Risk Management and Resilience: Building the Bridge to Business Continuance

Michele L. Turner MBCP, FBCI, CISA, CRISC, GRCP
DRI- Foundation Director and Instructor

AGENDA

❏ Background
- ❏ DRI Summary
- ❏ Presenter Summary

❏ Setting the Stage- Related Terms and Definitions

❏ Vehicle Diagnostics (The Facts)

❏ Rules of the Road (Tactical and Strategic Roles and Responsibilities)

❏ Maintenance Schedule (Governance, Risk and Compliance)

❏ Critical Fix towards Resiliency (Operational Risk- Business Continuity)

❏ Bridge to Wellness and Key Takeaways

Who we are

- We provide education, accreditation, and thought leadership in business continuity and related fields.
- Founded in 1988, we are the oldest and largest organization of our kind.

What we do

- We offer in-depth courses ranging from introductory to masters level, as well as specialty certifications.

15,000+
Certified Professionals

Certified Professionals in
100+
Countries

ANSI
ANSI ACCREDITED PROGRAM
CERTIFICATE ISSUER

Classes
offered in
14
Languages

Courses
held in
50
Countries

CQI | IRCA
APPROVED TRAINING PARTNER

BAEM
Conference
Bay Area's Emergency Managers

Renaissance Nashville Hotel • February 11–14, 2018

DRI•2018
The Professional's Conference

join us
Nashville

"As the certified professionals conference, you know the folks you'll be interacting with, that you'll be networking with, come with a level of experience, a level of expertise, and a level of education that are on par with a certified professional."
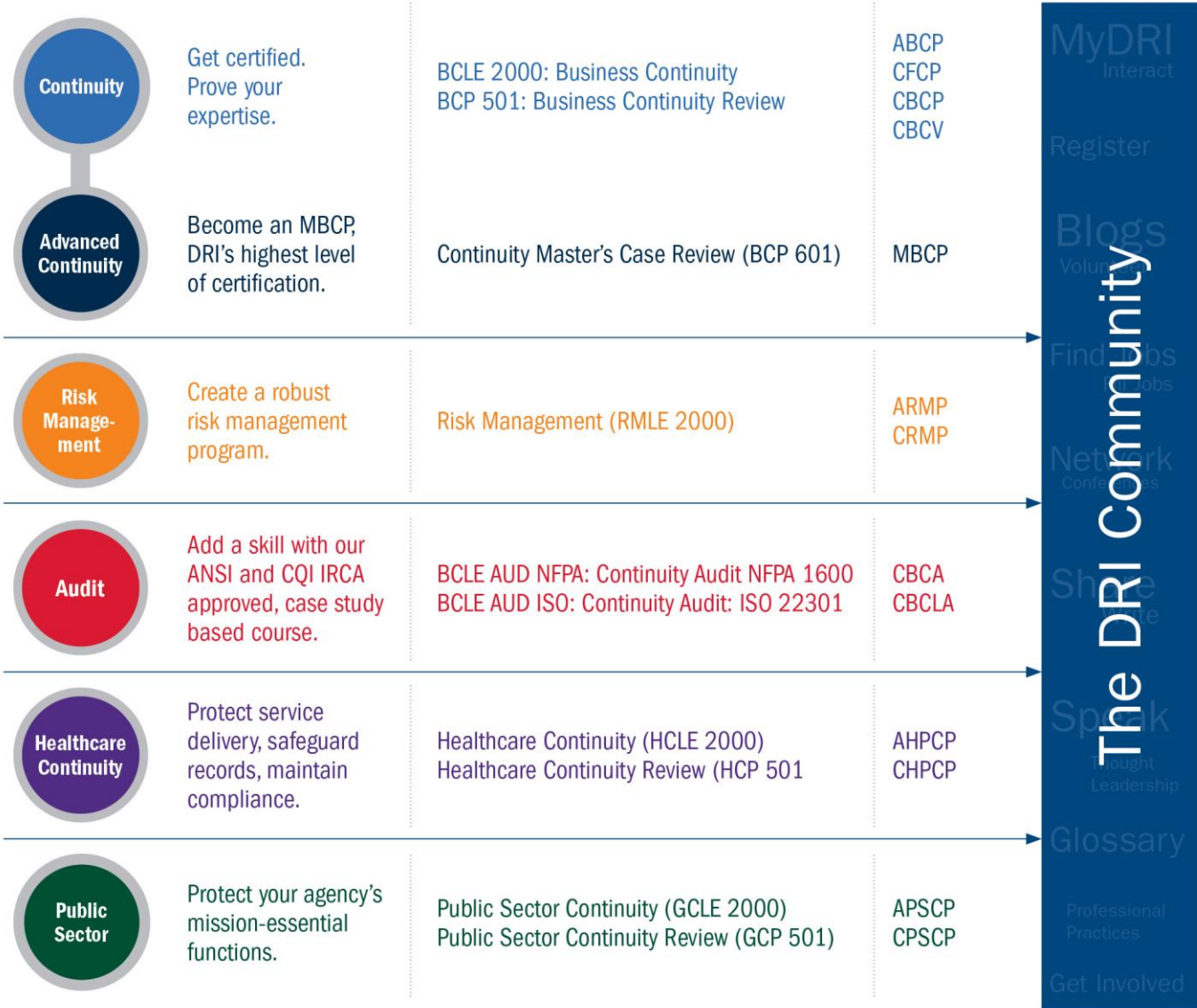
www.driconference.org

