OCTAVE: FORTE Process Training

Step 3: Identify Resilience Requirements of Assets

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

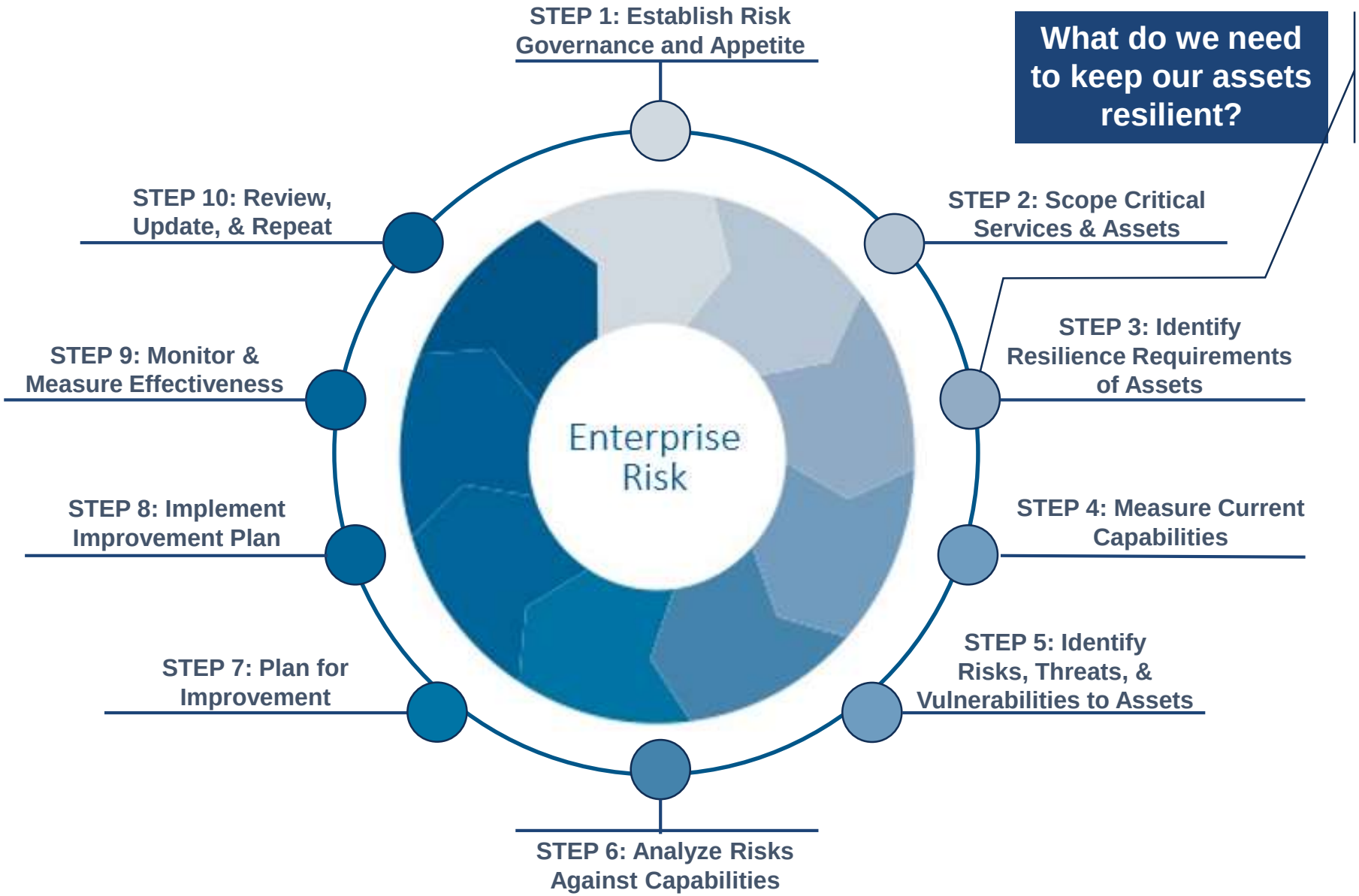
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0477

What do we need to keep our assets resilient?



© 2019 Carnegie Mellon University

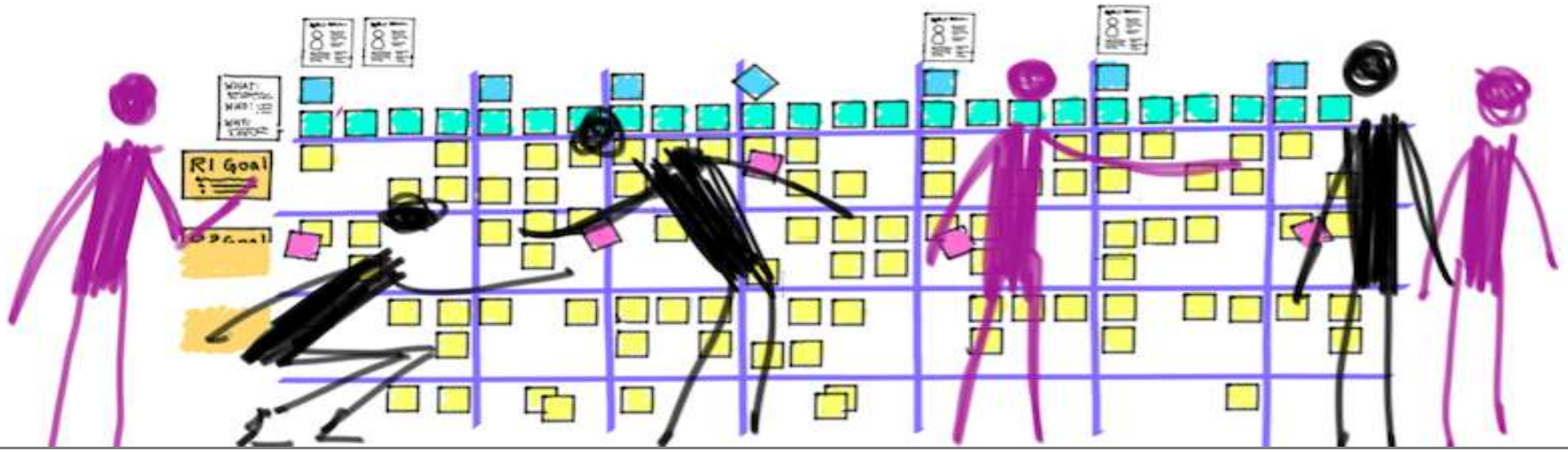
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Resilience Requirements of Assets
Determining Requirements

Operational resilience: How well a system can maintain continuity of critical services in the presence of disruptive events

Think about the services your organization provides that are most critical to its survival and success

How and when would those services be restored if disrupted?



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Develop Resilience Requirements
Based on Asset Support of Services

Derive resilience requirements from previous/current information security risk assessments and business impact analyses

Identify and document High Value Services (HVSs) critical to organizational mission, then map them to the assets (HVAs) that support them

Base resilience requirements on the asset's contribution to the support of those services

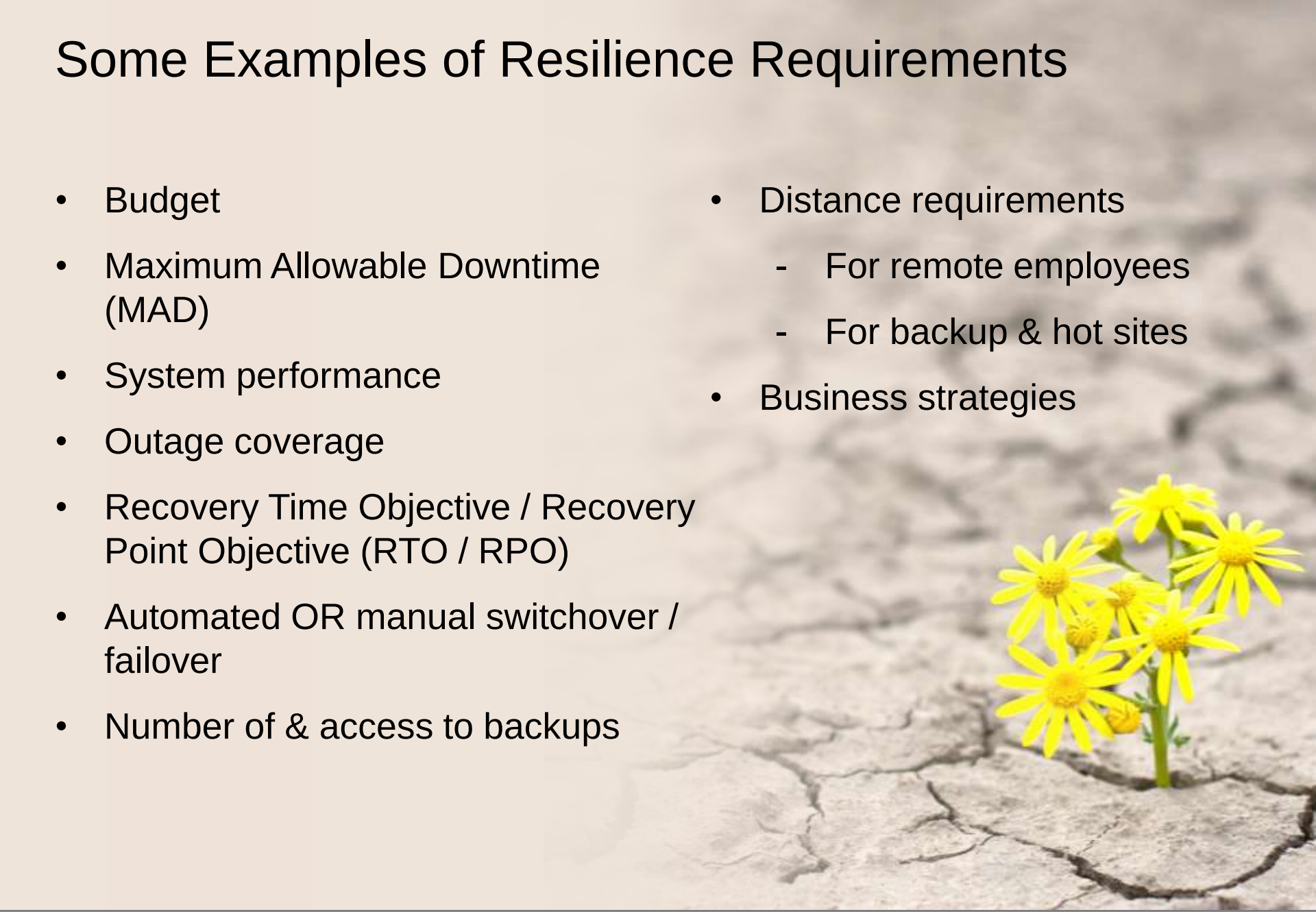
Document CIA requirements for each asset supporting a critical service

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Some Examples of Resilience Requirements

- Budget
- Maximum Allowable Downtime (MAD)
- System performance
- Outage coverage
- Recovery Time Objective / Recovery Point Objective (RTO / RPO)
- Automated OR manual switchover / failover
- Number of & access to backups
- Distance requirements
  - For remote employees
  - For backup & hot sites
- Business strategies



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Developing Asset Requirements

Asset Requirements CIA Matrix (Riesgo Example)

Asset Name	Confidentiality	Integrity	Availability
Manufacturing Facility	Access to facilities must be limited to employees and permitted guests only	The site must be monitored for any unwanted changes to data	Backup site plans must be in place and facility upkeep must be regulated
Employees	Employee information must be secure and releasing of company information must be prohibited	EAP in place to support employees	Employee succession plan must be up to date, points of contact must be established
Customer Data	Customer database requires firewalls, access controls, encryption, and IDS	Checks on data must be ran periodically, audit trail of data must be used	Data must be stored on secondary external backup server for emergencies or high activity

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Resilience Requirements of Assets
Who determines requirements?

Service owners & custodians, asset owners & custodians

Asset owners have ultimate responsibility for identifying, establishing, and communicating the requirements of assets

Requirements must be understood and agreed upon by custodians

- Owners develop and monitor the requirements

- Custodians implement requirements

Revisit asset requirements through periodical security risk assessment, business impact analysis, and asset owner interviews

Validate that asset requirements serve the goals of organizational drivers

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Resilience Requirements of Assets
Managing Changes

There are constant changes to asset status & importance

Organizations should revisit resilience requirements regularly

Some grounds for a resilience requirements review may be:

- Staff changes (hiring/firing of employees, promotions, etc.)
- Information changes (Creation, alteration, or deletion of data or files)
- Technology changes (Adding new components, retirement of old tech)
- Facility changes (Adding, altering, or retiring of facilities)
- Vendor & vendor contract changes
- The creation of a new, related asset – review asset dependencies to document & attempt to resolve conflicting requirements

Discussion: How often should resilience requirements be revisited?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Resilience Requirements of Assets
Managing Changes (cont.)

Recommendations for managing requirement changes include:

- Document asset changes in the asset inventory
- Document requirement change history with rationale for changes
- Evaluate impact of asset changes on existing resilience requirements
- Establish communication channels to ensure consensus on requirements between owners and custodians
- Consider the factors: strategic objectives, risk appetite, and operational constraints of the organization

© 2019 Carnegie Mellon University

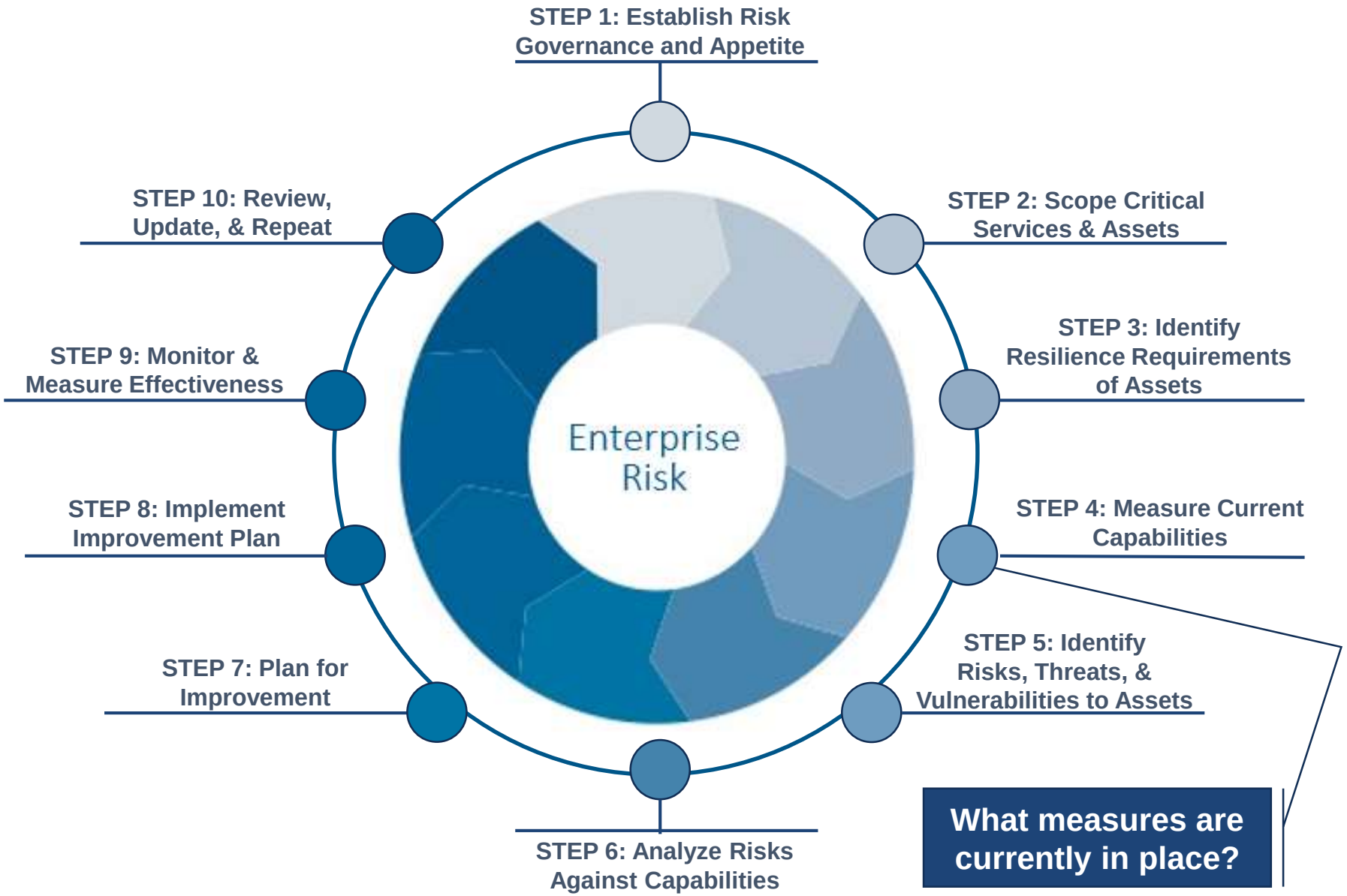
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 4: Measure Current Capabilities

