MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

METRICS THAT MATTER: INCIDENT MANAGEMENT

Jason Fricke

Senior Cyber Security Engineer

CERT Program, Software Engineering Institute, Carnegie Mellon University

Katie Stewart

Senior Engineer

CERT Program, Software Engineering Institute, Carnegie Mellon University

Session Objectives

Learn how to develop meaningful metrics that drive action within an organization

See a set of case studies around developing meaningful metrics for incident management

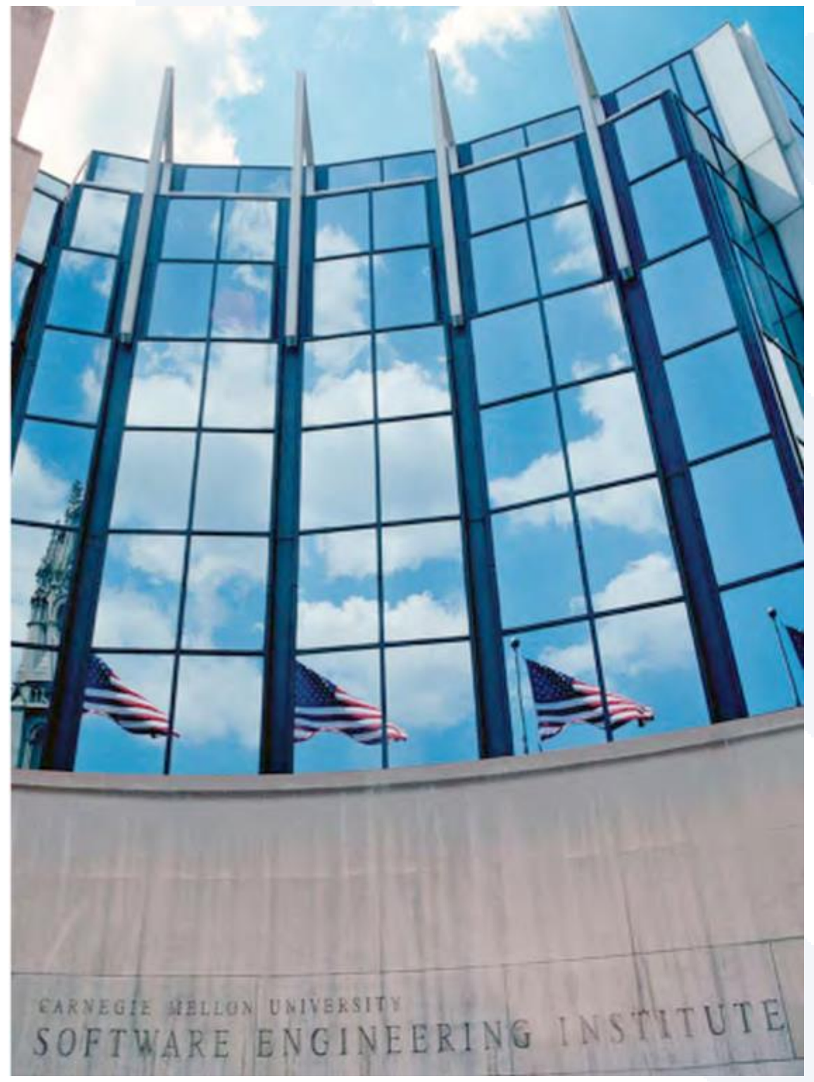
Understand how to leverage metrics to drive workforce efficiencies

Hear an example of meaningful metrics for incident management

Receive the steps needed to develop meaningful metrics within the enterprise

"[Distribution Statement A] Approved for public release and unlimited distribution."

Who we are



Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at SEI
- Focused on information security, insider threat, operational risk management, security metrics, and governance

First things first – Why measure?

If what you are measuring doesn't drive action, consider if it should be measured at all.

Demonstrate that your security program has measurable business value

Provide data for decision making

Answer key strategic questions

Demonstrate that your control objectives are (and continue to be) met

Justify new investments and to show improvement

"[Distribution Statement A] Approved for public release and unlimited distribution."

Designing a meaningful metric

Who is the metric for?

What is being measured?

Where is the data/information stored?

When/how frequently are the metrics collected?

Why is the metric important?

How is the data collected and used?

