOCIATION OF BOARDS OF EDUCATION

---

## RISK MANAGEMENT

**MD PRIMA - VIRTUAL MEETING**

JOHN MAGOON – [JMAGOON@MABE.ORG](mailto:JMAGOON@MABE.ORG)


- **“Nothin to it, but to do it”**
- From “Flossy” while hiking the [Northfield-Placid trail](#) on [“Trail Tales”](#)

# TELL THEM WHAT YOU'RE GOING TO TELL THEM

- Share my experiences with Risk Management and Business Continuity
- Encourage you to:
  - Perform a Gap Analysis of your ERM Program
  - Use standards related to your RM Program
  - Work with other departments within your organization

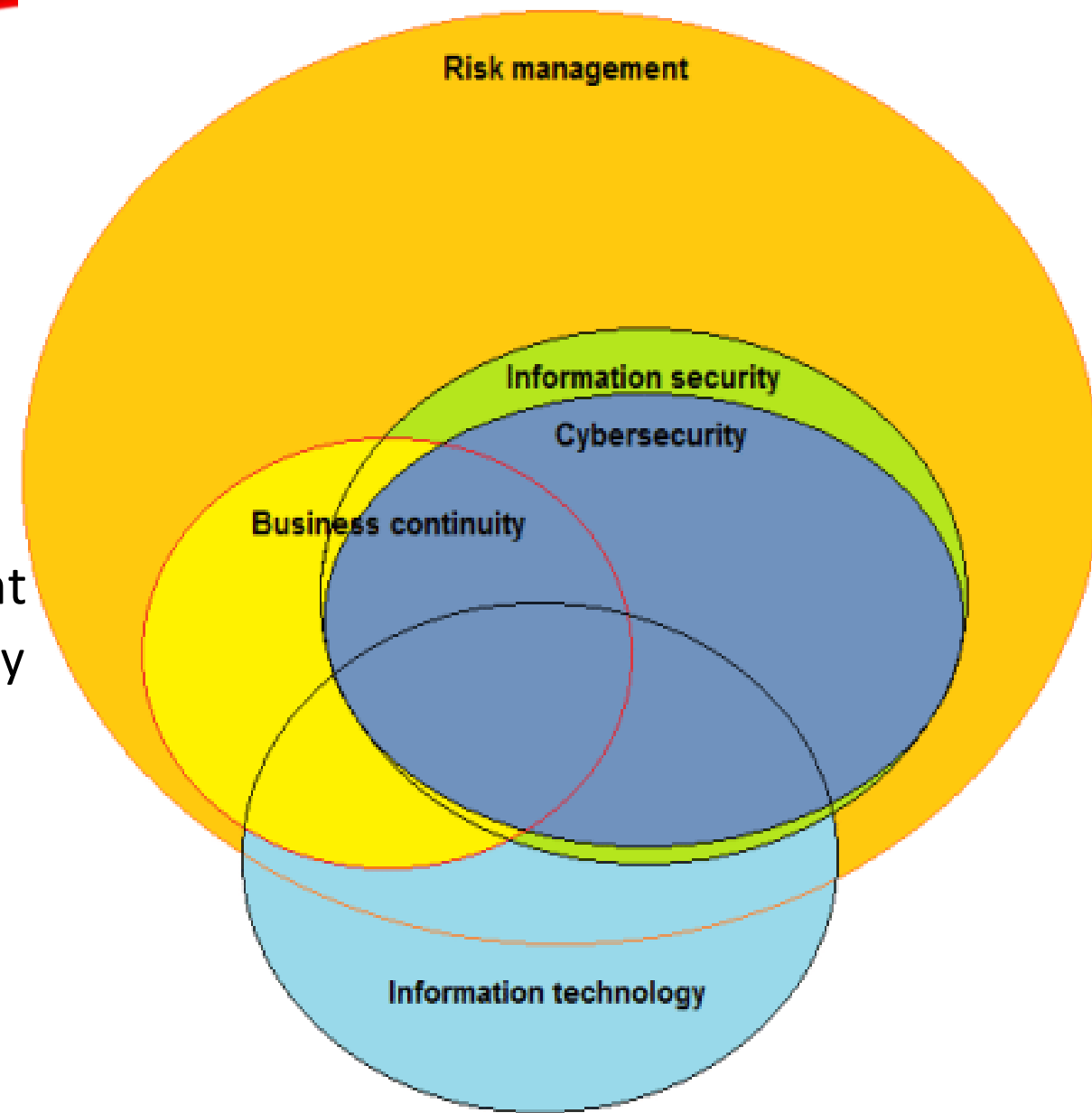
slido

In a given week, what do you spend most of your time on?  
(Enter as many words as you like)

 Start presenting to display the poll results on this slide.

## Overlap between standards –

- **ISO 31000** – Risk Management
- **ISO 27001** – Information Security Management
  - **NIST 800 – 39** – Managing Information Security Risk
- **ISO 22301** – Security and Resilience (Business Continuity)
- **ISO 45001** – Occupational Health and Safety
- **ISO 9001** – Quality Management



# PROGRESSION OF RISK MANAGEMENT

- 1987 – ISO 9001\* – Quality Control Standard, promotes TQM, Defines Risk
- 1992 - COSO Internal Control – Addresses risk and introduces Integrated Framework
- 2004 - COSO ERM, Integrated Framework – (as an answer to Sarbanes Oxley)
- 2004 - RIMS publishes first Risk Maturity Model
- 2009 - ISO 31000 – Risk Management, based largely on AS/NZS 4360:2004.
- 2012 – ISO 22301\* - Security and resilience – Business continuity management systems
- 2014 - PRIMA began their ERM Series?
- 2016 - OMB revised Circular No. A-123, Managements Responsibility for Internal Control.

<https://patimes.org/enterprise-risk-management-public-sector/>

[https://obamawhitehouse.archives.gov/omb/circulars\\_a123\\_rev/](https://obamawhitehouse.archives.gov/omb/circulars_a123_rev/)

<https://www2.deloitte.com/us/en/pages/public-sector/solutions/tackling-enterprise-risk-management-in-government.html>

<https://www.pwc.se/sv/pdf-reports/enterprise-risk-management-in-the-public-sector.pdf>

\*Certificate/Auditable



# BUSINESS CONTINUITY/CONTINUITY OF OPERATIONS BASICS

You need:

- Access to Acceptable Hardware
- Licensed Software
- Access to your Data
- Access to Vital Records
- The ability to Communicate (Internet, phone, email, SMS)
- Essential Staff ( ideally three deep)
- A Command System – (ICS)
- A Physical Location to do business
- To Base decisions on your RPO and RTO

## Business Continuity Management

*BCM* is a holistic management process that is used to ensure that operations continue, and that products and services are delivered at predefined levels, that brands and value-creating activities are protected, and that the reputations and interests of key stakeholders are safeguarded whenever disruptive incidents occur. This is achieved by identifying potential threats, by analyzing possible impacts, and by taking steps to build organizational resilience.