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

What Measures Are in Place to Keep Assets Resilient?
Controlling Resilience

Controls can be defined as the measures instituted to guide or regulate the activities or operations of a machine, person, or system

Controls are put in place to enhance the security and resilience of assets, either to adhere to legal requirements or for personal security

The effectiveness of controls therefore directly determines whether or not resilience requirements are being met

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Assessing Current Resilience Capabilities

Objective: Create a register of risk management controls, procedures, and plans and gather data to assess their effectiveness

Start by establishing control objectives

- Set targets for performance based on strategic objectives, risk tolerance, service/asset resilience requirements, etc.
  - Setting performance objectives assists in establishing appropriate levels of controls
- Prioritize control objectives
  - Are controls meeting the crucial objectives you have set for them?
- Identify activities that enable or enhance the achievement of objectives

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Control Types

Multiple ways to categorize controls: preventative, detective, and corrective **or** administrative, technical, and physical, but can also be broken down into:

Standard Controls: Common sense controls that any successful organization should have

- Access controls, passwords, locks, etc.

Compliance required: Controls required by law

- SOX requirements, FISMA, sprinkler system, etc.

Best Practice: Controls that are generally accepted as being most effective in the industry, but may be out of reach for smaller companies

- Security cameras, antivirus software, intrusion detection system

Want to haves: Controls that are desired to increase security or resilience that are out of reach or potentially excessive

- Biometric access control, multi-factor authentication, etc.

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Assessing Controls
Questions To Ask

- *Most importantly, are all applicable compliance requirements handled sufficiently by controls?*
  - If not, can current controls be modified to?
- *Are the controls currently in place satisfying the crucial objectives set for them? If not, does risk appetite justify overlooking the gap?*
- *Are there any gaps where a service objective is not adequately satisfied by any controls?*
  - If so, can current controls be modified? What is the most cost effective option to adequately satisfy our objectives?

Discussion: What are some “want to have” controls for your company? How would their addition enhance realization of control objectives? Do its benefits outweigh the costs?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Managing Compliance Obligations

Most companies have some form of regulations that must be complied to, whether mandated by government, their industry, or internally

Having a compliance plan in place assists in making effective and efficient decisions for satisfying requirements

- Establish guidelines / standards
- Inventory obligations
- Analyze obligations
- Establish ownership for obligations
- Monitor / measure compliance

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Measuring Current Resilience
Leveraging Resilience Maturity Assessments

CERT Cyber Resilience Review: Free, internal assessment of your organization's resilience capabilities

Provides gap analysis to give recommendations for improvement

Guides in the 10 following areas:

- Asset management
- Controls management
- Configuration and change management
- Vulnerability management
- Incident management
- Service management
- Risk management
- External dependencies management
- Training and awareness
- Situational awareness

CERT CRR

© 2019 Carnegie Mellon University

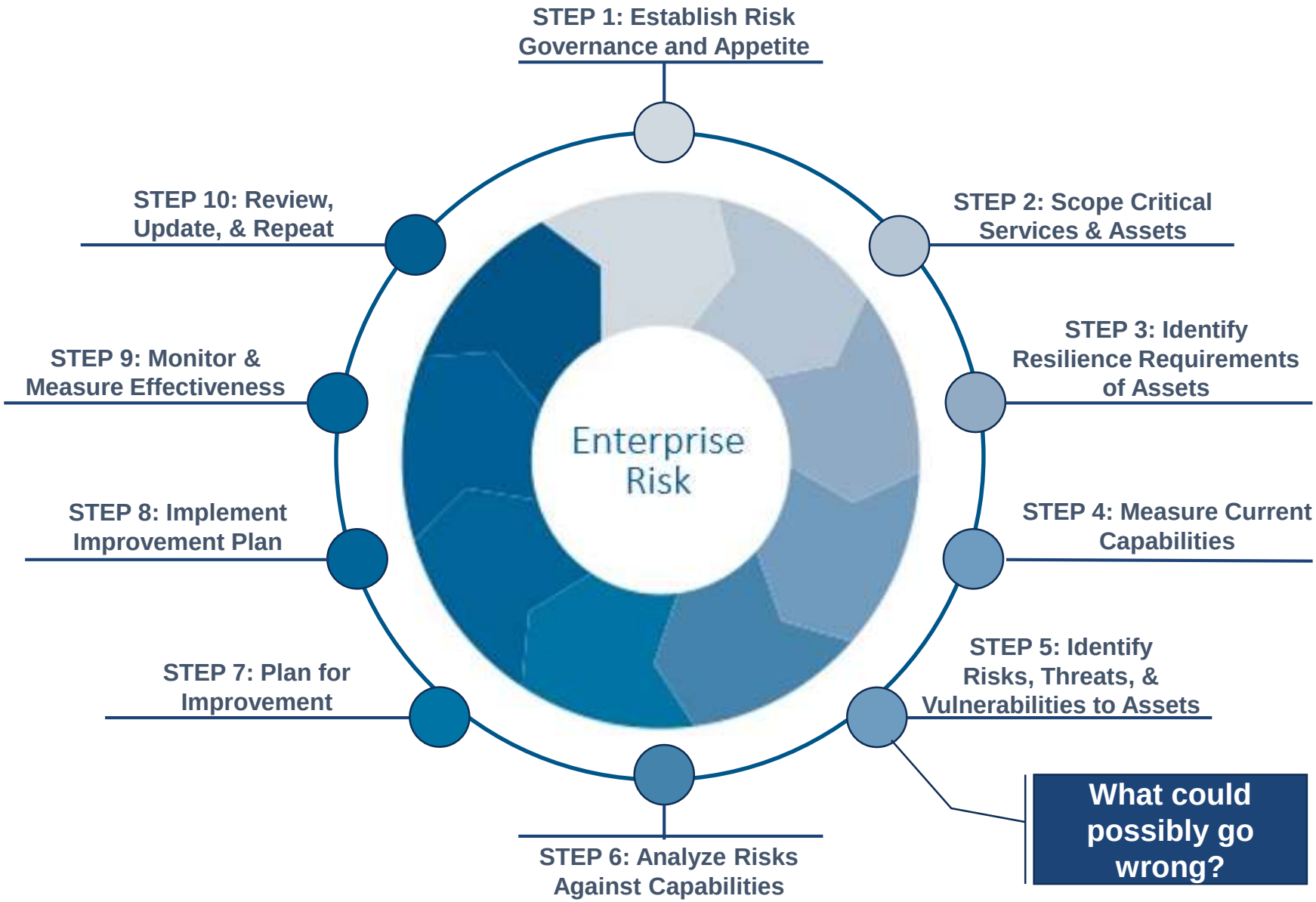
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 5: Identify Risks, Threats, and Vulnerabilities to Assets

© 2019 Carnegie Mellon University

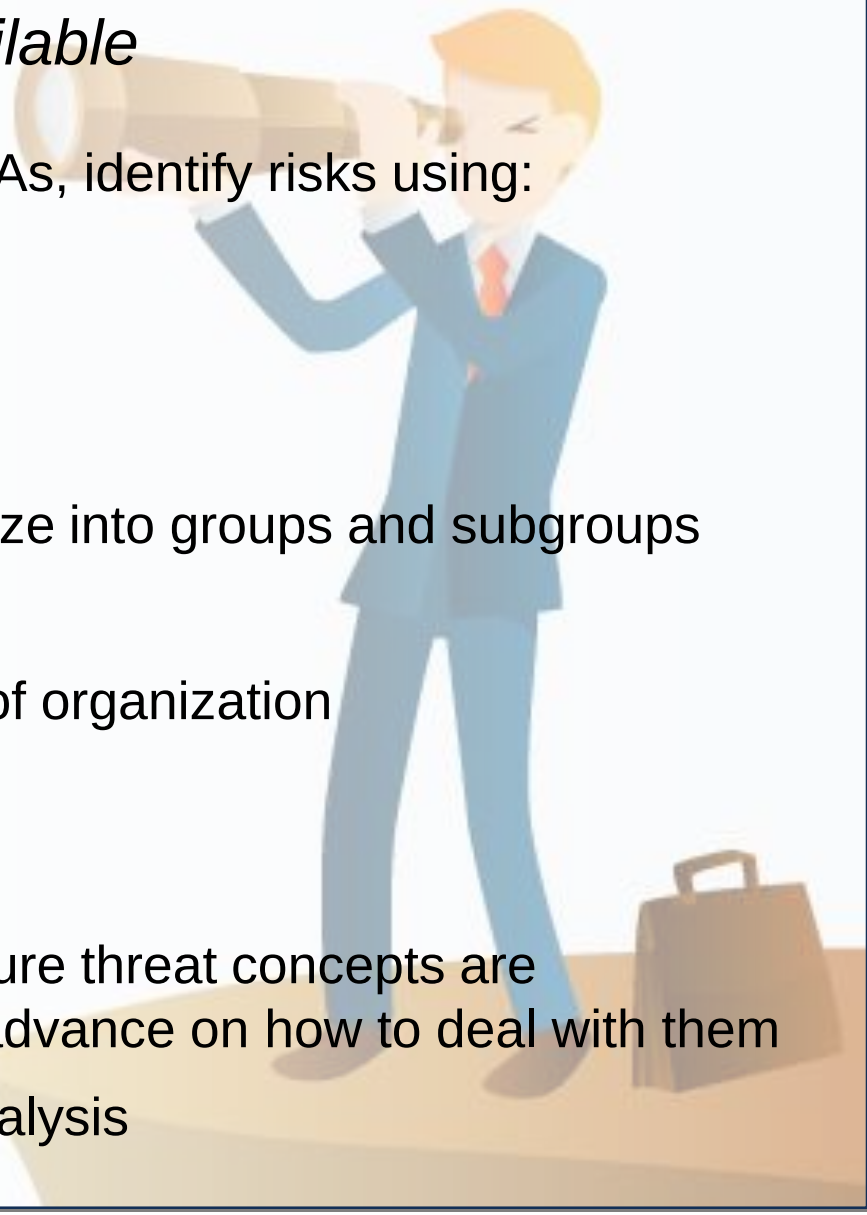
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Risk Identification
Many Tools & Techniques are Available



Given an understanding of HVSs and HVAs, identify risks using:

- Interviews with key stakeholders
- Scenario planning
- Affinity Diagrams
  - Brainstorm, discuss ideas, categorize into groups and subgroups
- Penetration testing
- Review of registers from other parts of organization
- Assumption analysis
- Nominal group technique
- Threatcasting: technique in which future threat concepts are forecasted and plans are created in advance on how to deal with them
- FMEA – Failure Mode and Effects Analysis

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Quantitative Facilitation

Fill in the Gaps With the Best Data Available

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Failure Mode and Effects Analysis (FMEA)
Structuring Risk Mitigation

- Inductive reasoning that helps identify potential failure modes based on past experience with similar products or processes
  - *"How could our process fail, and how can we prevent that?"*
- Analyze the causes and effects of different kinds of failures
- Rate severity, occurrence likelihood, detection ability, and risk priority
- Determine actions to mitigate the risk

Process Step	Potential Failure Mode	Potential Failure Effect	SEV	Potential Causes	OCC	Current Process Controls	DET	RPN	Action Recommended
What is the step?	What are ways the step can go wrong?	What is the impact on the customer if failure mode is not prevented?	How severe is the effect on the customer?	What is the cause of the failure mode?	How frequently is the cause likely to occur?	What are the existing controls for prevention or detection of the failure mode?	How probable is detection of the failure mode or its cause?	Risk priority (SEV x OCC x DET)	What actions can reduce occurrence of the mode or improve its detection?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Failure Mode and Effects Analysis (FMEA)
Completed Example – Commercial Banking

Process Step	Potential Failure Mode	Potential Failure Effect	SEV[1]	Potential Causes	OCC[2]	Current Process Controls	DET[3]	RPN[4]	Action Recommended
What is the step?	In what ways can the step go wrong?	What is the impact on the customer if the failure mode is not prevented or corrected?	How severe is the effect on the customer?	What causes the step to go wrong (i.e., how could the failure mode occur)?	How frequently is the cause likely to occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is detection of the failure mode or its cause?	Risk priority number calculated as SEV x OCC x DET	What are the actions for reducing the occurrence of the cause or for improving its detection? Provide actions on all high RPNs and on severity ratings of 9 or 10.
ATM Pin Authentication	Unauthorized access	• Unauthorized cash withdrawal • Very dissatisfied customer	8	Lost or stolen ATM card	3	Block ATM card after three failed authentication attempts	3	72	
	Authentication failure	Annoyed customer	3	Network failure	5	Install load balancer to distribute workload across network links	5	75	
Dispense Cash	Cash not disbursed	Dissatisfied customer	7	ATM out of cash	7	Internal alert of low cash in ATM	4	196	Increase minimum cash threshold limit of heavily used ATMs to prevent out-of-cash instances
	Account debited but no cash disbursed	Very dissatisfied customer	8	• Transaction failure • Network issue	3	Install load balancer to distribute workload across network links	4	96	
	Extra cash dispensed	Bank loses money	8	• Bills stuck to each other • Bills stacked incorrectly	2	Verification while loading cash in ATM	3	48	