Attributes of a meaningful metric

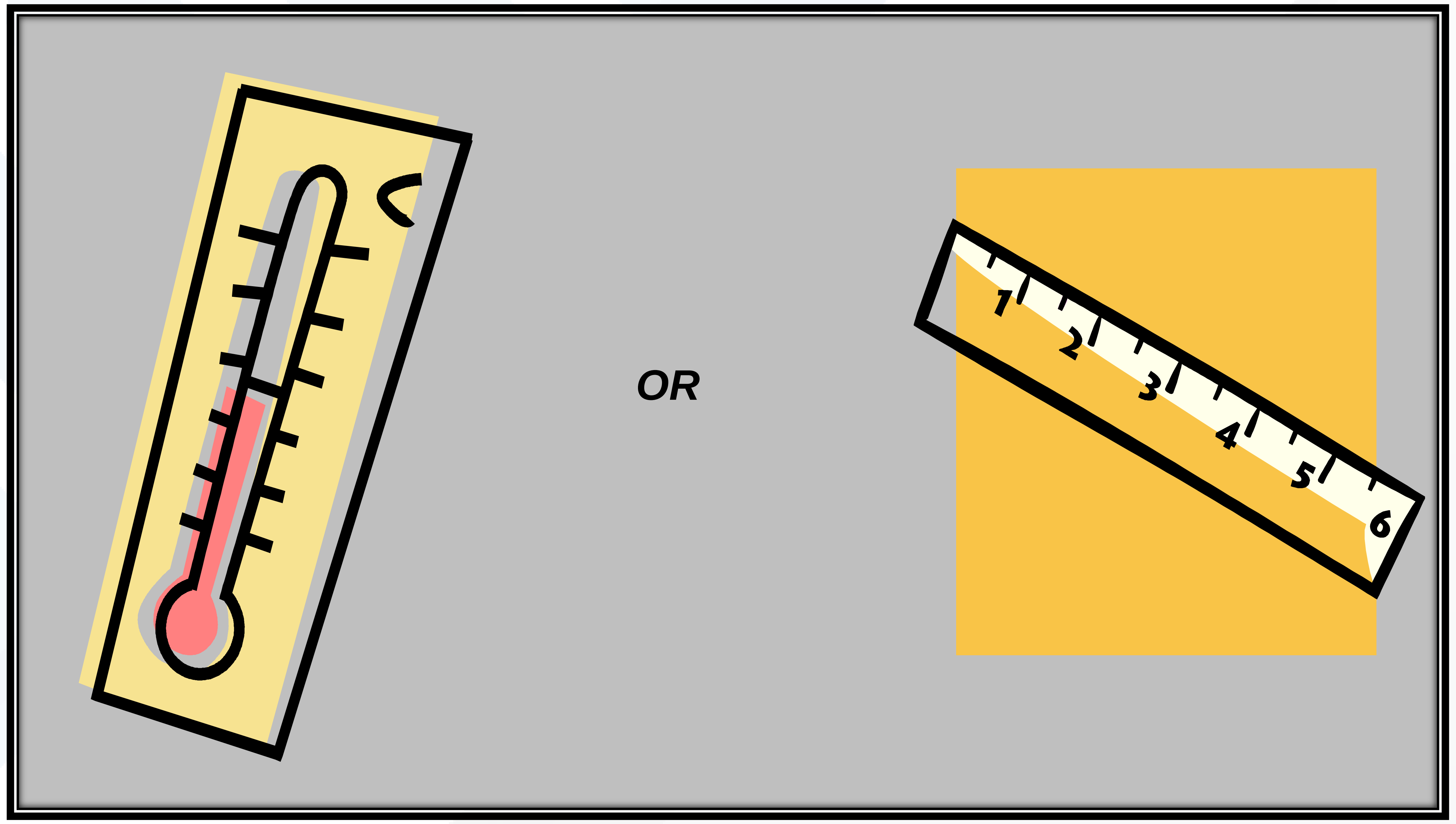
Accurate

Precise (Enough)