([Praxiom](https://www.praxiom.com/) – ISO 22301)

## Enterprise Risk Management

ERM is a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. (COSO ERM – Integrated Framework – 2004)

<https://www.praxiom.com/> - ISO Definitions

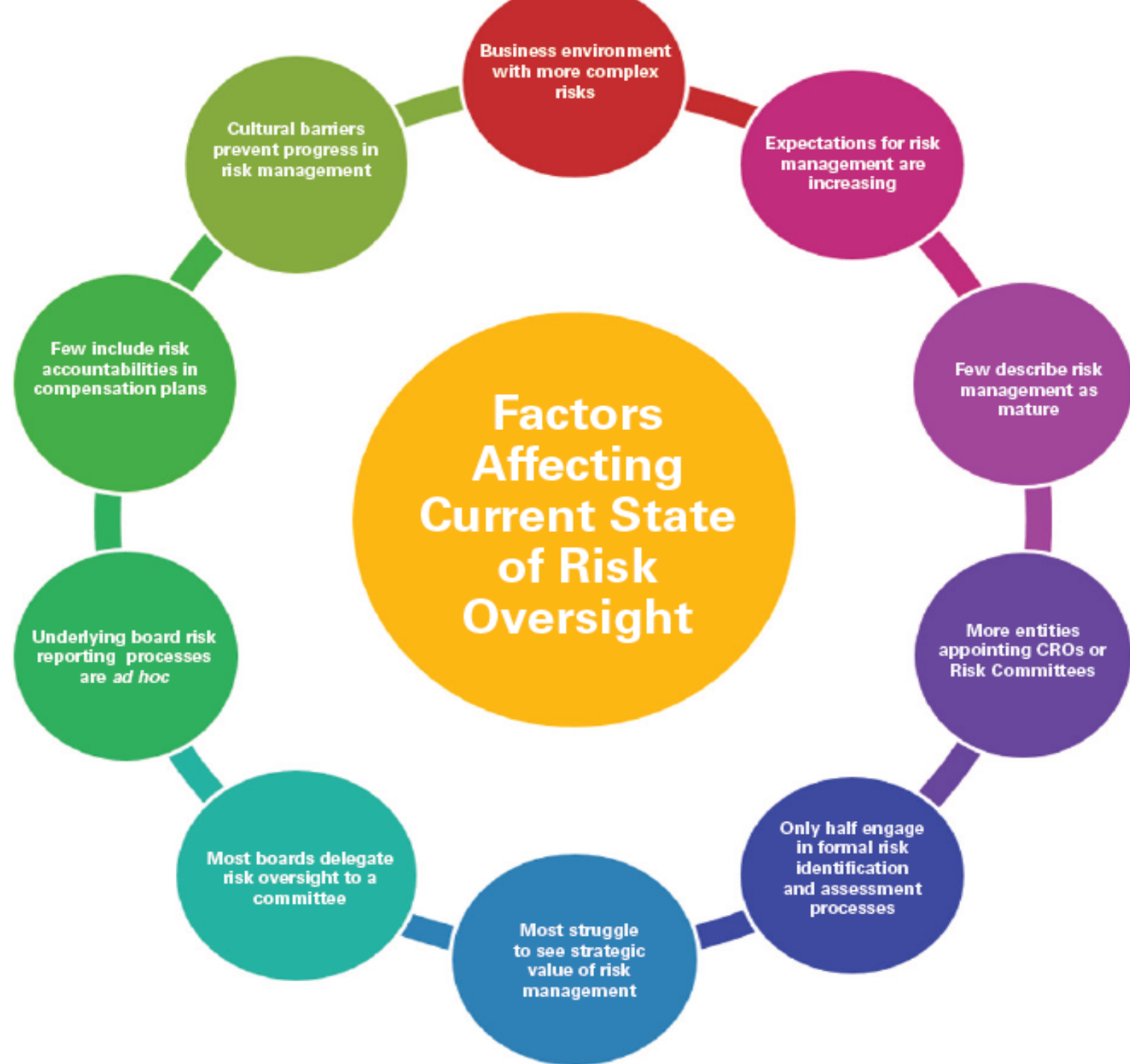
<https://drii.org/resources/viewglossary> - DRii Glossary



# NC STATE UNIVERSITY ERM INITIATIVE

- Published the 11<sup>th</sup> annual “State of Risk Oversight Report” in April of 2020

[WWW.ERM.NCSU.EDU](http://WWW.ERM.NCSU.EDU)



# FRAMEWORKS

12

- A RECENT POST TO THE ASSOCIATION OF SCHOOL BUSINESS OFFICIALS

*Good morning!*

*I have been asked to put together an RFP to look for expertise to help us put together a risk management framework. Has anyone put together a similar RFP that they would be willing to share with us?*

-----

*Reta Morgan*

*CFO\Secretary Treasurer*


*Foundations for the Future Charter Academy*

*[reta.morgan@ffca-calgary.com](mailto:reta.morgan@ffca-calgary.com)*

*Calgary, Alberta, Canada*



# Do you have a Formal Risk Management Framework?

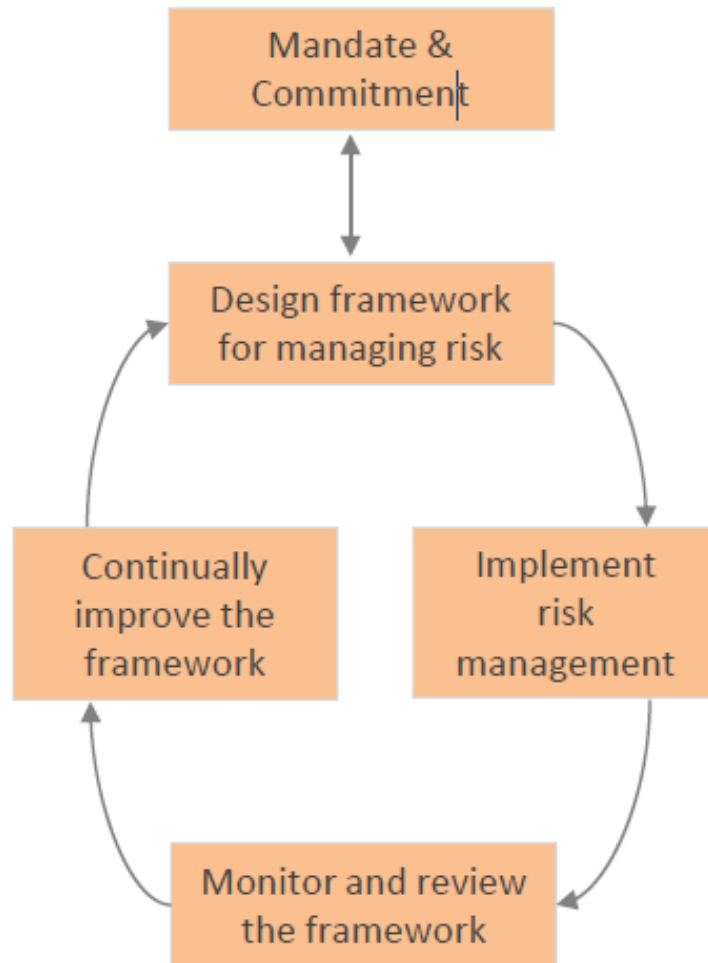
 Start presenting to display the poll results on this slide.