Bay Area Emergency Managers Conference 2017
Genentech Event Center, South San Francisco, CA

BAEM
Bay Area's Emergency Managers
Conference

Career tracks

Track	Description	Courses	Certifications
Continuity	Get certified. Prove your expertise.	BCLE 2000: Business Continuity BCP 501: Business Continuity Review	ABCP CFCP CBCP CBCV
Advanced Continuity	Become an MBCP, DRI's highest level of certification.	Continuity Master's Case Review (BCP 601)	MBCP
Risk Management	Create a robust risk management program.	Risk Management (RMLE 2000)	ARMP CRMP
Audit	Add a skill with our ANSI and CQI IRCA approved, case study based course.	BCLE AUD NFPA: Continuity Audit NFPA 1600 BCLE AUD ISO: Continuity Audit: ISO 22301	CBCA CBCLA
Healthcare Continuity	Protect service delivery, safeguard records, maintain compliance.	Healthcare Continuity (HCLE 2000) Healthcare Continuity Review (HCP 501	AHPCP CHPCP
Public Sector	Protect your agency's mission-essential functions.	Public Sector Continuity (GCLE 2000) Public Sector Continuity Review (GCP 501)	APSCP CPSCP

The DRI Community

MyDRI Interact
Register
Blogs Volunteer
Find Jobs Jobs
Network Conferences
Share Donate
Speak Thought Leadership
Glossary
Professional Practices
Get Involved

CBCV Certification

Show your **customers** that you speak their **language**

Become a Certified Business Continuity Vendor (CBCV)

- Created for vendors who recognize the importance of business continuity best practices and want to demonstrate a commitment to the profession.

- All active CBCVs in good standing are eligible to be listed in the Certified Vendor Directory on drii.org.