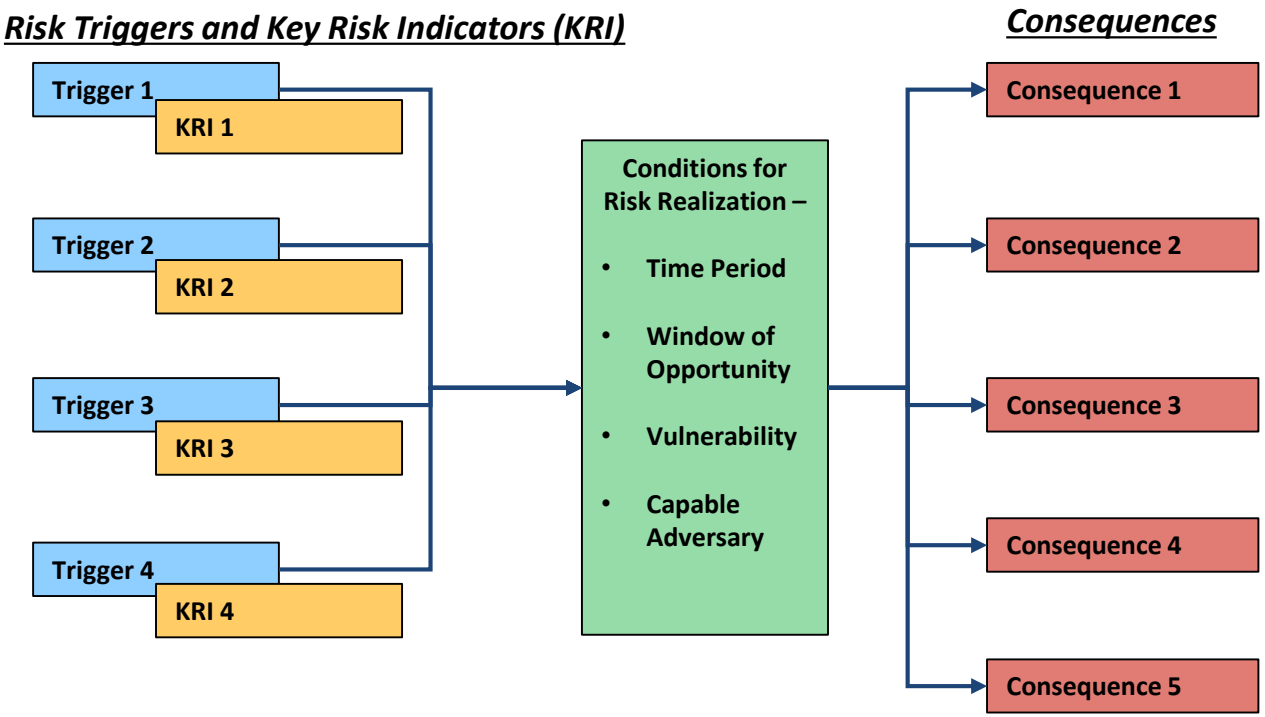
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Toolkit: Risk Tree
One Tool to Use for Risk Analysis

Category: Risk Title

Scope Statement: <Typically an "if, then" statement>



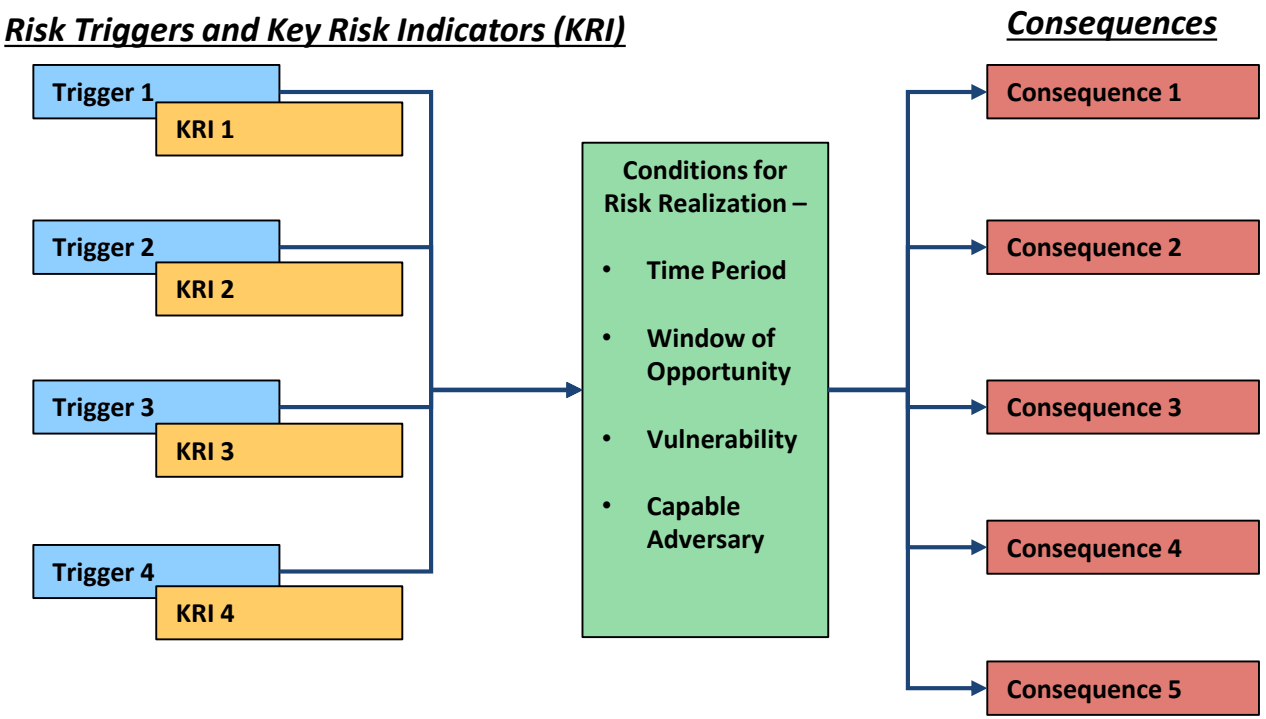
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Risk Tree Example

Category: Risk Title

Scope Statement: If the organization suffers a major interruption in logistical support, then mission and lives could be jeopardized. Opportunistically, if uncertainty is removed from the logistical chain, then resources could be saved and mission success rates could improve.



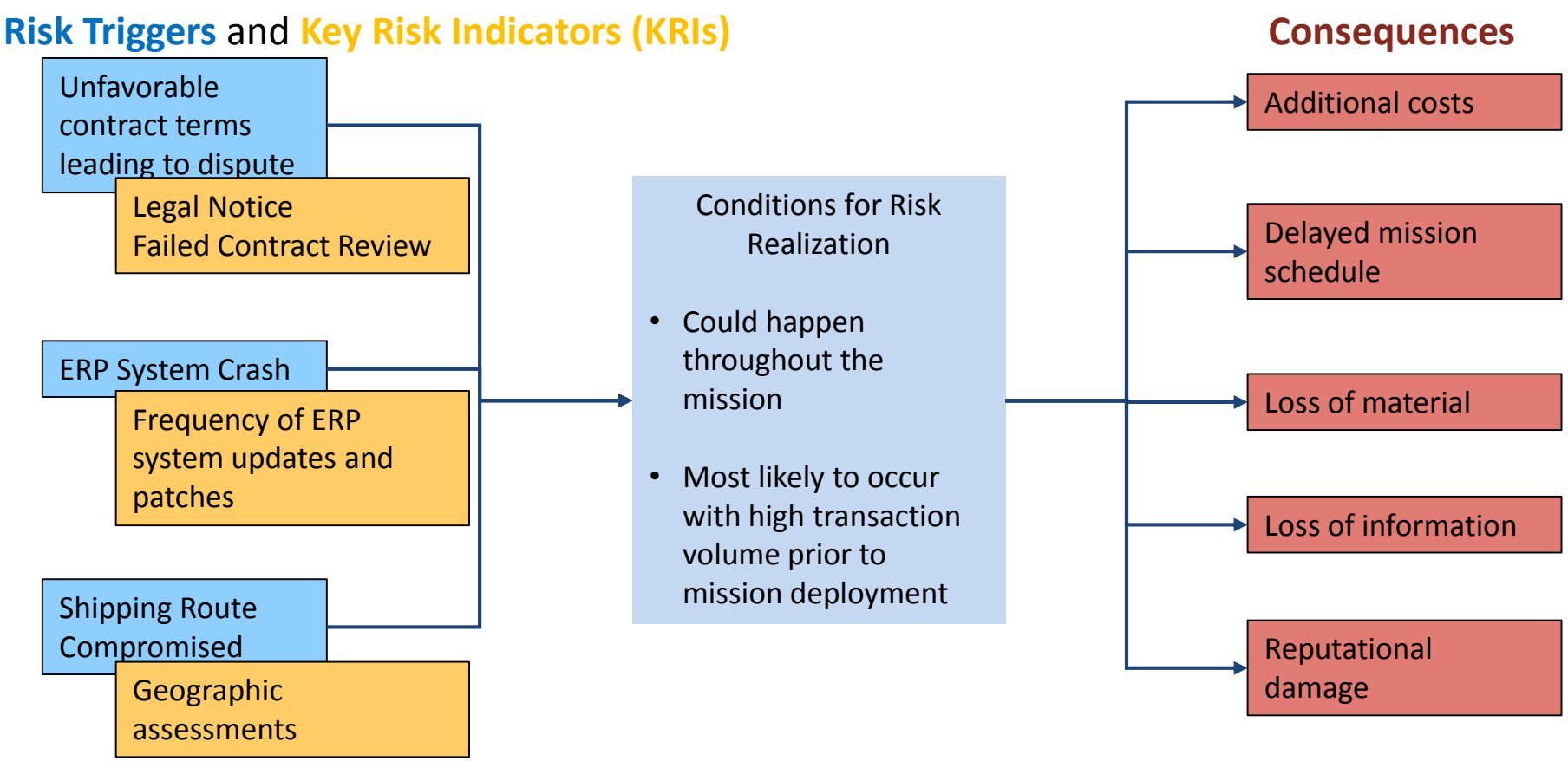
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Potential Solution

Operations: Logistics Resilience

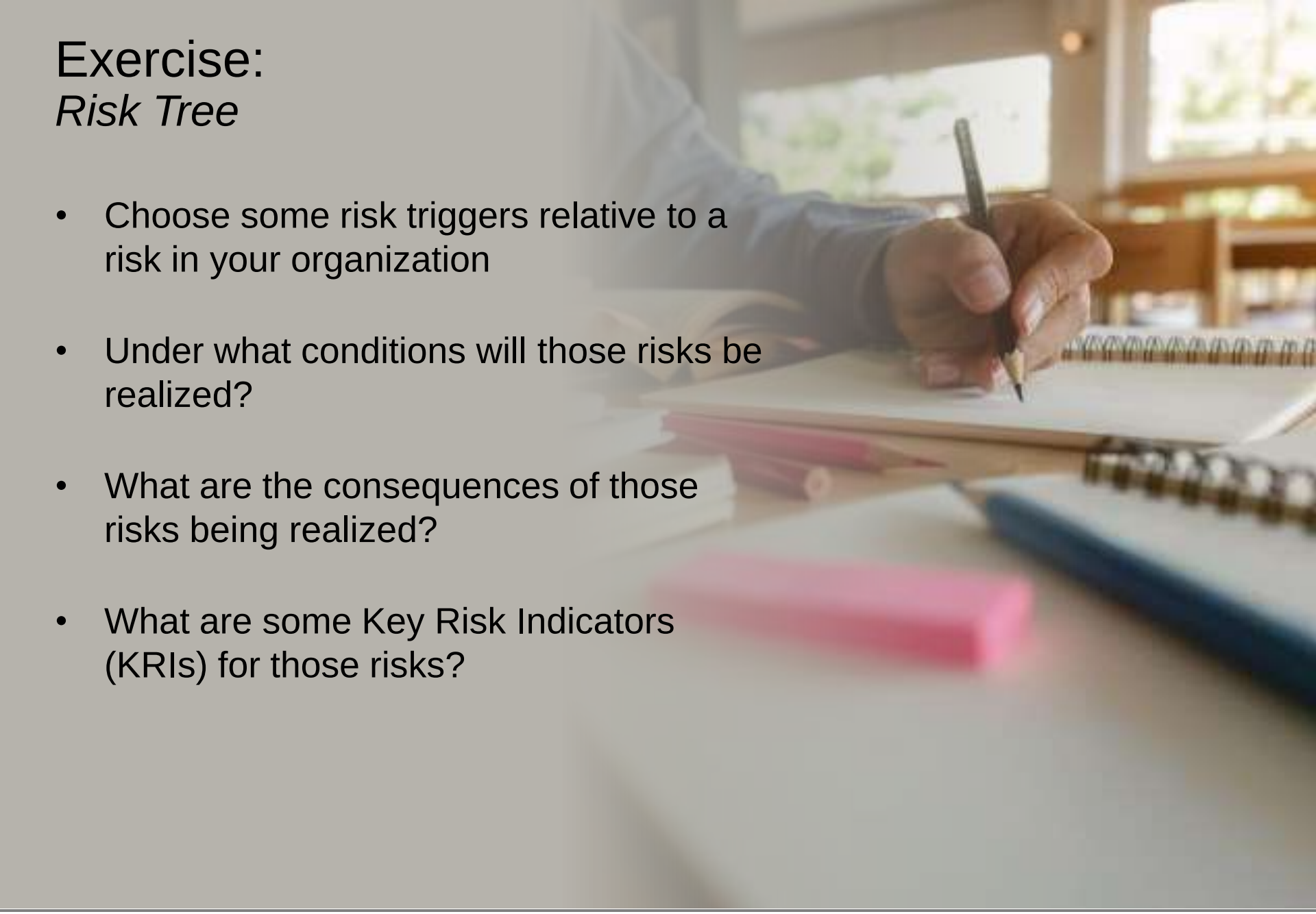
Scope Statement: If the organization suffers a major interruption in logistical support, then mission and lives could be jeopardized. Opportunistically, if uncertainty is removed from the logistical chain, then resources could be saved and mission success rates could improve.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Exercise:
Risk Tree



- Choose some risk triggers relative to a risk in your organization
- Under what conditions will those risks be realized?
- What are the consequences of those risks being realized?
- What are some Key Risk Indicators (KRIs) for those risks?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Example of Risk Register Documentation Step
Documenting Identified Risks

Risk Definition (if/then statement): If the organization suffers a major interruption in logistical support, then mission and lives could be jeopardized. Opportunistically, if uncertainty is removed from the logistical chain, then resources could be saved and mission success rates could improve.