# ISO 31000 Risk Management Model

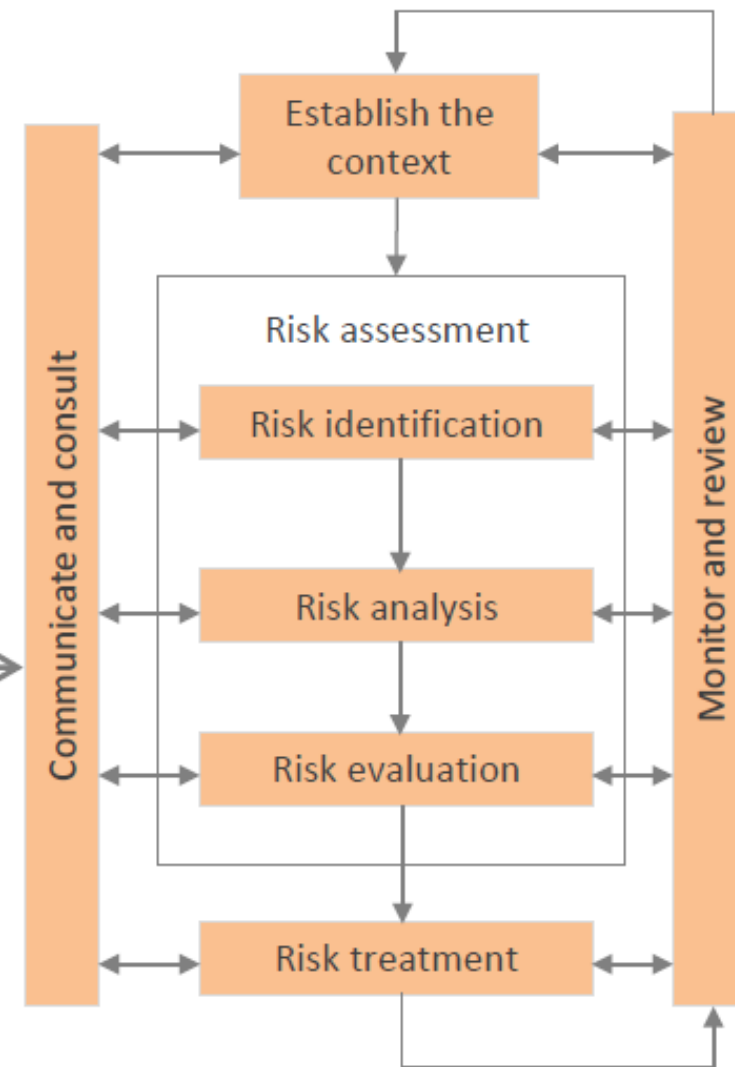
## Principles

- 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

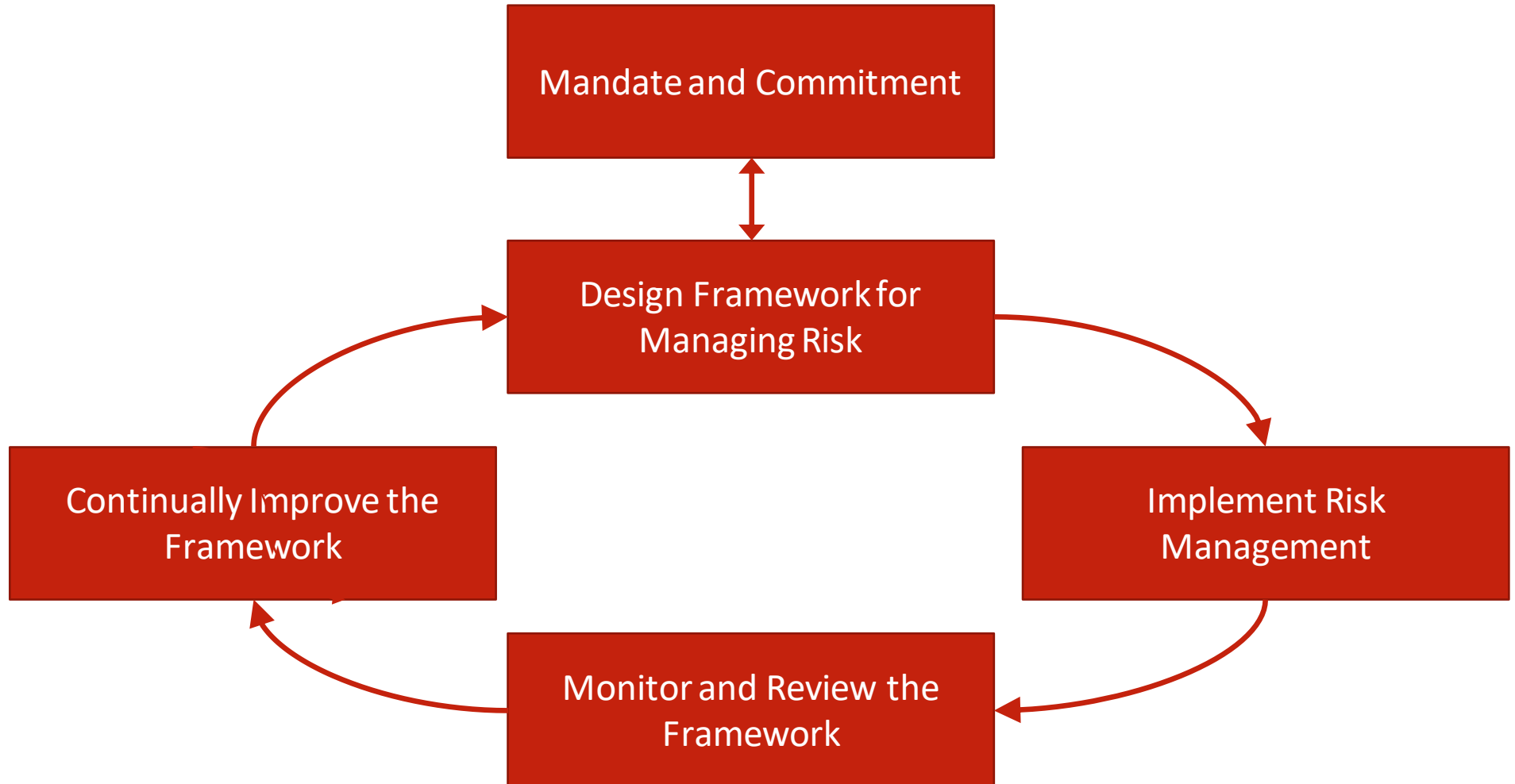
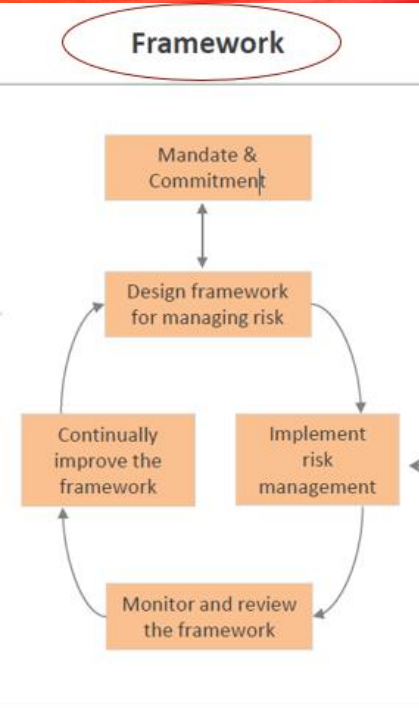