CERTIFIED BUSINESS
DRI
CBCV
CONTINUITY VENDOR

BAEM Conference
Bay Area's Emergency Managers

CBCV

"Having my DRI certification has been a real boon in helping me understand the processes my clients are working through and also to encourage my clients who don't have a BC program in place. It has also allowed me to present more at various functions due to my credentials." - CBCV
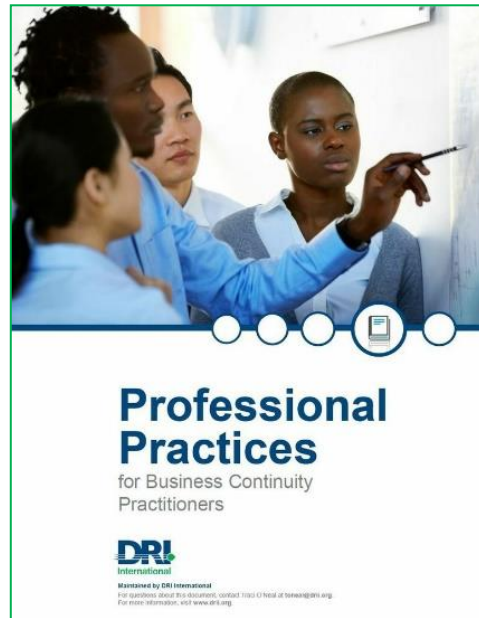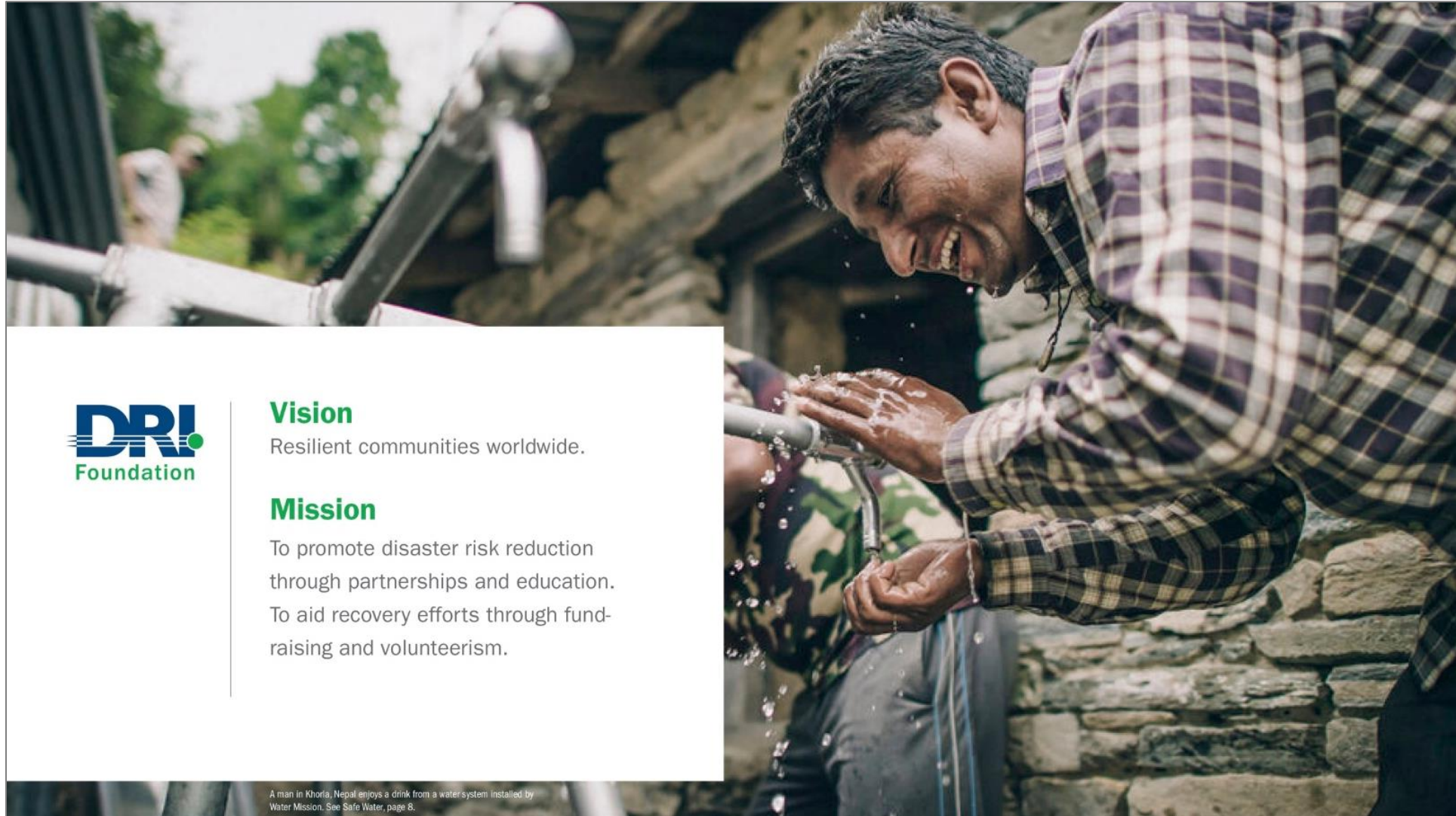
DRI Resource Library

- Our website contains free informational resources, job listings, and a presentation library.