Trigger Event Description		Add trigger event	Remove Trigger Event	Strategy	Associated KRIs	Associated Event Response	Weight	Likelihood	
	Title							I	R
1	Unfavorable Contract Terms Leading to a dispute			Accept (-)	a, b	A	Whole	High	medium

Trigger Response		ADD Trigger Response	REMOVE Trigger Response	Response Owner	Associated Trigger Event	Budget		Controllability		
						Allocated	Spent	P	I	V
A	Seek legal review of all contracts prior to submission for final authorization			Legal Department	1	K$1000	K$1	Y	R	

Key Risk Indicators (KRIs)			ADD KRIs	Remove KRIs		Associated Trigger Event	Value	
	Title	KRI Definition					Current	Critical
a	Legal Notice	Customer submission of legal notice to the organization				1	Green	More than 1
b	Failed Contract Review	Contract Review or deliverable rejected by customer				1	Green	More than 1

© 2019 Carnegie Mellon University

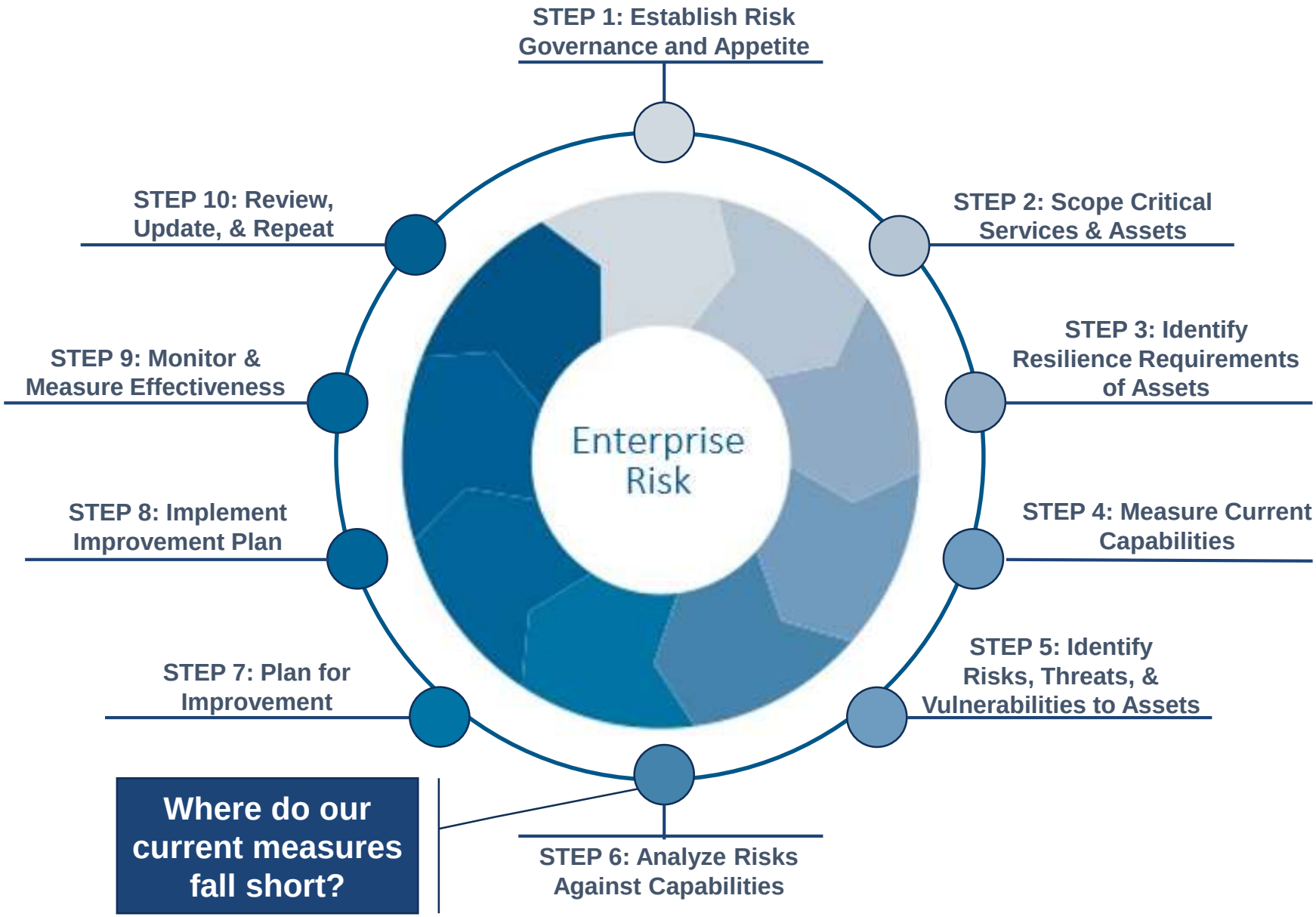
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 6: Analyze Risk Against Capabilities

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Collecting Data
Numbers are Crucial

- Controls such as firewalls, intrusion detection systems, intrusion prevention systems, and anti-malware systems hold important data
- Log correlation tools can use activity data to form reports, give warnings, and make suggestions
- Compare the data from your current controls to risk appetite to analyze what solutions are working well and what could be improved

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Determining Likelihood of a Risk

Risk likelihood can be difficult to be certain about, but there are multiple methods to make sure it is as close to accurate as possible:

Probability of Occurrence:

- Ideally, a definite number can be determined to estimate how likely the event is, however, this can be difficult
- Can be calculated with prior industry data, control data, or evaluating software

Category Ranking:

- Classifying risks into categories (e.g. High, medium, low, or always, often, sometimes, rarely, never)

Ordinal Ranking:

- Listing risks in order of likelihood to occur

Relative Likelihood:

- Comparing risk likelihood to that of another understood risk

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Pitting Risks against Current Capabilities

Advantages of Enterprise Risk Management Software

Enterprise risk management software is widely available to assist in many aspects of risk analysis

<u>Common ERM software features include:</u>

- Threat and vulnerability analysis
- Compliance management
- Vendor/third-party risk management
- Modeling and forecasting
- IT governance and security
- Incident management
- Audit management
- Financial reporting
- Policy management
- Notifications

Do independent research and find ERM software that closely aligns with your organization's goals and operational needs

[A good checklist for ERM quality]

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

ERM Software

Two examples: RSA Archer and Sword Active

RSA Archer:

- Enhances risk identification, assessment, controlling, and monitoring
- Can assist in decision making based on your risk appetite
- Integrated risk management to manage full scope of risks

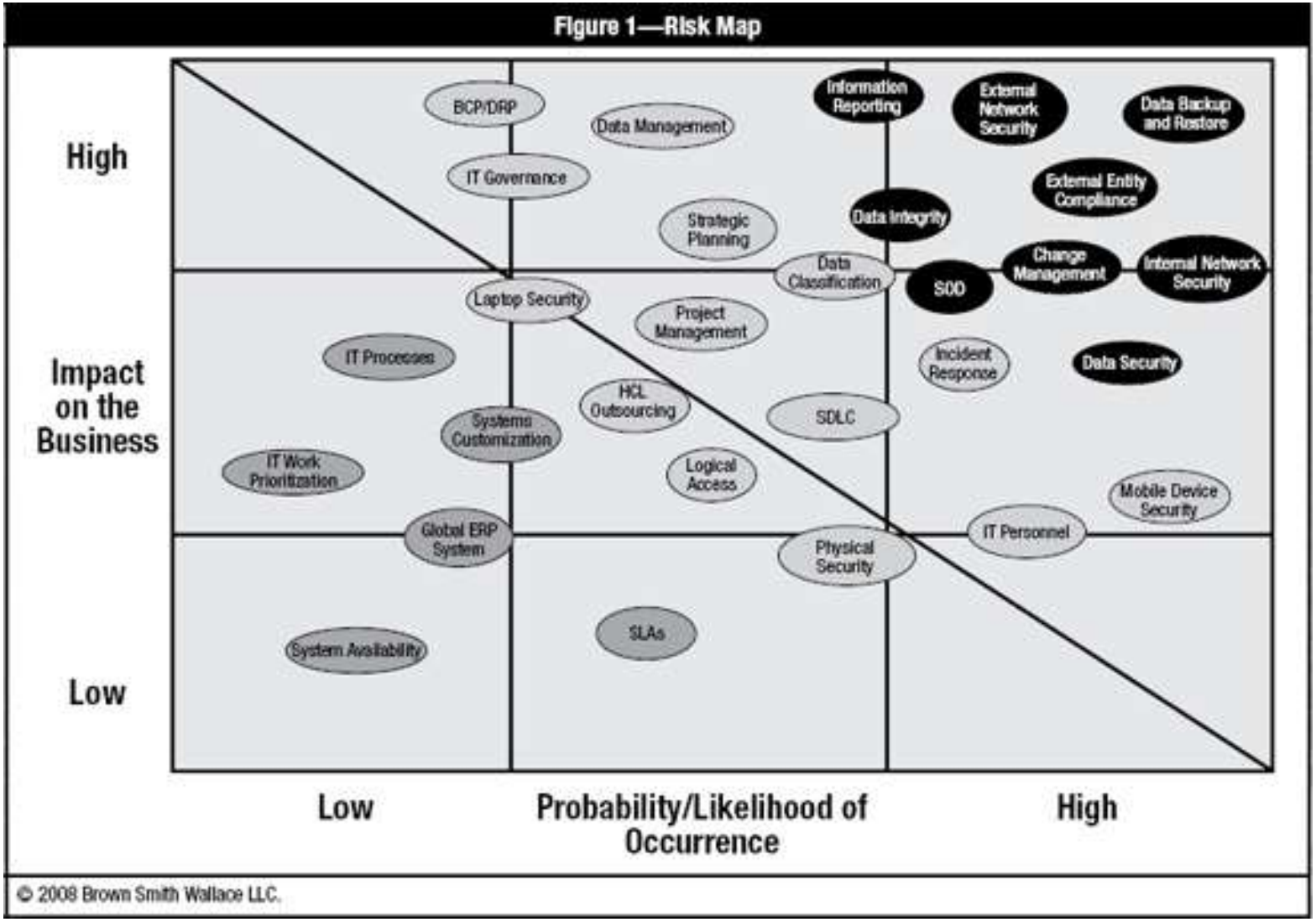
Sword Active Risk Management:

- Executive dashboards, centralized risk registers, automated alerts, graphic analysis
- Can assist in risk project management and strategic business planning
- Also integrated, addresses risk management needs of entire organization

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Business Impact Analysis

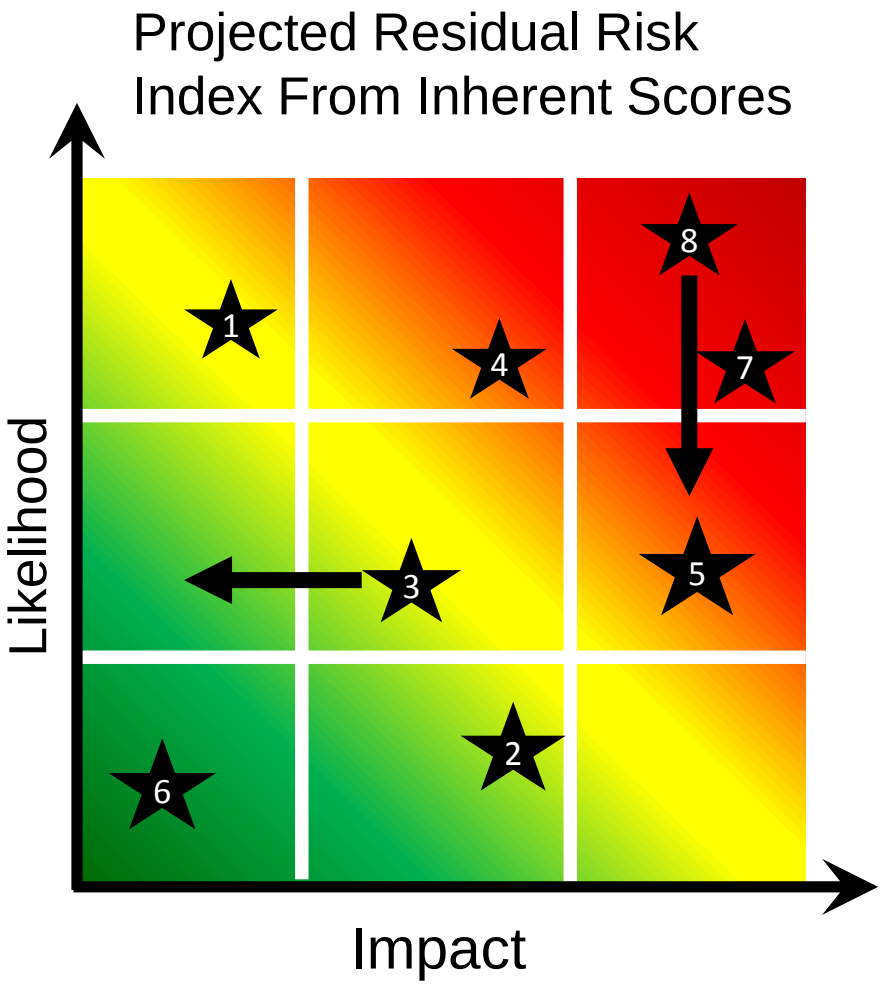


© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Plotting Risks Using a Heat Map

Where can you make the biggest impact?



Number	Risk
1	Cyber Security Breach
2	Talent Attrition
3	Compliance Violation
4	Unplanned Outage
5	Safety Incident
6	Overregulation
7	Loss of Customer
8	Insider Threat

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

What should we tackle first?
Prioritizing Individual Risks

- Risk appetite statements give a sense of the level of the risk
- Better methods for determining the order in which risks are addressed
- Including the grid & arc methods (borrowed from the LUMA Institute)
- Refer to the risk appetite statement after the exercise to see if priorities are largely consistent or change when examined a different way

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Prioritizing Risks By Likelihood and Cost
LUMA Method

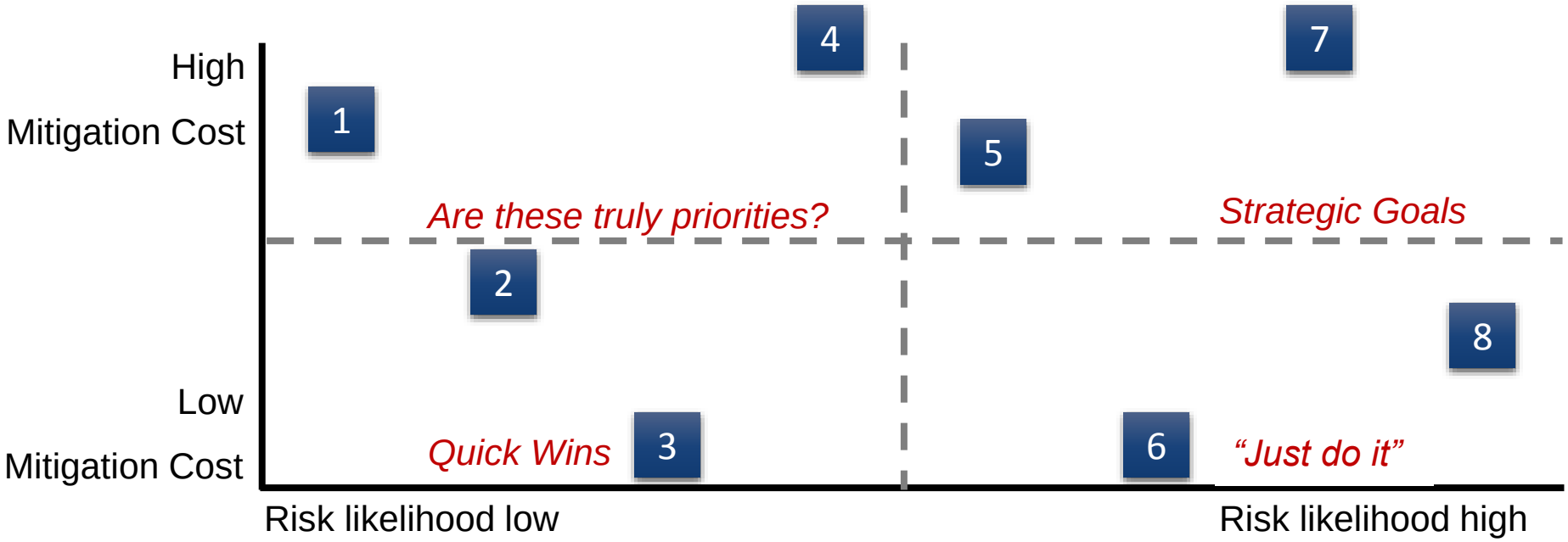
1. List risks
2. Categorize in order of relative likelihood
3. Categorize in order of relative cost
4. Grid or arc method to determine where to concentrate efforts