## Process



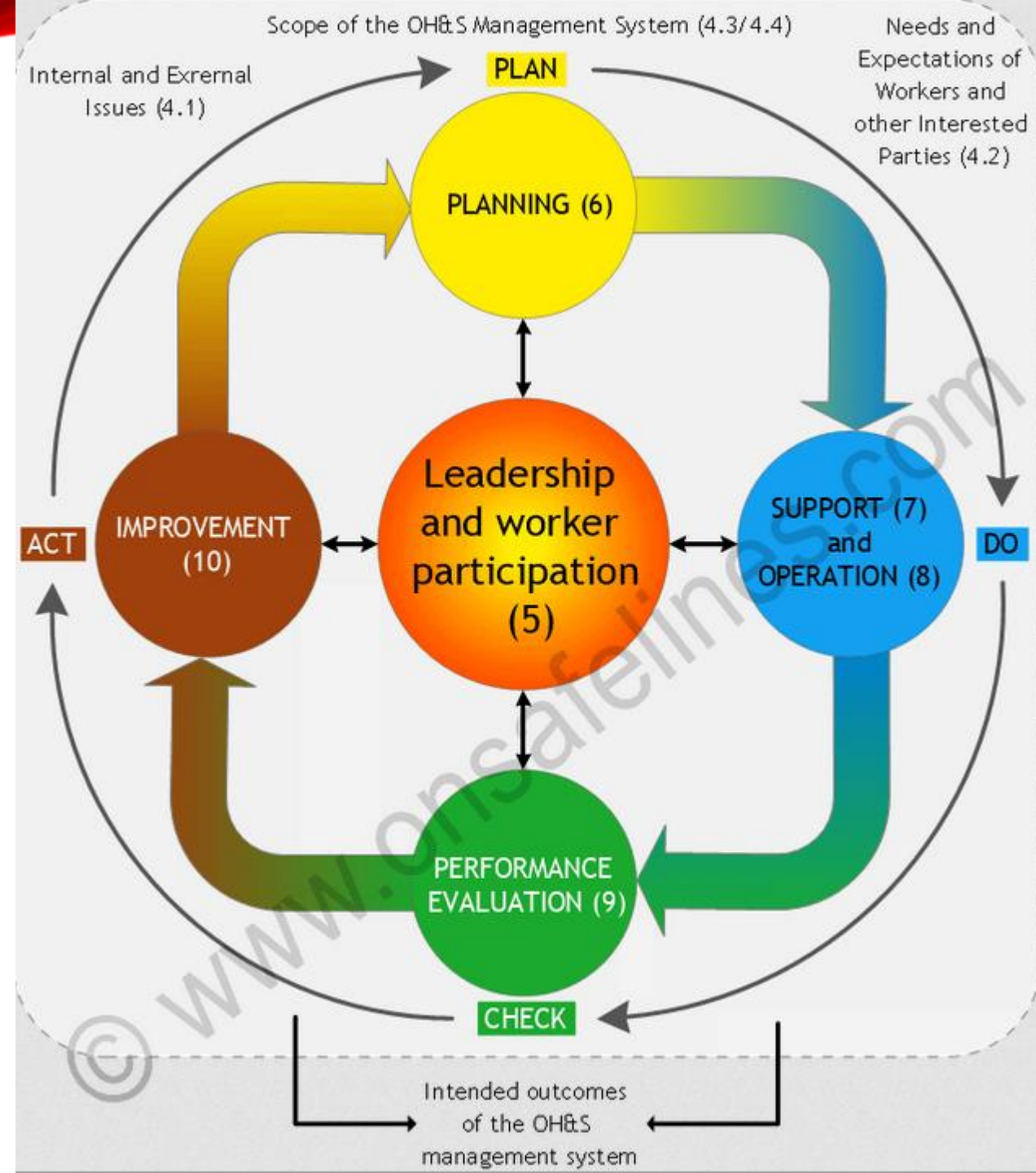
# RISK MANAGEMENT FRAMEWORK

## Framework





- ISO 45001 - Occupational Health & Safety Management System





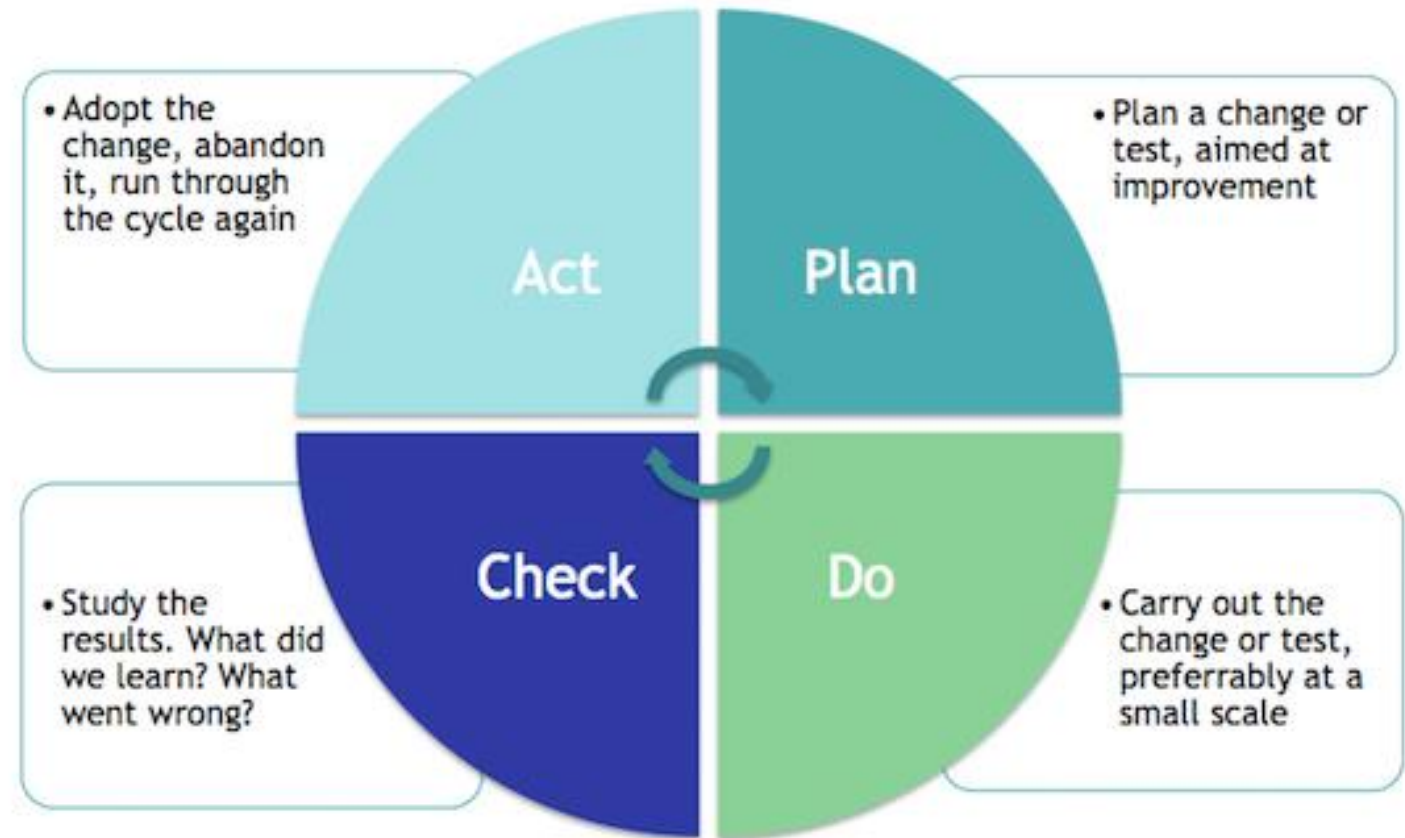
# Content of ISO 22301

Introduction	5 Leadership	8 Operation
0.1 General	5.1 General	8.1 Operational planning and control
0.2 The Plan-Do-Check-Act (PDCA) model	5.2 Management commitment	8.2 Business impact analysis and risk assessment
0.3 Components of PDCA in this International Standard	5.3 Policy	8.3 Business continuity strategy
1 Scope	5.4 Organizational roles, responsibilities and authorities	8.4 Establish and implement business continuity procedures
2 Normative references	6 Planning	8.5 Exercising and testing