- The Professional Practices serve as the heart of our teachings and thought leadership and are available in their entirety.
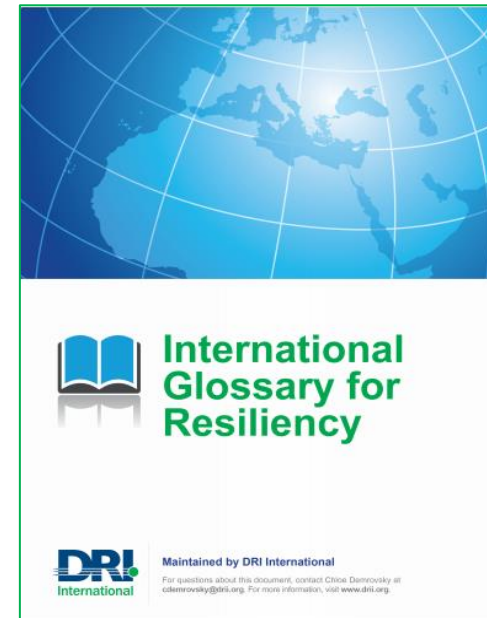
DRI Foundation: Charitable giving and volunteerism

Vision
Resilient communities worldwide.

Mission
To promote disaster risk reduction through partnerships and education. To aid recovery efforts through fundraising and volunteerism.

A man in Khoria, Nepal enjoys a drink from a water system installed by Water Mission. See Safe Water, page 8.

Helping those who protect us

The Veterans Outreach Program (VOP) helps veterans transition into the professions of emergency response, crisis management, business continuity and disaster recovery.

- Helping those who protect us

- Providing free training (sponsored or Montgomery GI Bill)

- Providing career guidance

- Reaching out to military and veterans' organizations to provide free seminars

Background- Presenter Summary

❑ 24 years in the Business Continuity Industry
  ❑ Masters of Science in Business Continuity- Norwich University

❑ Subject Matter Expertise in Governance, Risk, Compliance and Controls
  ❑ Technology, Financial, E-Commerce, Consulting

❑ Engaged with Disaster Recovery Institute (DRI) for 15+ years
  ❑ Certification Commission, Strategic Alliances Commission, DRI Foundation Director, Instructor, Professional Practices Review

❑ And... I'm a Grandma!!!!

Brainteaser

FINISHED FILES ARE THE RESULT OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS.

How many "F's" do you see in the above sentence?

Setting the Stage: Terms and Definitions

Common Terminology

- Risk Management (ISACA)

- Policy Management (OCEG)

- Compliance Management (OCEG)

- Governance (ISACA)

- GRC (DRII)

- BCM (DRII)

- Resilience (DRII)

Risk management

Policy

Compliance

Governance

Governance, Risk and Compliance (GRC)	GRC is the umbrella term covering an organization's approach across Risk and these three areas. Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations. (BCI)
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. (ISO 22301)
Resilience	The adaptive capacity of an organization in a complex and changing environment. *ASIS Editor's Note:* a. Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event. b. Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must. (ASIS)

Vehicle Diagnostics- The Facts

- Team Strategy
- Business Objectives
- Current challenges
- Nuances in terminology
- Heads up on associated regs coming down the pipe

| Releases | Requirements | Service Level Agreements |

Rules of the Road- Tactical

Responsible (*doer*):
- Owns the problem/project
- Ensures that work is done correctly and meets deadlines
- Performs the task

Accountable (*"the buck stops here"*):
- Must sign-off on work

Consult (*in the loop*):
- Has information and/or capability necessary to complete the work

Inform (*keep in the picture*):
- Must be notified of results, but need not be consulted