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Prioritizing Risks By Likelihood and Cost
LUMA Grid Method

1. List risks
2. Categorize in order of relative likelihood
3. Categorize in order of relative cost
4. Grid or arc method to determine where to concentrate efforts

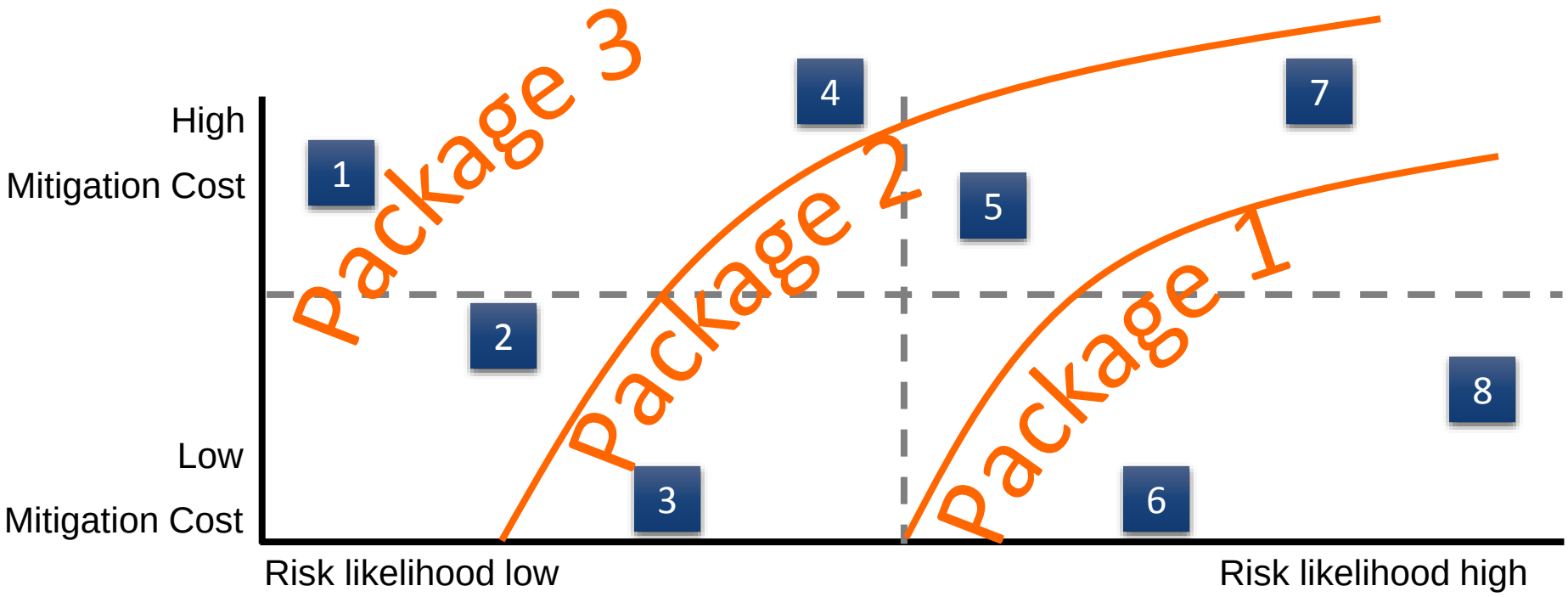


© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Prioritizing Risks By Likelihood and Cost
LUMA Arc Method

1. List risks
2. Categorize in order of relative likelihood
3. Categorize in order of relative cost
4. Grid or arc method to determine where to concentrate efforts



© 2019 Carnegie Mellon University

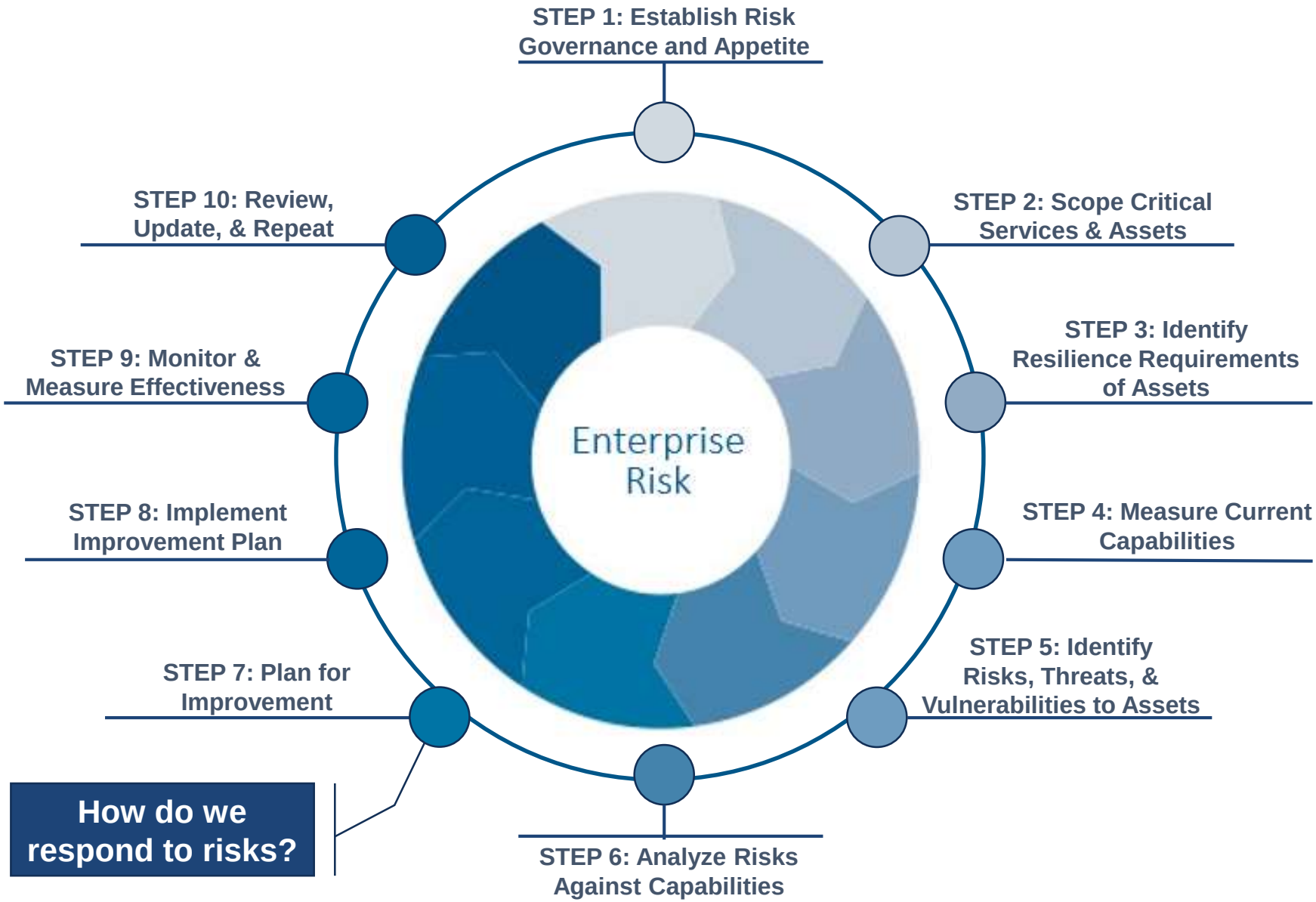
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 7: Plan For Improvement

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Next Step Beyond Assessment
Make a Business Case to Manage Risk

Two types of response planning

- Eliminate or mitigate triggers
- Prepare for a day that may never come

At a high level, balance options are

- Accept
- Avoid
- Mitigate
- Transfer
- Enhance
- Exploit
- Share

It is impossible to have 100% security, some **residual risk** will always remain

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Goals
Setting SMART goals

Knowing now how current controls stack up against risks, you now beginning planning for improvement

Goal setting is a great first step to brainstorm potential improvement plans, and later assists in evaluating success

Always try to make goals SMART:

- **Specific** – clearly stated
- **Measurable** – by clear, objective measurement
- **Attainable** – can it truly be achieved?
- **Relevant** – will this benefit us?
- **Timely** – what is the timeframe for achievement?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Setting SMART goals
Effective Goal Setting Example

S Specific	M Measurable	A Attainable	R Relevant	T Timely
In the next year, we want to train employees on social engineering tactics and lower our phishing exposure	We will continue to collect data on instances of phishing attacks and response to in-house phishing campaigns	Employee training can be mandated	Providing adequate training will show beneficial results for our company	All employees will be required to take the training in the next 3 months

Discussion: What goals does your organization have to improve resilience?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Selecting Risks to Respond to
Utilizing Decision Matrices

We can't respond to all of them; How should we prioritize and select risks to respond too?

Decision making method in which risks are compared to weighted criteria, resulting in a priority number

List risks in rows and weighted criteria in columns

Base criteria on ways the actualized risk can affect your organization and the complexity of a response

Decision Matrix: Long Wait Time

Criteria → / ↓ Problems	Customer pain 5	Ease to solve 2	Effect on other systems 1	Speed to solve 2	
Customers wait for host	High—Nothing else for customer to do 3 × 5 = 15	Medium—Involves host and bussers 2 × 2 = 4	High—Gets customer off to bad start 3 × 1 = 3	High—Observations show adequate empty tables 3 × 2 = 6	28
Customers wait for waiter	Medium—Customers can eat breadsticks 2 × 5 = 10	Medium—Involves host and waiters 2 × 2 = 4	Medium—Customer still feels unattended 2 × 1 = 2	Low—Waiters involved in many activities 1 × 2 = 2	18
Customers wait for food	Medium—Ambiance is nice 2 × 5 = 10	Low—Involves waiters and kitchen 1 × 2 = 2	Medium—Might result in extra trips to kitchen for waiter 2 × 1 = 2	Low—Kitchen is design/space limited 1 × 2 = 2	16
Customers wait for check	Low—Customers can relax over coffee, mints 1 × 5 = 5	Medium—Involves waiters and host 2 × 2 = 4	Medium—Customers waiting for tables might notice 2 × 1 = 2	Low—Computerized ticket system is needed 1 × 2 = 2	13

© 2019 Carnegie Mellon University

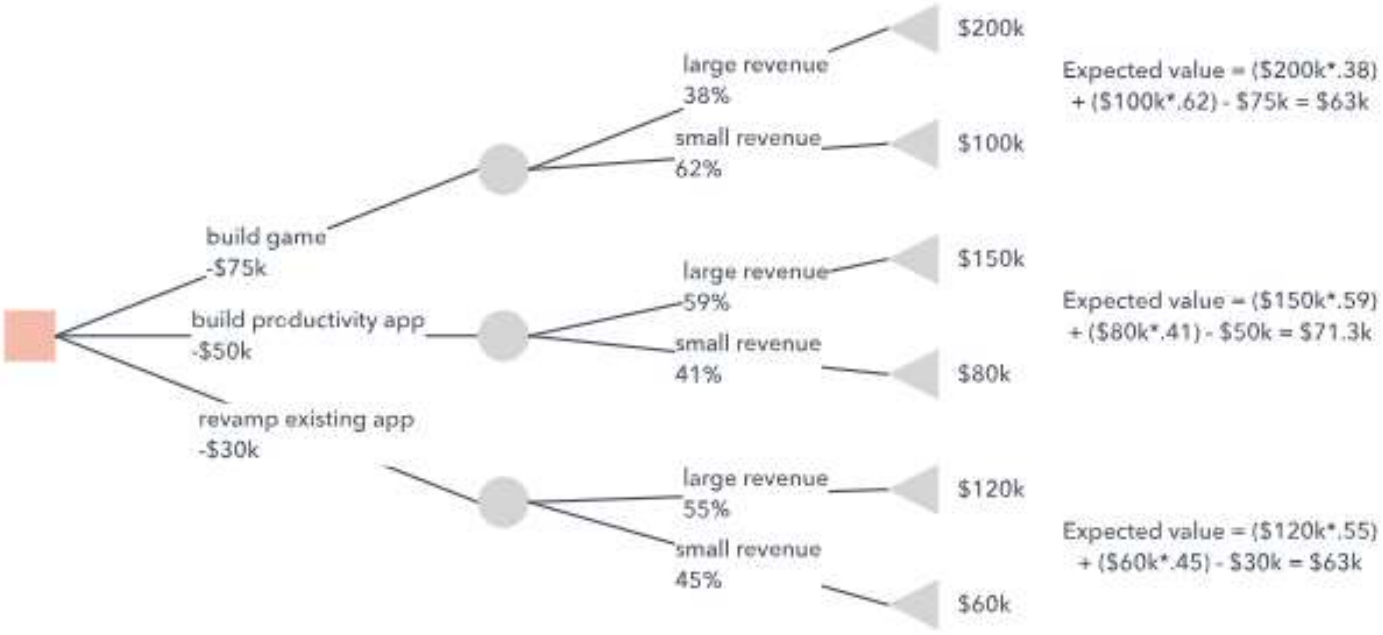
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Selecting Risks to Respond to
Utilizing a Decision Tree

Similar decision making method in which future pros and cons are forecasted to compare the possible outcomes of multiple options

Typically utilized to predict monetary expenditure and return

Probability of events is also taken into consideration to give expected values



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Building the Response Plan
Work for a Solution

Response plans can vary:

Projects or Just Do Its

- Capital investment
- Training
- Communication
- Policy change
- Contingency planning
- Organizational change
- Asset procurement

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Gathering governance support
Defining "Executive"

"An executive is defined as a person responsible for the administration of a business or department. […] An executive who is focused on the business operations and processes associated with the [project] would be a likely candidate to act for project success. Ideally, this executive is positioned close enough to the project to have a genuine impact on it."

–Project Management Institute

Effective executives ask questions

- How can I help?
- What is the plan/ the status compared to the plan?
- Are resources being allocated effectively?