3 Terms and definitions	6.1 Actions to address risks and opportunities	9 Performance evaluation
4 Context of the organization	6.2 Business continuity objectives and plans to achieve them	9.1 Monitoring, measurement, analysis and evaluation
4.1 Understanding of the organization and its context	7 Support	9.2 Internal audit
4.2 Understanding the needs and expectations of interested parties	7.1 Resources	9.3 Management review
4.3 Determining the scope of the management system	7.2 Competence	10 Improvement
4.4 Business continuity management system	7.3 Awareness	10.1 Nonconformity and corrective action

# Information security and PDCA (Plan-Do-Check-Act)

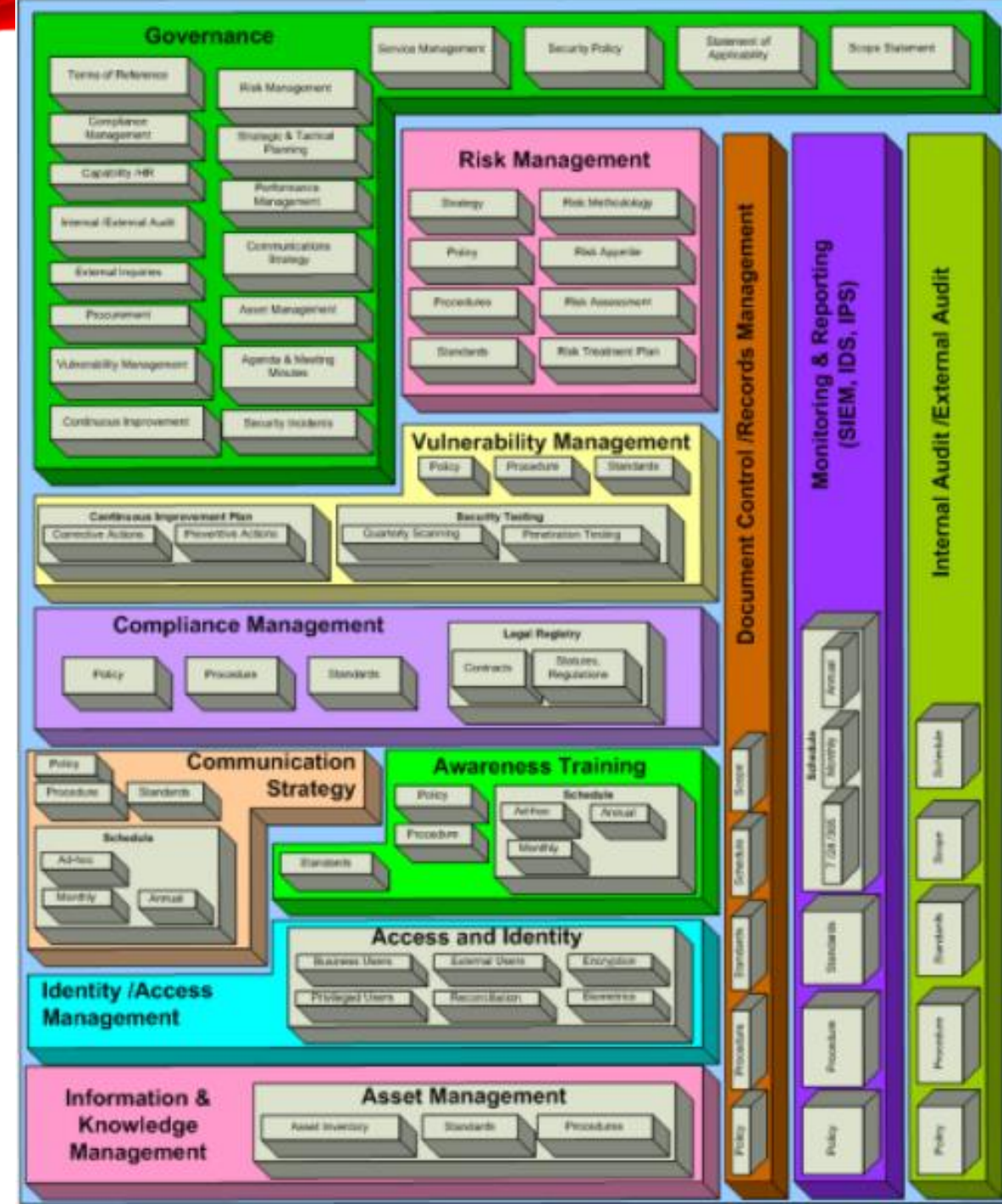
8 February 2017 | [Sieuwert van Otterloo](#) | Security