	Task	Engineering Team	Sr Leaders	Governance, Business Continuance, Compliance, Risk Management	Partners
Ex.	Sample Task Name	R (team members name)	A (team members name)	C (team members name)	I (team members name)
1	Identify Risk				
2	Develop RACI				
3	Document the Need				
4	Gain Approval				
5	Publish Final				
6	Maintain				
7					
8					

Rules of the Road- Strategic

❑ Identifies Priorities based on Strategic Roadmap
❑ Provides final Approval

❑ Review Progress of Final Deliverables
❑ Provide feedback on completion

❑ Develops Milestones and Target Timeframes for success

Board

Sr Leadership

Governance Committee

Steering Committee

Working Groups
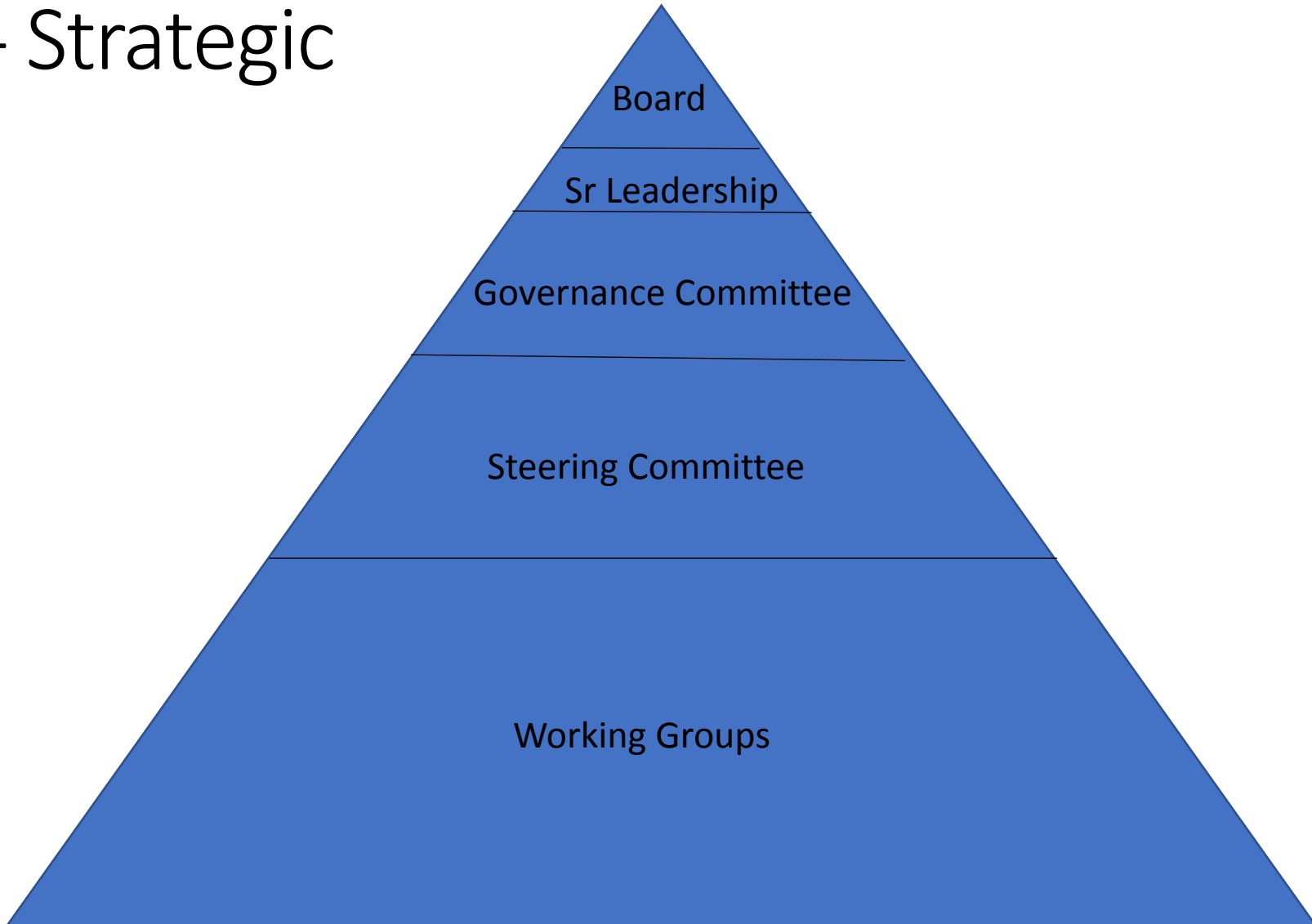
Maintenance Schedule- Governance