© 2019 Carnegie Mellon University

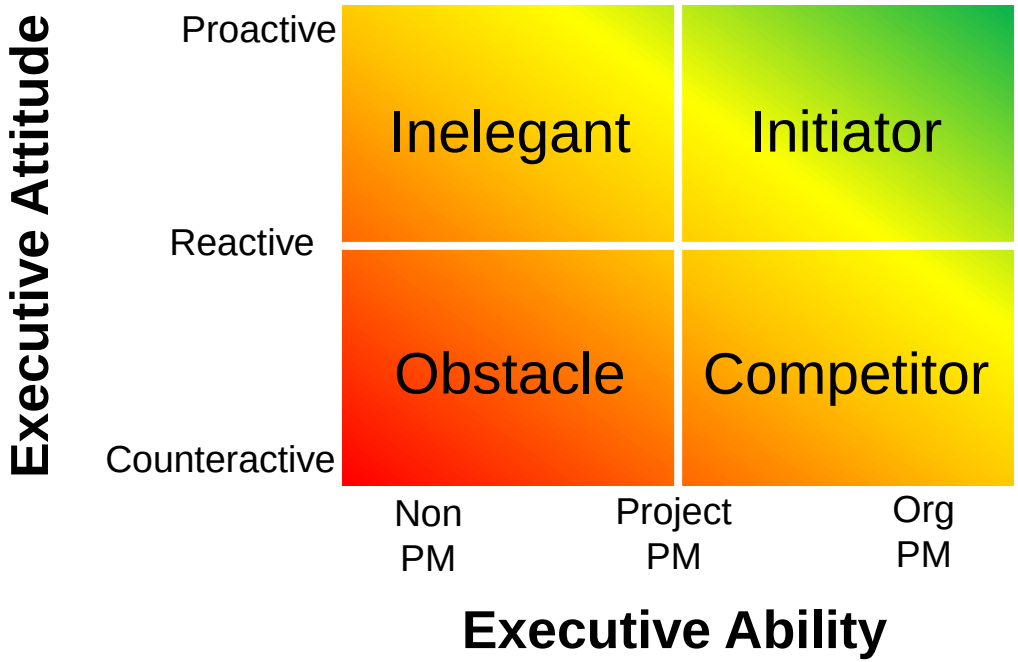
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Gather Governance Support

Remember the risk committees and subcommittees structure

Executives should already be a part of the plan, but if they're not…

Use the Executive Support for Projects Model to determine how to approach an executive for project support



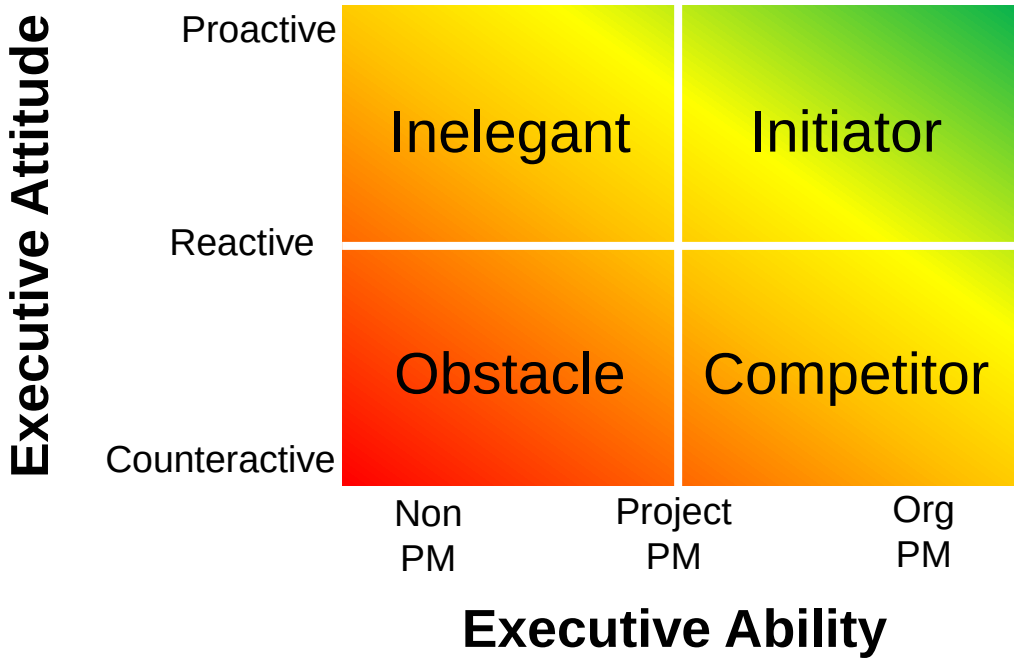
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Classifying Executives' Support

Executive Attitude Axis: how willing is the exec to take action for the project's success?

Executive Ability Axis: The executive's project management ability



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

How should I work with my executive?
Proactive Executives

Initiator: Attitude: Proactive | Ability: Organizational

- Concern for taking actions, knowledgeable of org-specific project management
- Benefit by using full and open communications

Inelegant: Attitude: Proactive | Ability: Non-project management

- Takes action, but poor understanding of project management
- Well-intentioned actions may be ineffective
- Benefit by taking the lead, identifying the actions for the executive to take, and helping the executive take these actions

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

How should I work with my executive?

Counteractive executives

Competitor: Attitude: Counteractive | Ability: Project management skills

- Concern for agendas counter to project success, thorough knowledge of good project management at the organization
- May subjugate your project for the betterment of a competing one
- Benefit from keeping well informed of the executive actions and by looking for a common ground in reducing the level of competition

---

Obstacle: Attitude: Counteractive | Ability: Non-project management

- Concern for agendas counter to project success, little understanding needed for project management
- Likelihood of unpredictable behavior and impact on project success
- Benefit from some insulation from and resilience to the executive, by striking an alliance with a more supportive executive, and from efforts to raise the executive's project management knowledge level

© 2019 Carnegie Mellon University

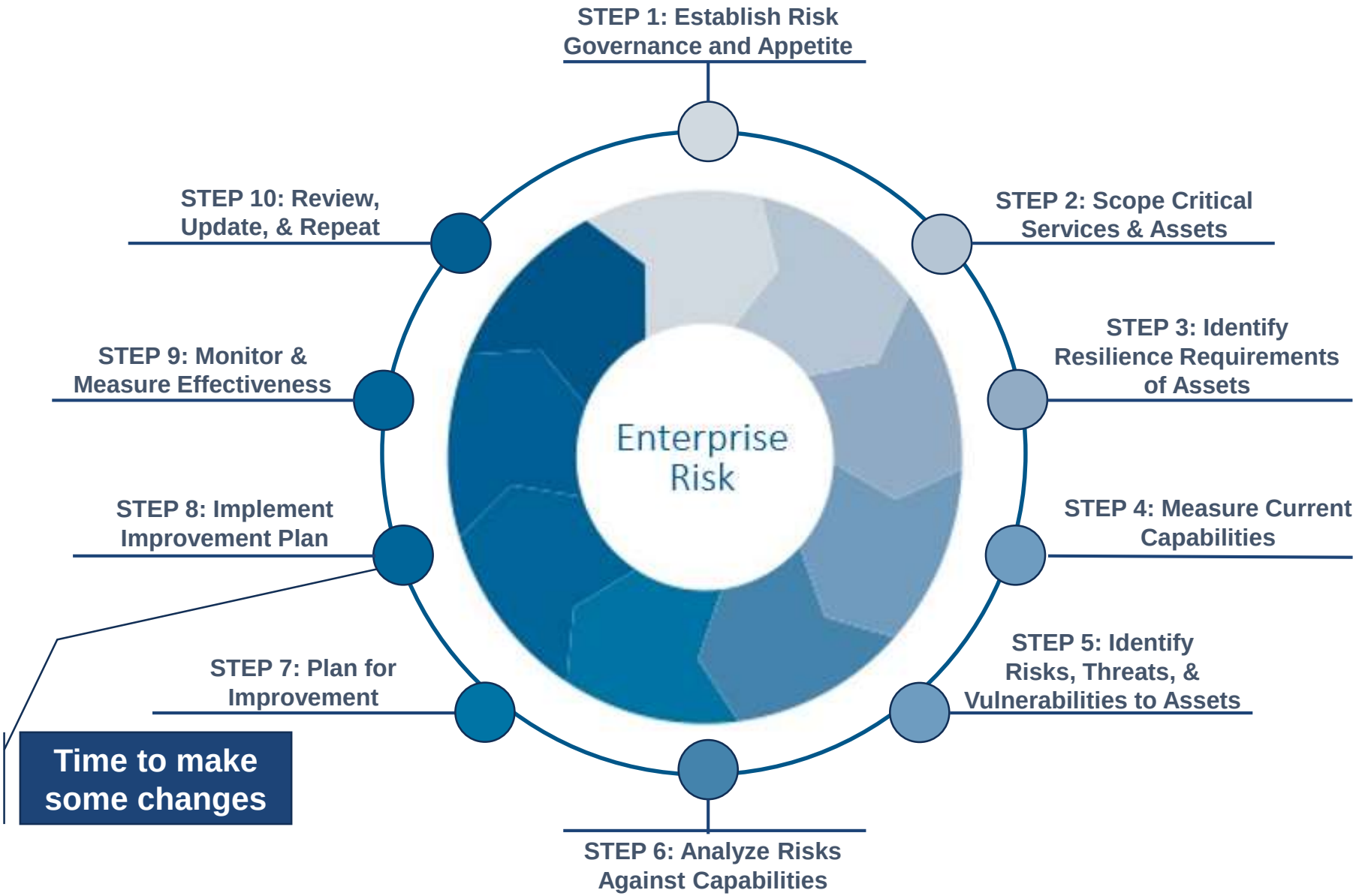
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 8: Implement Improvement Plan

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Where do we go from here?

Once accepted by the governance structure, owners should

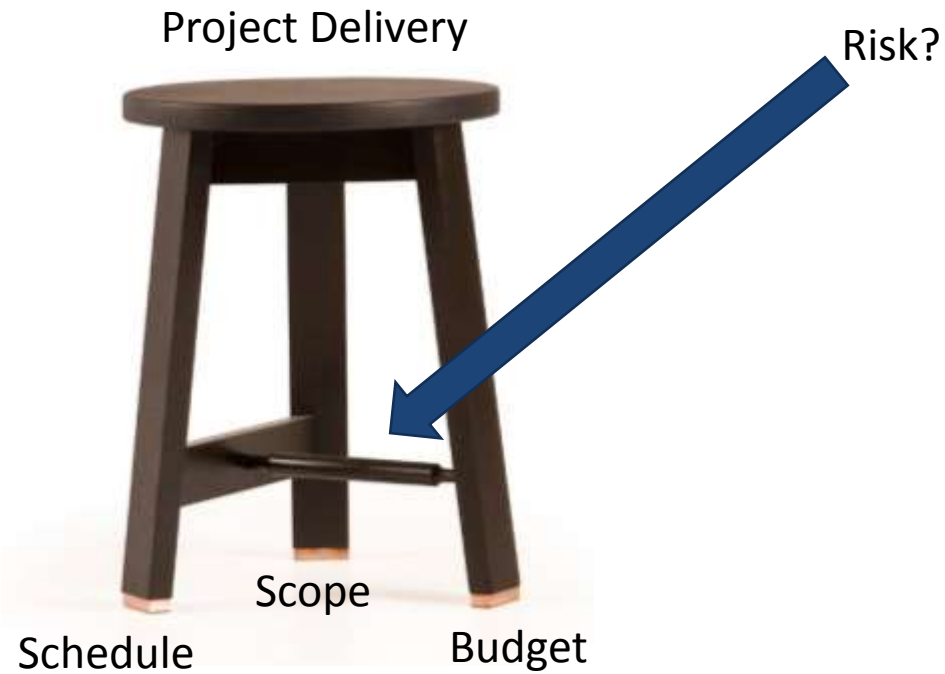
- Establish a chartered project
- Use metrics to measure project delivery
- Establish and measure success criteria
- Set milestones towards project completion

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Setting Project Priorities
The Triple Constraint

- All projects are bound by a concept known as the **"Triple Constraint"**
  - **Scope, Schedule, and Budget**
- It is nearly impossible to alter one of these constraints without affecting another.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Response Plan Implementation
Project Management

Manage each effort as a distinct project

- Scope
- Schedule
- Budget

Regular project reviews with risk owners are crucial

- Frequency of the reviews depend upon complexity and scope

Earned value metrics may be useful

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Response Effectiveness Metrics
You Get What You Measure

Measurement may not be immediately intuitive

Some metrics may focus upon

- Dollars invested
- Change in likelihood of risk
- Change in impact
- Change in risk velocity

Some metrics may examine implementation

- Schedule Performance Index (SPI)
- Cost Performance Index (CPI)

© 2019 Carnegie Mellon University

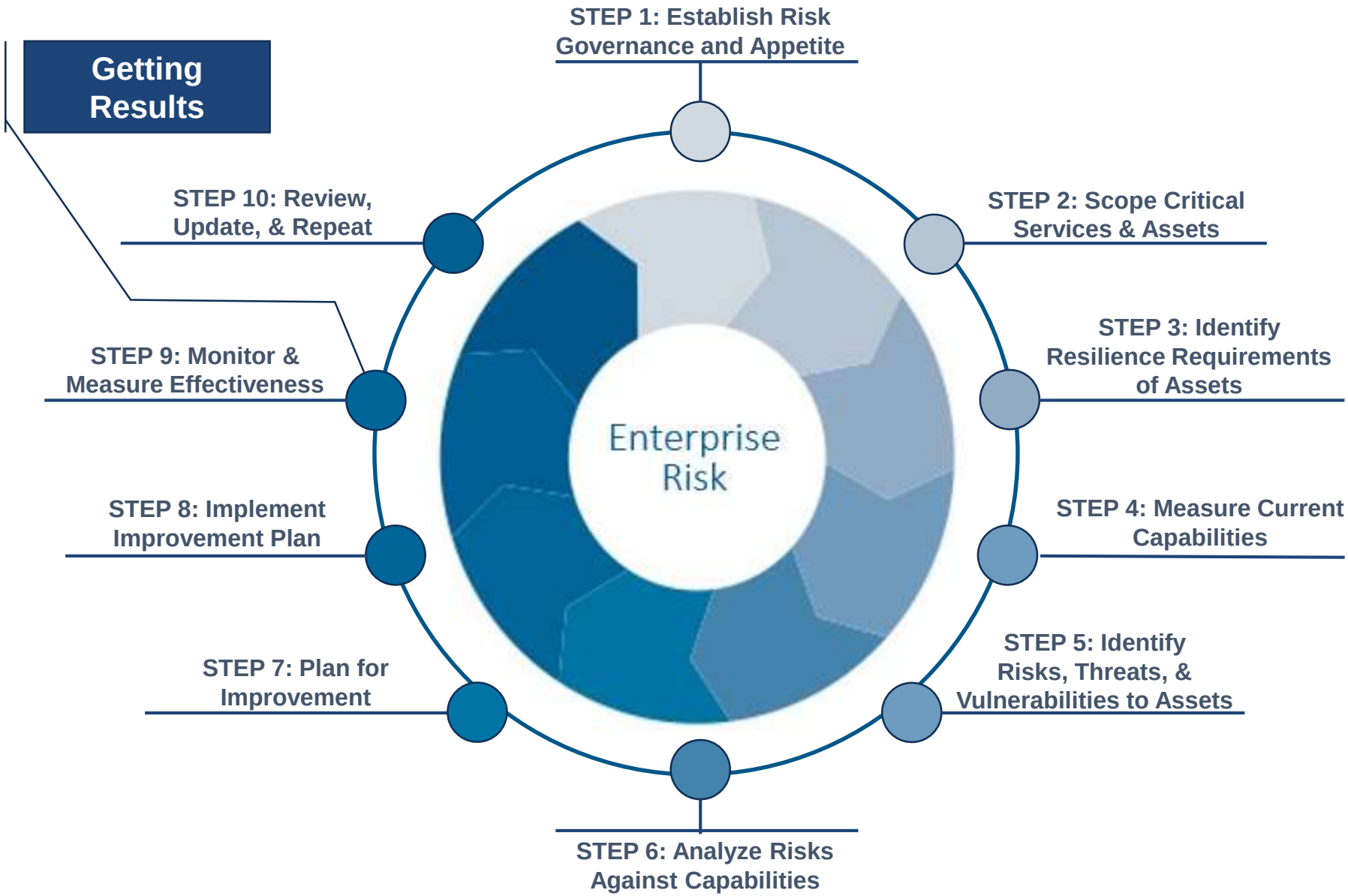
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 9: Monitor and Measure Effectiveness

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

GQIM: Goal Question Indicator Metric
A Method for Developing Metrics

Quantifying the capability of a process to build operational resilience

1. Identify the business objectives that require improved resilience
2. Develop goals for each objective
3. Develop ***quantifiable*** questions whose answers determine the extent to which goals are met
4. Identify information required to answer questions
5. Find metrics that will use selected indicators to answer the questions

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Asking Quantifiable Questions About Your Goals
How Can We Measure Progress Towards Goals

Question what improvements and progress can be measured

- *What percent of employees are responding to our test phishing campaigns?*
- *What percent of employees are entering credentials?*
- *What percent of employees are reporting our test phishing emails to IT security and following standard procedure from the IT security policy?*

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Metrics

How do you measure process improvement?