- **ISO 27001** - Information Security Management



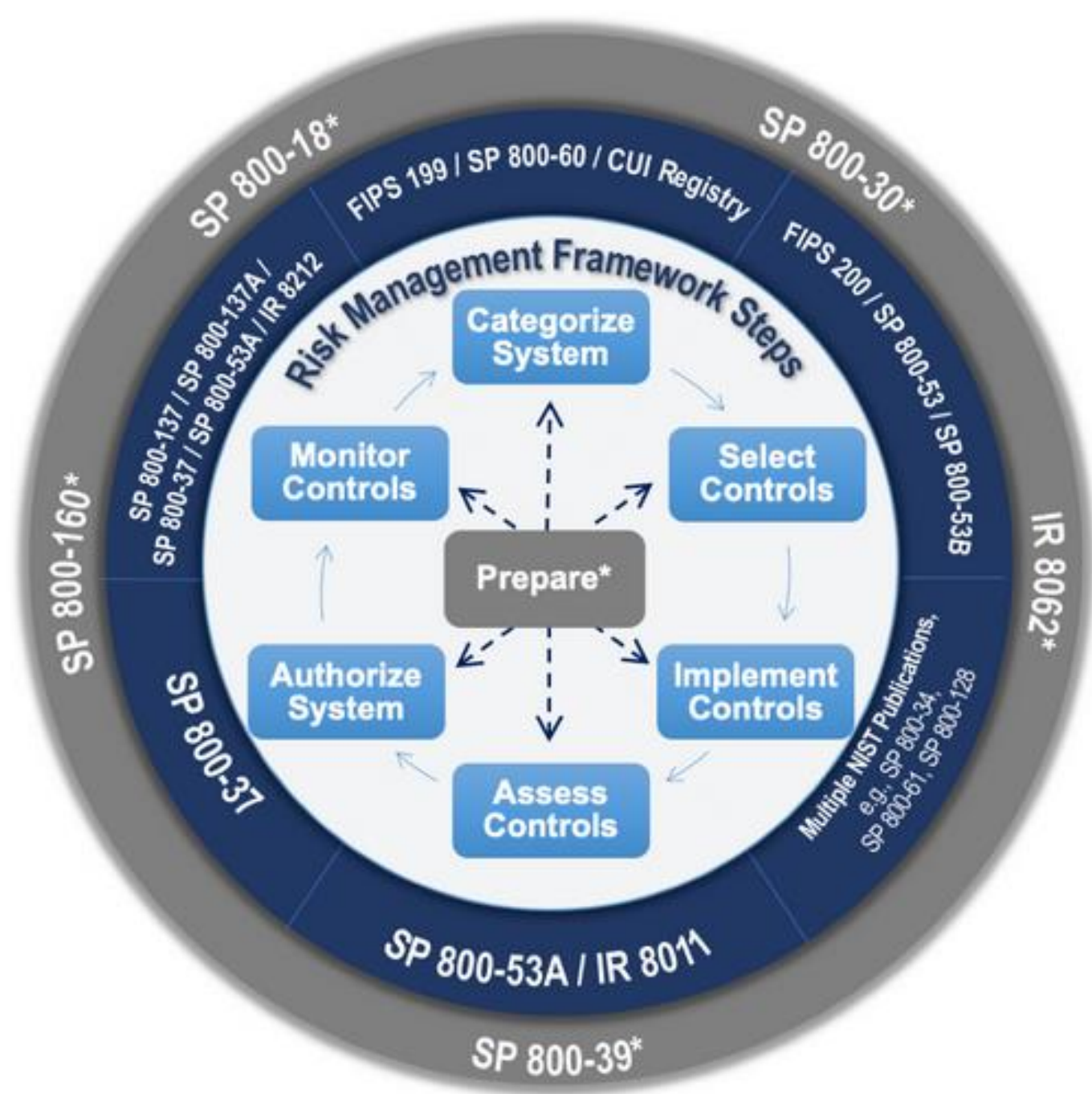
# ISO 27001 FRAMEWORK

- ISO 27001 includes Risk Management –
  - Strategy
  - Policy – Procedures
  - Standards
  - Risk Methodology
  - Appetite
  - Risk Assessment and Risk Treatment (Accept and Control, Avoid, Transfer contractually or Financially)





- **NIST 800 Series** - Has a Risk Management Framework designed for Cybersecurity and to support its IT Standards –
- <https://csrc.nist.gov/projects/risk-management/rmf-overview>



slido

State of ERM currently in place?

 Start presenting to display the poll results on this slide.

# ERM BABY STEPS

1. Make it about the Mission.
2. Create an Executive Risk Management Committee (Is there support?).
3. Agree on Terminology/Common Terms.
4. Implement the PDCA Cycle for ISO 31000.
5. Use ISO 31000 Clause 6 (Process) to Make Risk Informed Decisions.
6. Identify 3 or 4 Primary Risks to Address.
7. Identify several KPI's that support your Mission, and Continually Improve Upon them.
8. Consider TCOR – Total Cost of Risk = Retained Losses + Insurance Premiums + Risk Management Budget + Contracted RM Services (You can also capture Indirect cost of Losses, but more difficult to consistently calculate).



# THE VALUE OF MEASURING

- “Nothing Moves Unless its Pushed”
- “Nothing Moves Unless its Measured”



Before

We don't Know what we know <i>(Unknown Known)</i>	We Know what we know <i>(Known Known)</i>
We don't Know what we don't know <i>(Unknown Unknown)</i>	We Know what we don't know <i>(Known Unknown)</i>

Unknown ← → Known

After

We don't Know what we know	We Know what we know
We don't Know what we don't know	We Know what we don't know