❑ *Policies, Standards and Procedures (PSP)-*
  ❑ Policy "Why"- A statement of intent from a governing authority that guides business decisions in order to direct an organization's actions in pursuit of long term objectives
  ❑ *Standard "What"*-A documented requirement, rule, or practice monitored for compliance, and used to direct actions to satisfy the intent of a policy in whole or in part.
  ❑ *Procedure "How"-* A description of specific steps or a process that, when completed, satisfies in whole or in part one or more Standards.
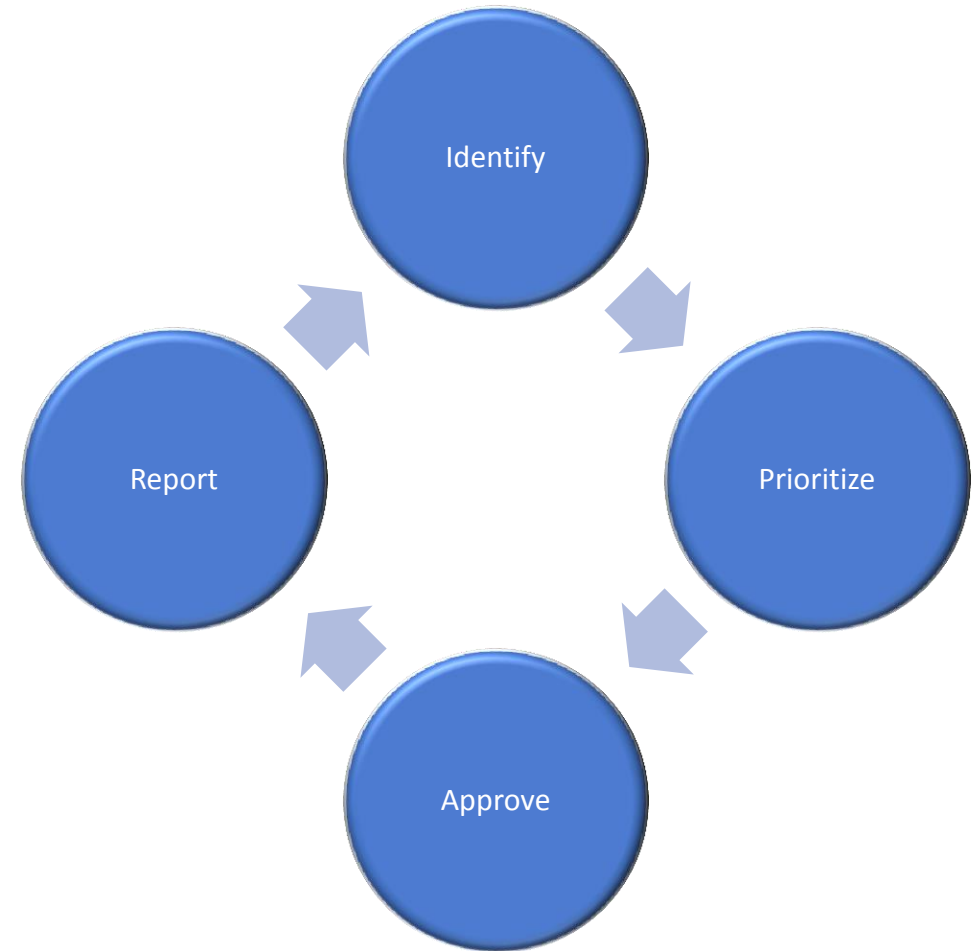

Understanding and Communication: 1 and 2 (United in the News)
3 and 4 (Oreck Vacuum)