Timely

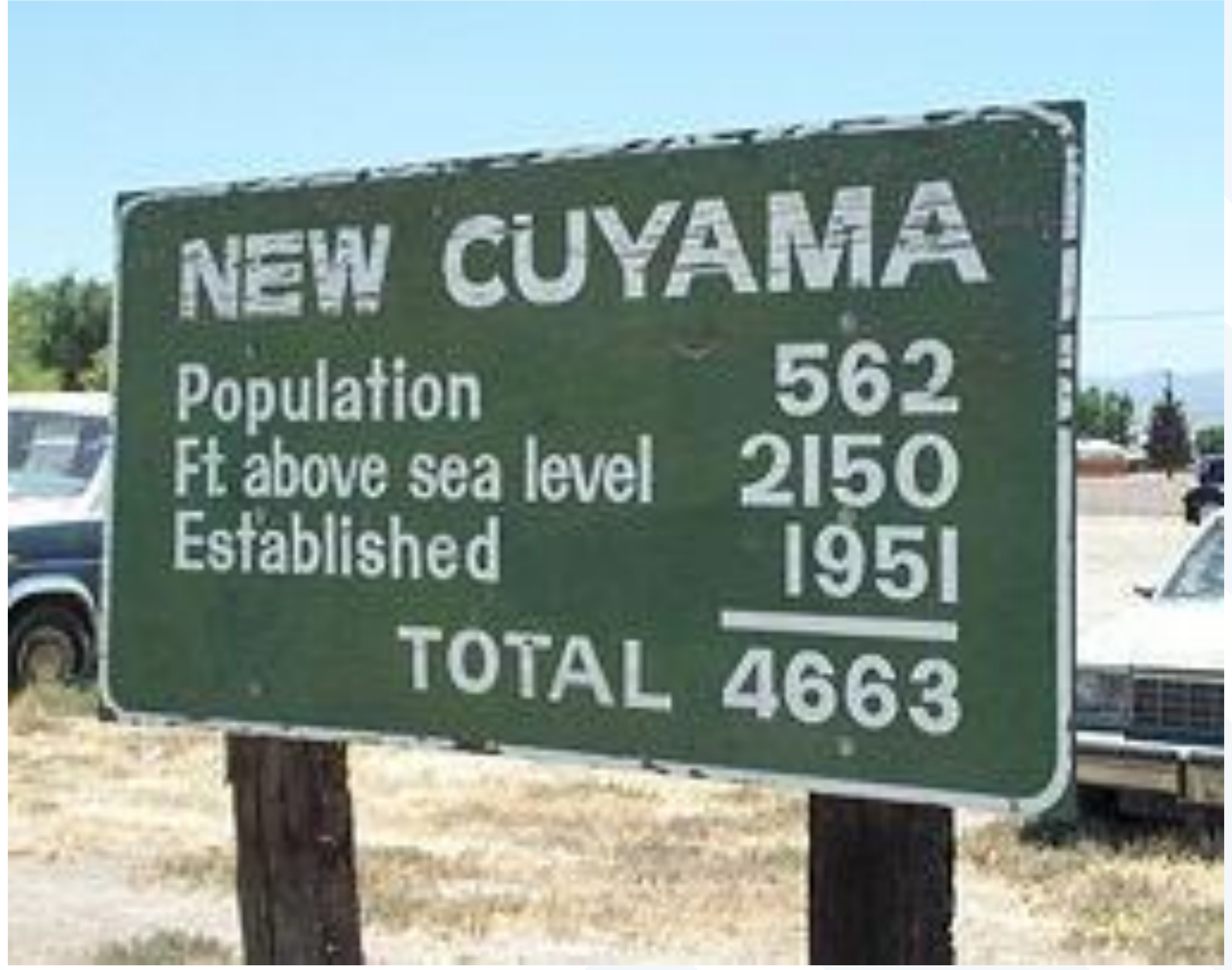
Objective

Cost Effective



Why is measurement so hard?

In short, we aren't asking the right questions.



What do I want to know or learn?

What decisions do I want to inform?

What actions do I want to take?