Unknown ← → Known

More Data

Less Data

# MSDE's Proposed Dashboard/Scorecard

## PPE for the General Classroom

% schools with masks available for teachers and students

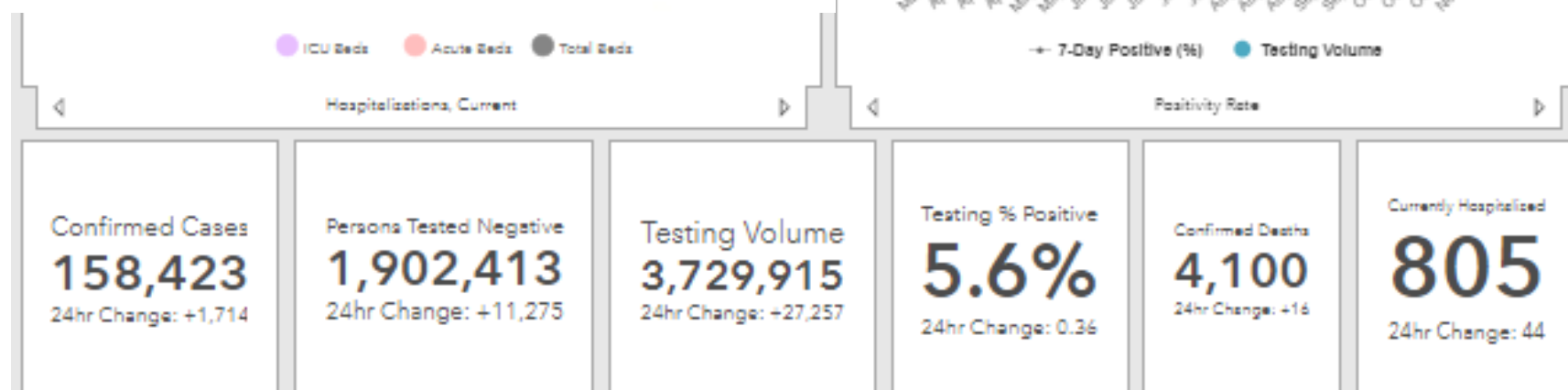
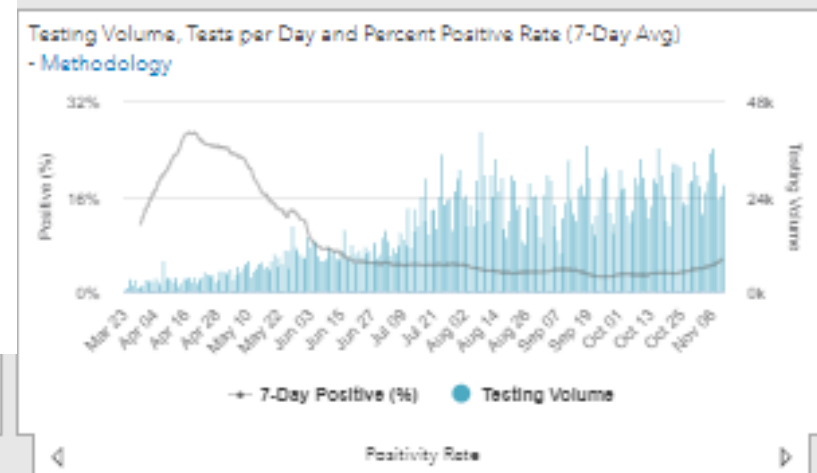
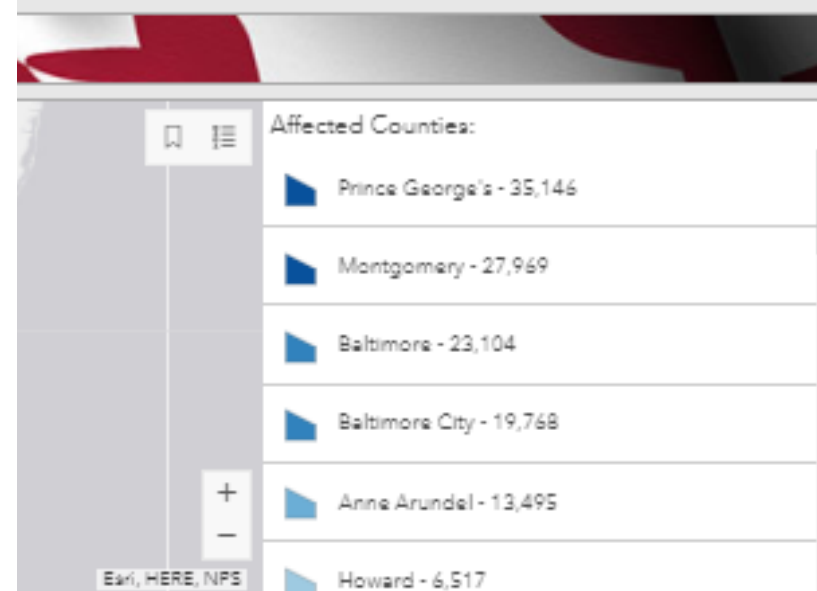
Green 95%; Yellow 80-94%; Red <80%

% schools with gloves available for each classroom

Green 95%; Yellow 80-94%; Red <80%

% schools with hand sanitizer available for each classroom

Green 95%; Yellow 80-94%; Red <80%







# RISK IDENTIFICATION AND ASSESSMENT EXERCISE

		RISK MANAGEMENT RISK ASSESSMENT FORM								
		THREATS	APPLICABILITY	PROBABILITY	THREAT FACTOR (sum plus 1)			IMPACT	WEIGHT	
		Natural	Applicable	Low = 1	Forewarning	Speed of Onset	Duration	Total	Low = 1	Prob.x
		Human	Not Applicable	Medium = 2	Yes = 0	Slow = 0	Short = 0	Threat	Medium = 2	TTF x
		Technical	Not Studied	High = 3	None = 1	Fast = 1	Long = 1	Factor	High = 3	Imp.
TYPE		THREATS	APPLICABILITY	PROBABILITY	Forewarning	Speed of Onset	Duration	Total	IMPACT	WEIGHT
HUMAN		Theft of Data		3	1	1	1	4	3	36
TECHNICAL		External Power Outage		3	1	1	0	3	3	27
HUMAN		Arson		2	1	1	1	4	3	24
TECHNICAL		Fire - Internal, Major		2	1	1	1	4	3	24
NATURAL		Pandemic		3	0	0	1	2	3	18
TECHNICAL		HVAC Failure		3	1	1	0	3	2	18
NATURAL		Snow Storm		3	0	0	1	2	3	18
NATURAL		Hurricane		3	0	0	1	2	3	18
HUMAN		Medical Emergency		3	1	1	0	3	2	18
HUMAN		Human Error, Maintenance		2	1	1	0	3	3	18
NATURAL		Public Water Supply Failure		2	1	1	1	4	2	16
TECHNICAL		Fire - Internal , Minor		2	1	1	0	3	2	12
TECHNICAL		Water Leak, Plumbing		2	1	1	0	3	2	12
TECHNICAL		Media Failure		2	1	1	0	3	2	12
TECHNICAL		Purchased Software Failure		1	1	1	1	4	3	12
TECHNICAL		Main Computer Failure		1	1	1	1	4	3	12
HUMAN		Loss of Key Staff		1	1	1	1	4	3	12
TECHNICAL		Electrical Power Surge		2	1	1	0	3	2	12
TECHNICAL		Telecommunications Failure		2	1	1	0	3	2	12
TECHNICAL		Internal Power Outage		2	1	1	0	3	2	12
NATURAL		Ice Storm		2	0	0	1	2	3	12
HUMAN		Bombing		1	1	1	1	4	3	12
HUMAN		Aircraft Crash		1	1	1	1	4	3	12
HUMAN		Cybersecurity Internal		1	1	1	1	4	2	8

						1	2	3	4	5	
						Insignificant	Negligible	Moderate	Extensive	Significant	
Likelihood	↑	Is expected to occur in most circumstances	>95%	Has occurred 9 or 10 times in the past 10 years in this organization or circumstances are in train that will almost certainly cause it to happen	E	Almost Certain	6	7	8	9	10
		Will probably occur in most circumstances	>65%	Occurred more than 7 times over 10 years in this organization or in other similar organizations or circumstances have such that it is likely to happen in the next few years	D	Likely	5	6	7	8	9
		Might occur at some time	>35%	Has occurred in this organization more than 3 times in the past 10 years or occurs regularly in similar organizations or is considered to have a reasonable likelihood of	C	Possible	4	5			
	↑	Could occur at some time	<35%	Has occurred 2 or 3 times over 10 years in this organization or similar organizations	B	Unlikely	3		5	6	7
	↑	May occur only in exceptional circumstances	<5%	Has occurred or can reasonably be considered to occur only a few times in 100 years.	A	Rare	2	3	4	5	6