From our previous example:

Number of employees involved in phishing campaign test

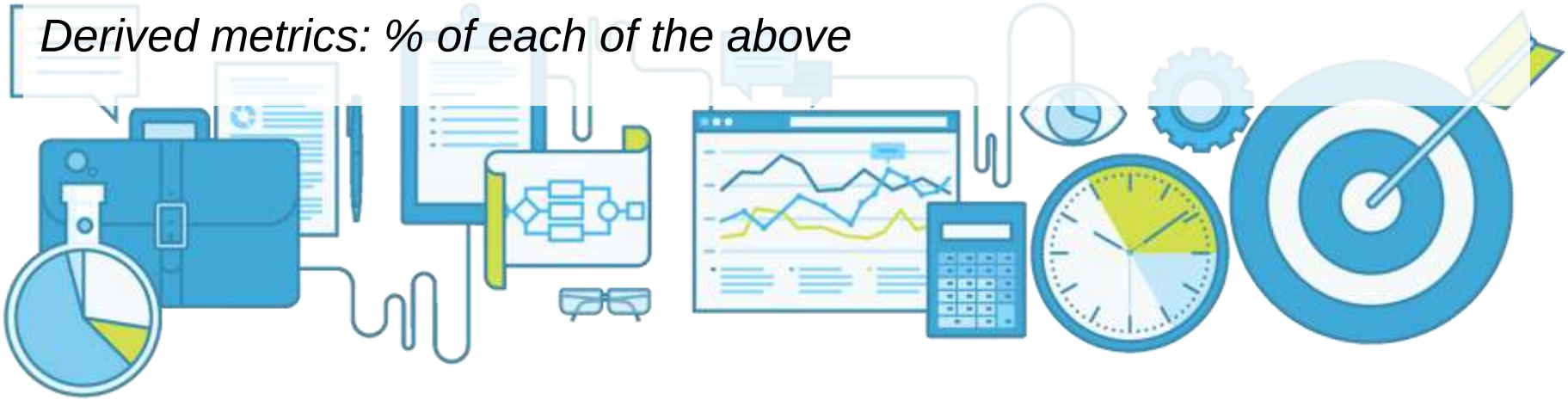
Number of employees that opened/clicked on the suspicious email

Number of employees that were "phished" i.e. entered their credentials on the credential-stealing site

Number of employees that reported the suspicious email

Number of employees that responded in round 2, after retraining

Derived metrics: % of each of the above

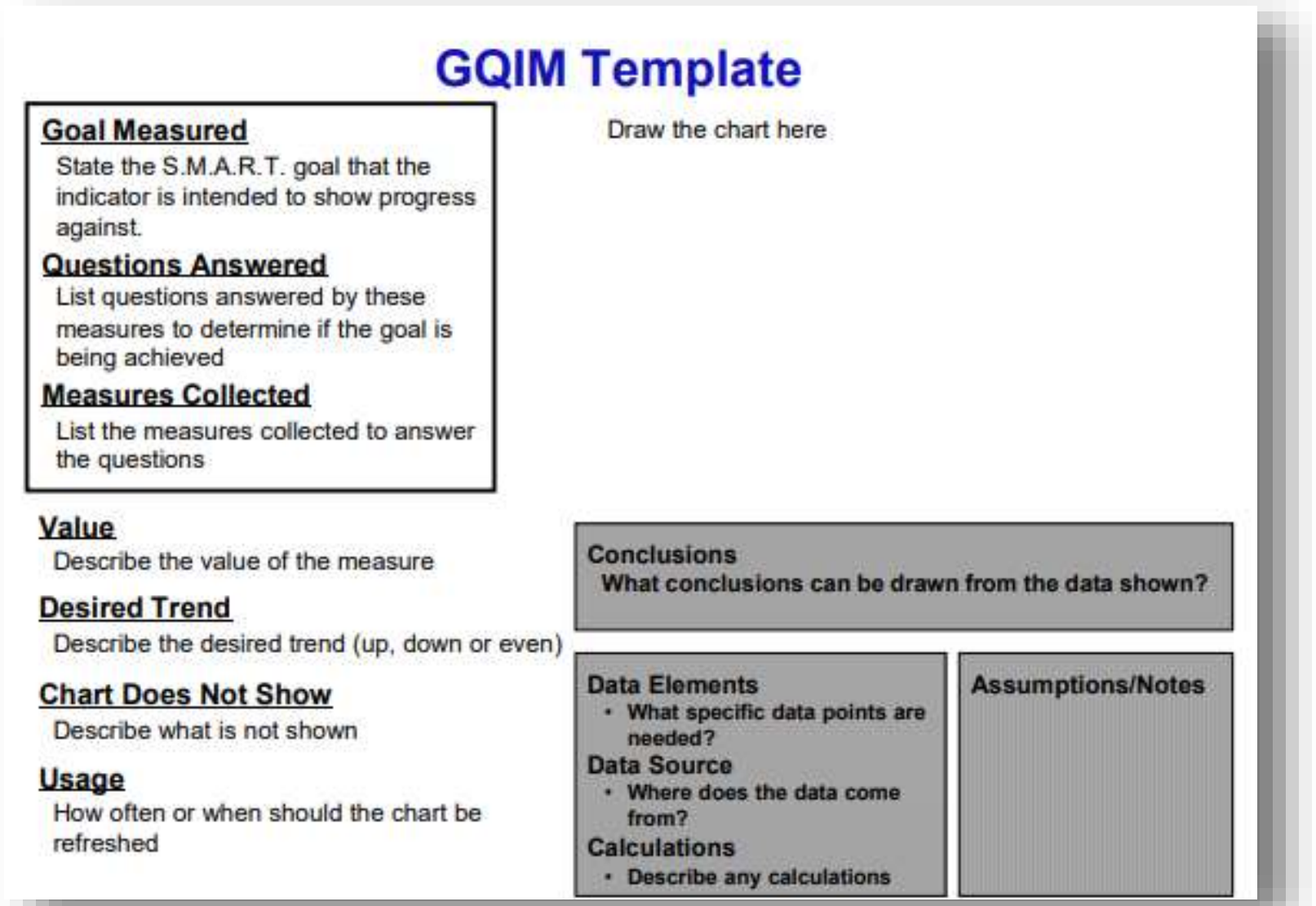


© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

GQIM Template

From The Chicago Software Process Improvement Network

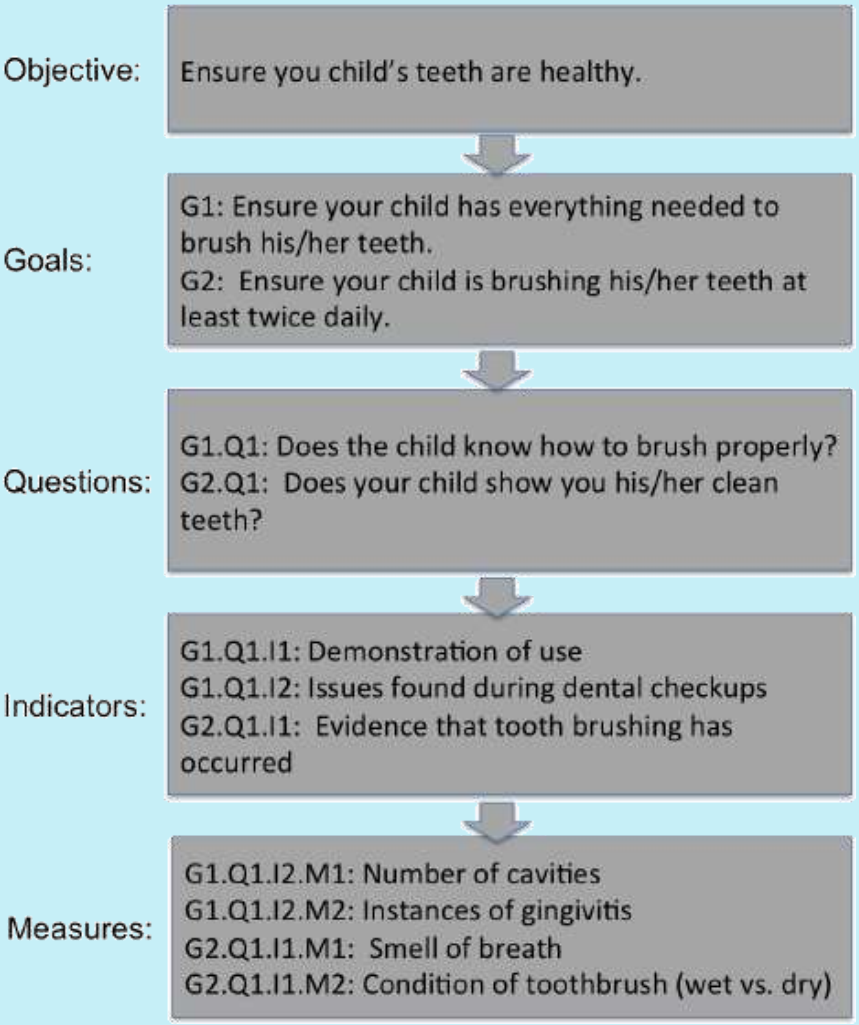


© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

GQIM Example

Courtesy of The IASTED Conference

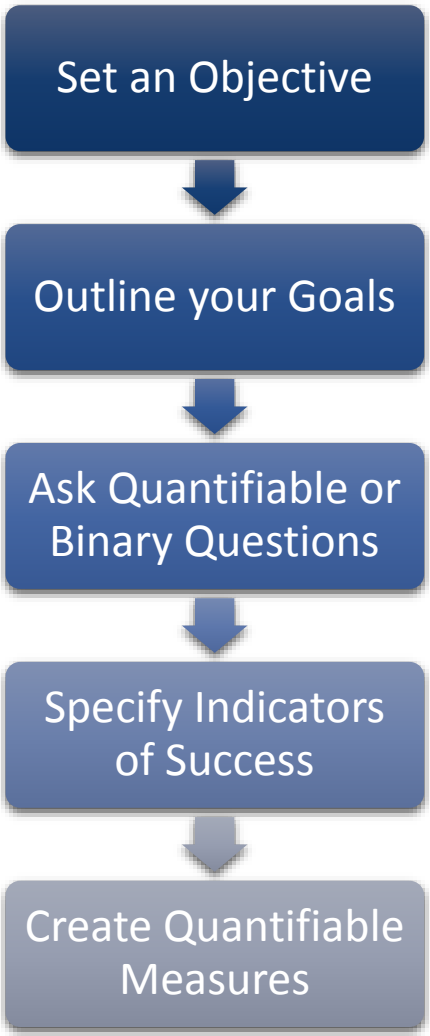


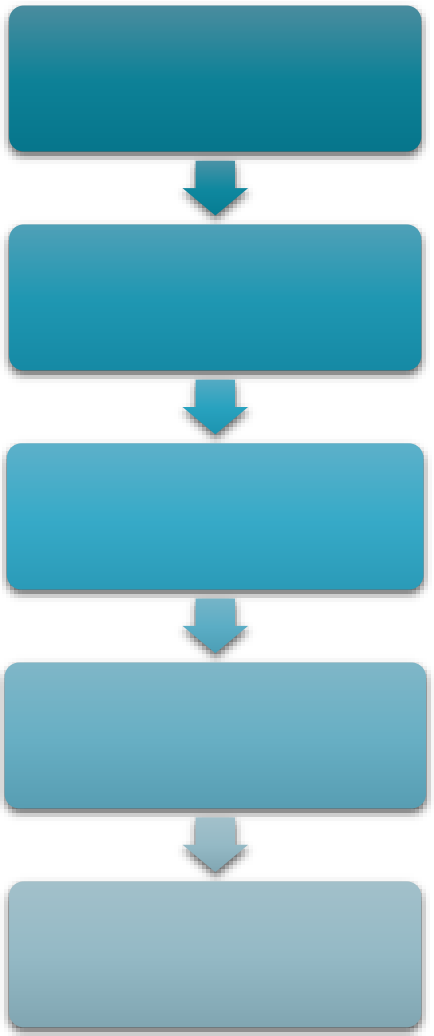
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Now it's your turn…

Create a GQIM Model for Your Program as a Class

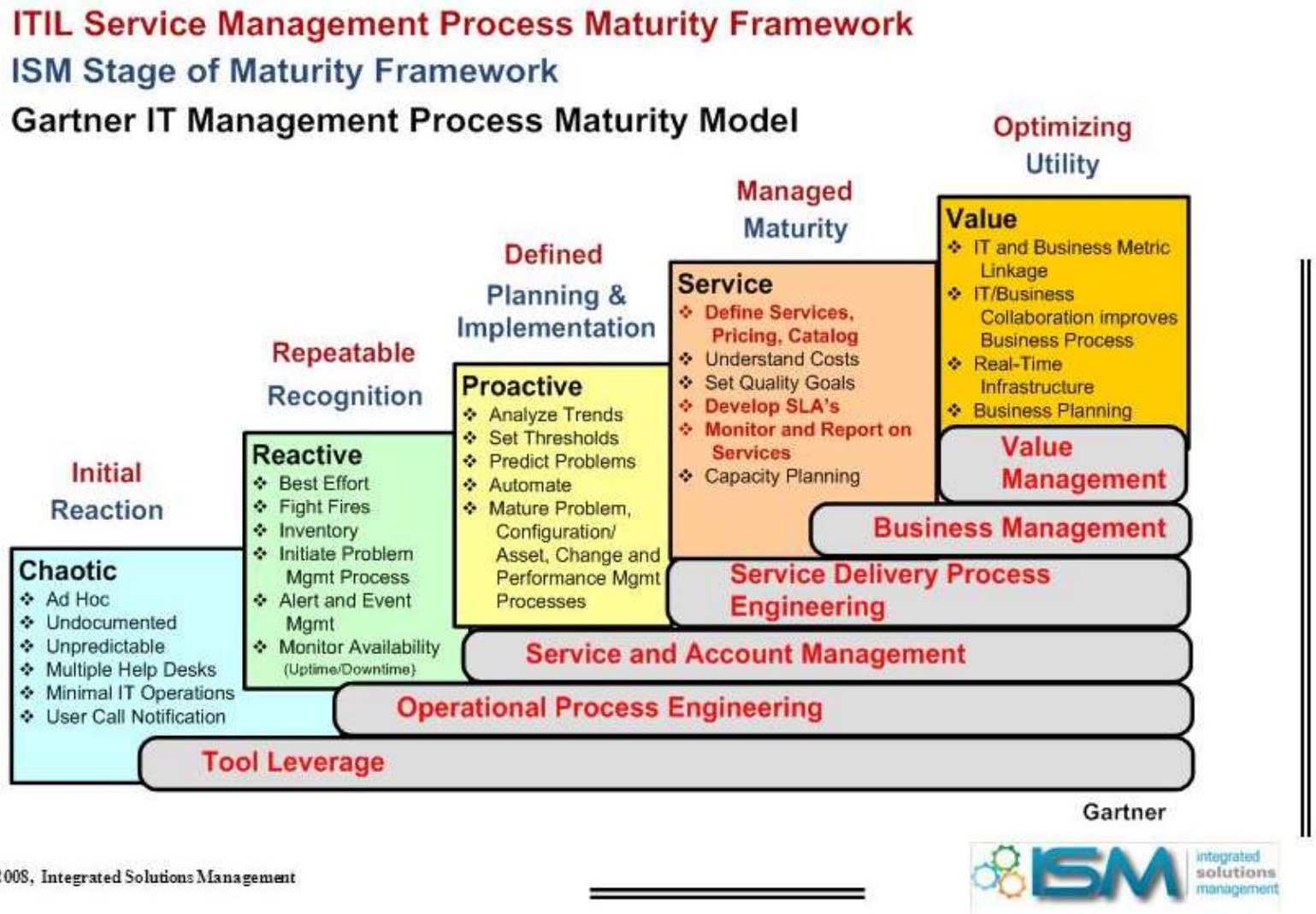




© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Determining Risk Management Maturity