Maintenance Schedule cont, - Risk
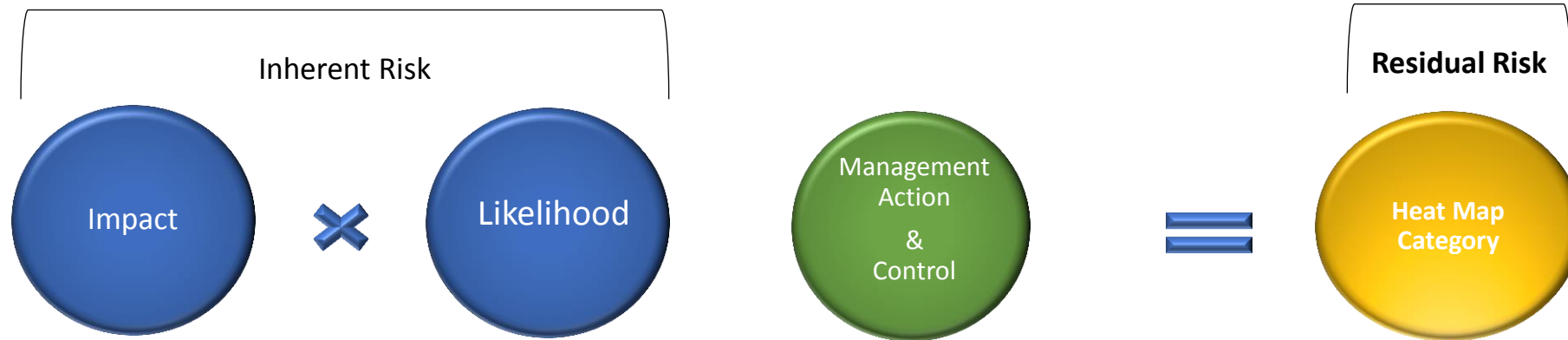
❑ *Risk-* **"What** *are the Challenges"*

[COSO and Deloitte Article- "Thought Leadership in ERM"](#)

Maintenance Schedule cont, - Risk

What is your teams strategy? → What are the business objectives that align to that strategy ? → What are the risks * associated with achieving? → What drivers fuel those risks? → What controls are in place to mitigate those risks?

Maintenance Schedule cont, - Risk

Inherent Risk

Impact $\times$ Likelihood

Management Action & Control

$=$ Heat Map Category

Residual Risk

Create a rating scale:

- Impact- (Operational, Financial, Customer, Legal, etc...)
- Likelihood- (Has it happened before, is it highly likely, not probable, etc...)
- Management Action and Control- (Are there metrics, is accountability in place, is a monitoring process in place, are there previous deficiencies, are policies, standards and procedures (psps) documented, etc...)
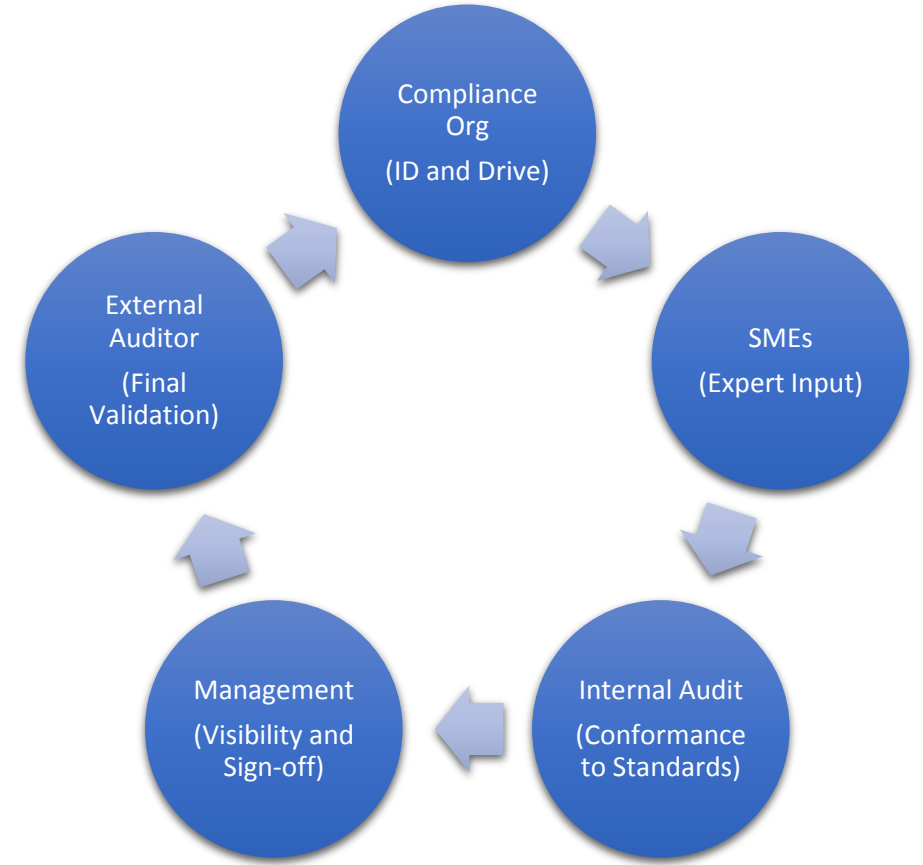
Maintenance Schedule cont, - Risk