FEMA Has their own Resources and Guides:

<https://www.fema.gov/emergency-managers/national-preparedness/continuity>

[https://www.fema.gov/sites/default/files/2020-07/Continuity-Assessment-Tool\\_020518.xlsx](https://www.fema.gov/sites/default/files/2020-07/Continuity-Assessment-Tool_020518.xlsx)

Consequence					
<b>People</b>	Minor injury or first aid treatment	Injury requiring treatment by medical practitioner and/or lost time from workplace.	Major injury / hospitalization	Single death and/or multiple major injuries	Multiple deaths
<b>Information</b>	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to the organizations operations.	Compromise of information sensitive to organizational interests.	Compromise of information with significant ongoing impact.
<b>Property</b>	Minor damage or vandalism to asset.	Minor damage or loss of <5% of total assets	Damage or loss of <20% of total assets	Extensive damage or loss <50% of total assets	Destruction or complete loss of >50% of assets
<b>Economic</b>	1% of budget (organizational, division or project budget as relevant)	2-5% of annual budget	5-10 % of annual budget	> 10% of budget	> 30% of project or organizational annual budget
<b>Reputation</b>	Local mention only. Quickly forgotten. Freedom to operate unaffected. Self-improvement review required	Scrutiny by Executive, internal committees or internal audit to prevent escalation Short term local media concern. Some impact on local level activities	Persistent national concern. Scrutiny required by external agencies. Long term 'brand' impact.	Persistent intense national public, political and media scrutiny. Long term 'brand' impact. Major operations severely restricted.	International concern. Governmental Inquiry or sustained adverse national/international media. 'Brand' significantly affects organizational abilities.
<b>Capability</b>	Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations.	Some impact on organizational capability in terms of delays, systems quality but able to be dealt with at operational level	Impact on the organization resulting in reduced performance such that targets are not met. Organizations existence is not threatened, but could be subject to significant review	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches).	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organization is threatened.

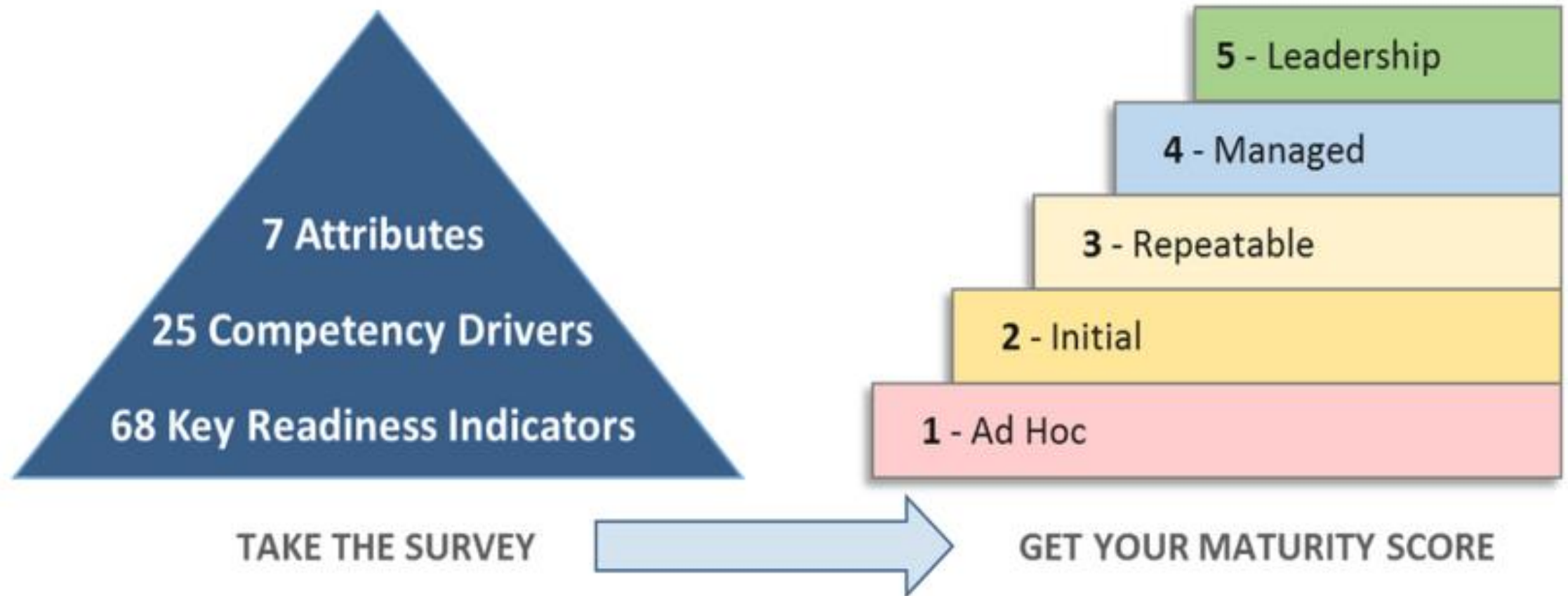


# RIMS RISK MATURITY MODEL

1. Adoption of ERM-Based Process
  2. ERM Process Management
  3. Risk appetite Management
  4. Root Cause Discipline
  5. Uncovering Risks
  6. Performance Management
  7. Business Resiliency and Sustainability
- These 7 Attributes are measured against 25 Competencies and their 68 Readiness Indicators on a scale of 1-10. It will define your Program into one of the following:
    - Ad-Hoc – Initial – Repeatable – Managed - Leadership

<https://www.rims.org/resources/strategic-enterprise-risk-center/risk-maturity-model>

# RIMS RISK MATURITY MODEL



# AON RISK MATURITY INDEX

1. Board-level commitment
2. Executive Leadership
3. Transparent risk communication
4. A culture of risk ownership
5. Data and analytics
6. Stakeholder participation
7. Risk-based decision making
8. Risk quantification
9. Optimized risk profile

<https://www.aon.com/risk-maturity-index>

# TELL THEM WHAT YOU TOLD THEM

- Share my experiences with Risk Management and Business Continuity
- Encourage you to:
  - Perform a Gap Analysis of your ERM Program
  - Use standards related to your RM Program
  - Work with other departments within your organization

JOHN MAGOON,  
RISK MANAGEMENT OFFICER,  
MARYLAND ASSOCIATION OF BOARDS OF  
EDUCATION

[JMAGOON@MABE.ORG](mailto:JMAGOON@MABE.ORG)

443-603-0399

- Also from Flossy - Not only is there...

**“Nothin to it, but to do it”** but **“You gotta Risk it to get the Biscuit!”**

COMMENTS? - QUESTIONS? - FEEDBACK?