Copyright 2008, Integrated Solutions Management

© 2019 Carnegie Mellon University

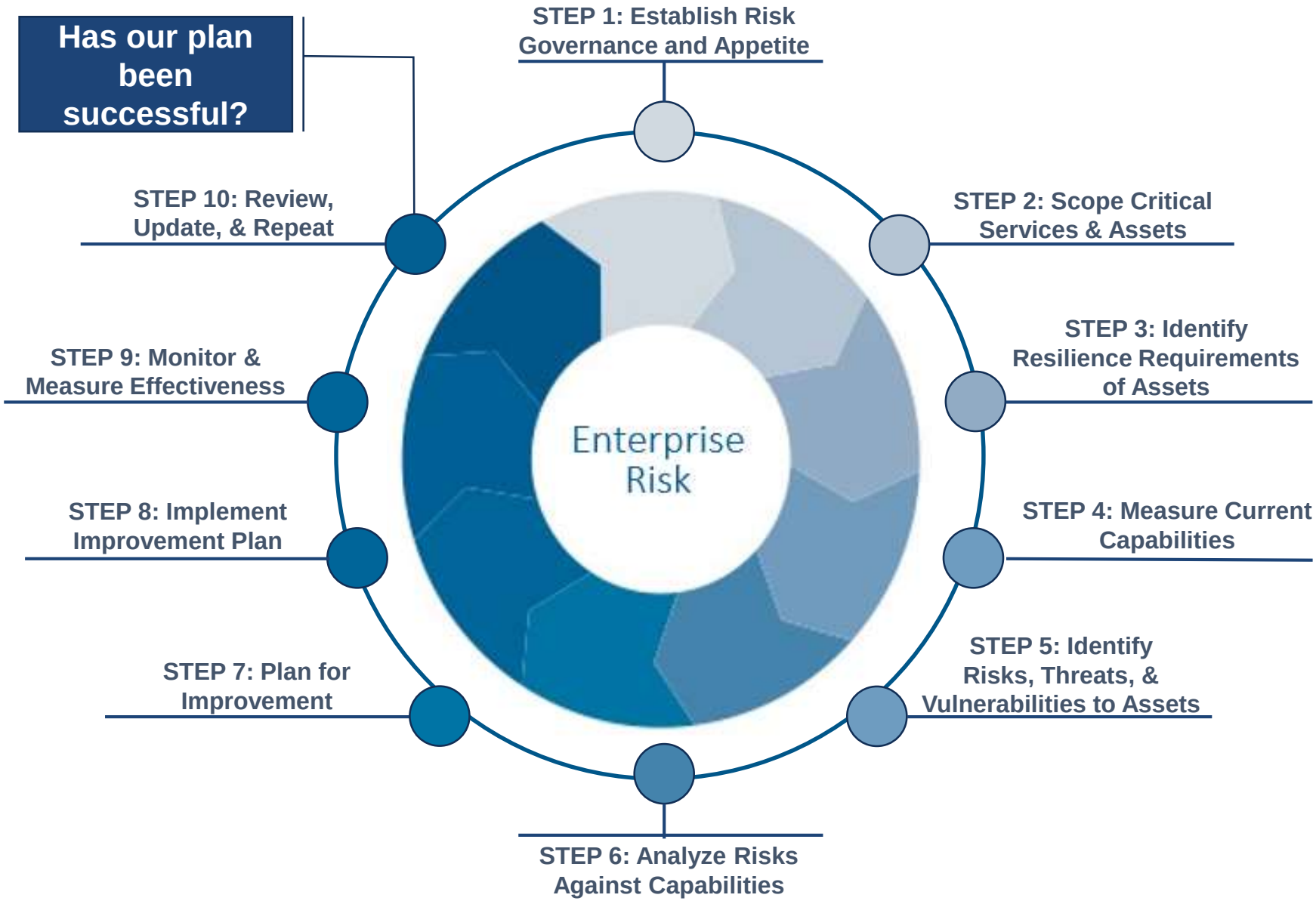
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE: FORTE Process Training

Step 10: Review, Update, & Repeat

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Reviewing Project Effectiveness
The end of the project lifecycle

- Meet with stakeholders and asset managers to ensure the project goals have been met
- Discuss with team members what went well, what didn't, and lessons learned
- Consider what would have been done differently and further improvements

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Measuring Performance
Balanced Scorecard Template

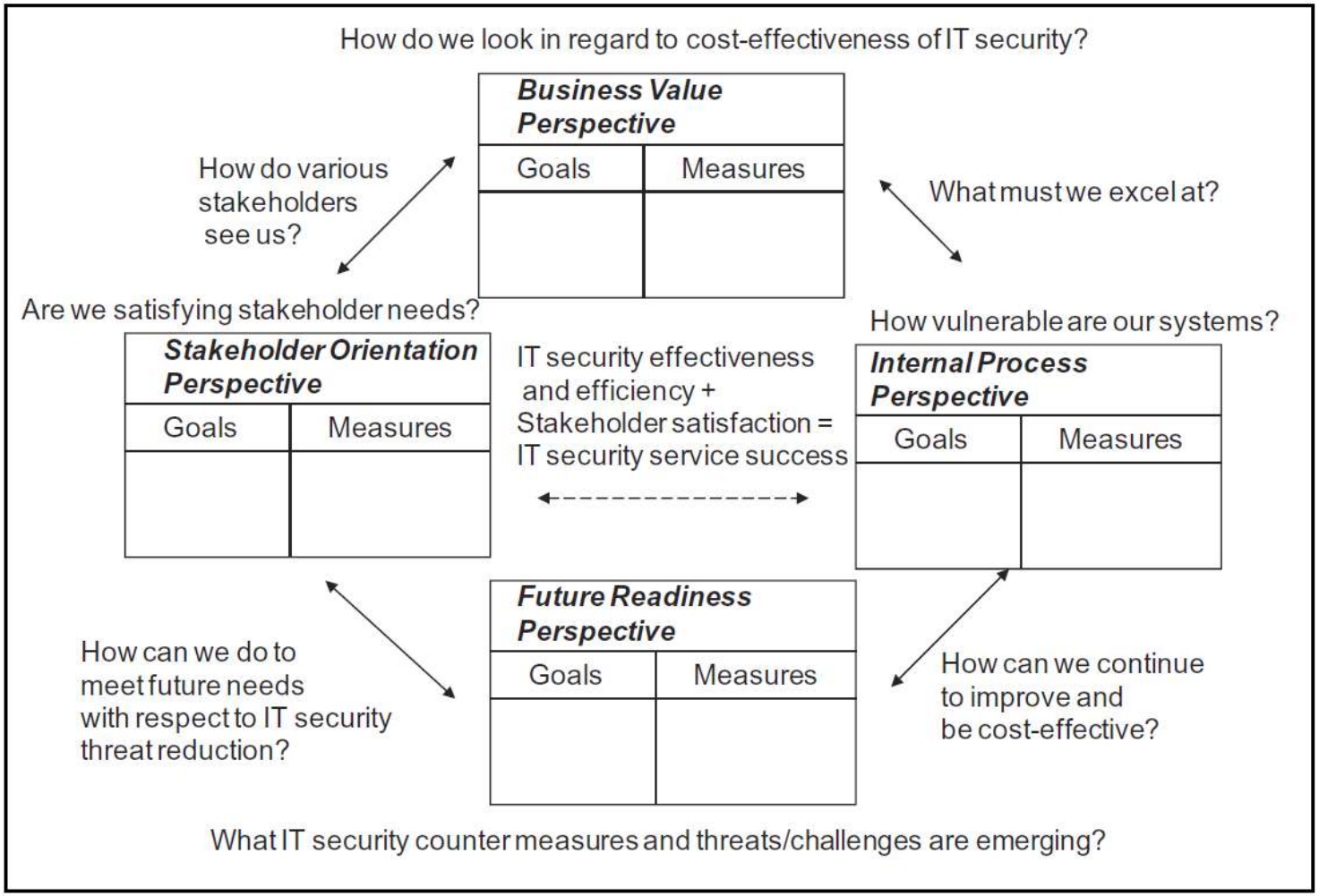


Figure 1: BSC Model for Information Security

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

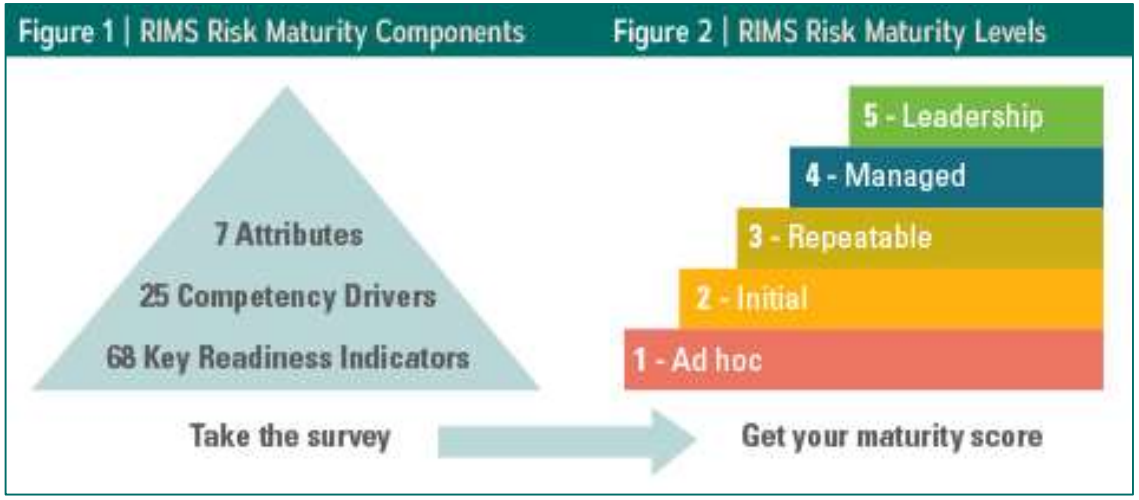
Determining Maturity

How do you know you are doing the right things?

Evolution may follow a maturity model approach

- SEI has a number of resources and tools for measuring capability maturity – RMM, Maturity Indicator Level Scale, etc.
- RIMS maturity assessment

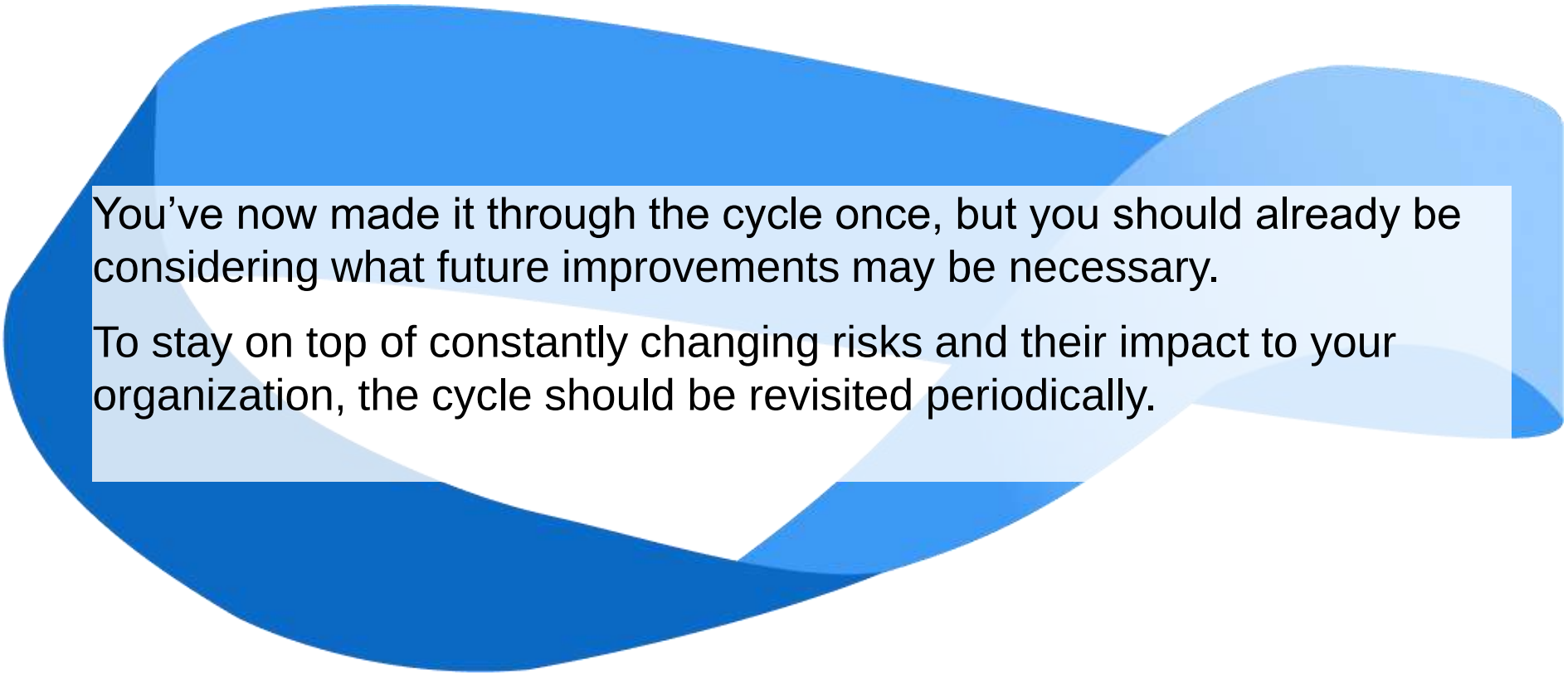
CERT-RMM Capability Level	MIL
Level 0: Incomplete	MIL0: Incomplete
Level 1: Performed	MIL1: Performed
Level 2: Managed	MIL2: Planned MIL3: Managed MIL4: Measured
Level 3: Defined	MIL5: Defined
	MIL6: Shared



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Repeat!
Risk Management Doesn't End



You've now made it through the cycle once, but you should already be considering what future improvements may be necessary.

To stay on top of constantly changing risks and their impact to your organization, the cycle should be revisited periodically.

Discussion: How often should the cycle be revisited?

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Contact Information

Presenter / Point of Contact

Brett Tucker
Technical Manager
Cyber Risk Management
Telephone: +1 412.268.6682
Email: batucker@sei.cmu.edu

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.