Rating	Description
High (3)	
Medium (2)	
Low (1)	

✓ Leverage Governance Structure
✓ Report on Risk Categories
✓ Gain Approval for Mitigation and Action Plans

Impact

High

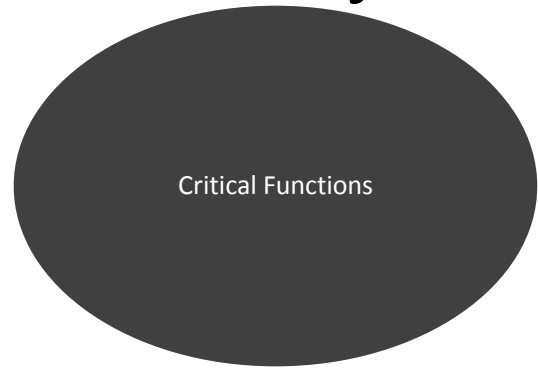Medium

Low

High Medium Low

Likelihood

Maintenance Schedule cont, - Compliance

❑ *Compliance-* ***"How*** *well are the controls being managed".*
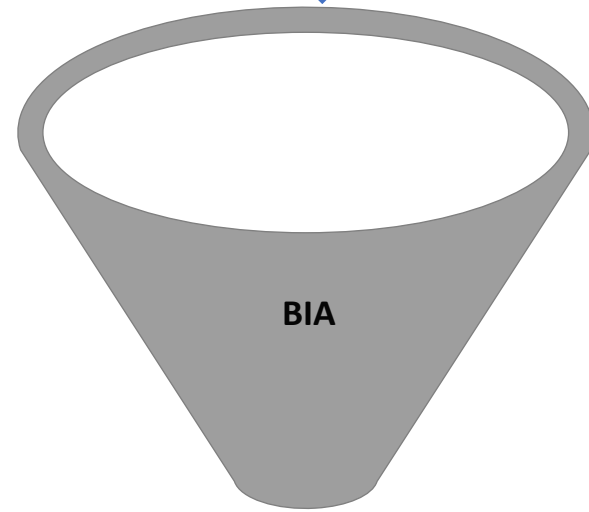❑ Roadmap
❑ Projects and Documentation

Critical Fix Towards Resiliency- Business Continuity

Leverage Risk Data

Critical Functions

DRII Professional Practices

Understanding Resilience

BIA

- Recovery Time Objective
- Recovery Plan Objective

Gaps Identification, Action and BC Plans

Bridge to Wellness and Key Takeaways

- ❑ Communication is Key
- ❑ Clarity on approach and roles and responsibilities is paramount
- ❑ Requirements- What is Needed??
- ❑ It takes a team, driving towards a common goal…

We Thank You!!

Michele L. Turner MBCP, FBCI, CISA, CRISC, GRCP
Senior Manager- Business Continuity and Risk
mlturner@amazon.com
W-206.435.5436 | M- 425.923.0635