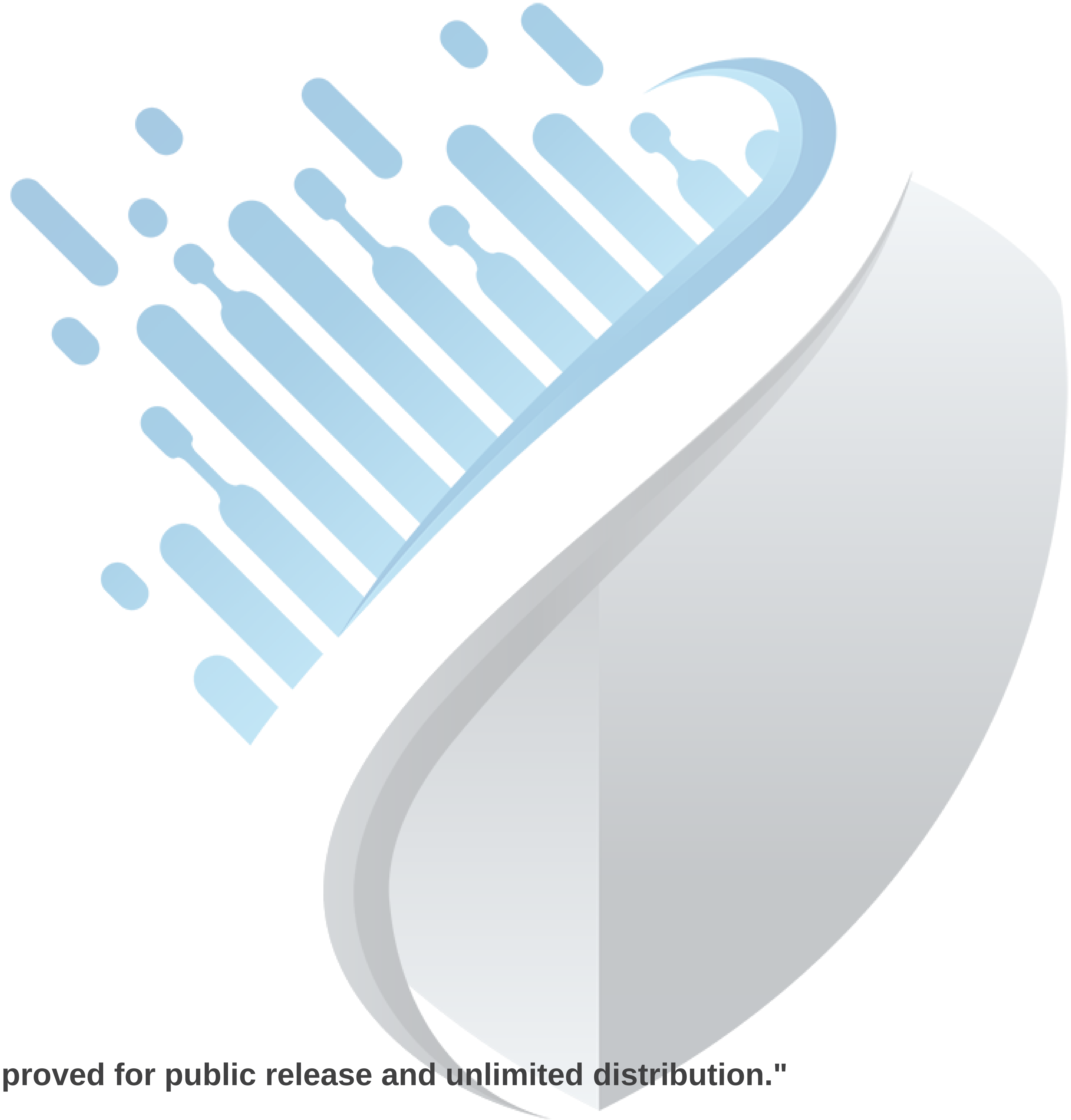
What behaviors do I want to change?

Informed by Douglas Hubbard, How to Measure Anything, John Wiley & Sons, 2010

InfoSecWorld Conference & Expo 2018

"[Distribution Statement A] Approved for public release and unlimited distribution."

WHAT WE HEARD



"[Distribution Statement A] Approved for public release and unlimited distribution."

Cybersecurity Operations Center (CSOC) Good Practices Project

Characterize multiple CSOCs in order to identify good practices and (recognized) deficiencies

- Infrastructure
- Organizational structure
- Personnel
- Processes

What makes a CSOC a good, well-performing CSOC?

CSOC Good Practices Project

Approach

- Conduct in-depth interviews with CSOC leaders
- Seven topical areas determined to be critical to the accurate characterization of a CSOC's structure and functions

Demographics

- Eight organizations across four sectors
- Organizations ranged in size from 8,000 - 650,000 employees
- Six to 700 CSOC/CSOC supporting personnel

"[Distribution Statement A] Approved for public release and unlimited distribution."

CSOC Good Practices Project: Findings

All organizations are struggling with metrics

- Regulatory requirements
- No coordination with leadership

Quality Control (QC)

- Metrics are needed
- QC is difficult to measure

“We aspire to measure a lot of things.”

CSOC Good Practices Project: Conclusions

Standard metrics are important…

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)

***but*, more sophisticated metrics are needed**

- Process improvements
- Automation and efficiencies

"We want [to develop] performance metrics."

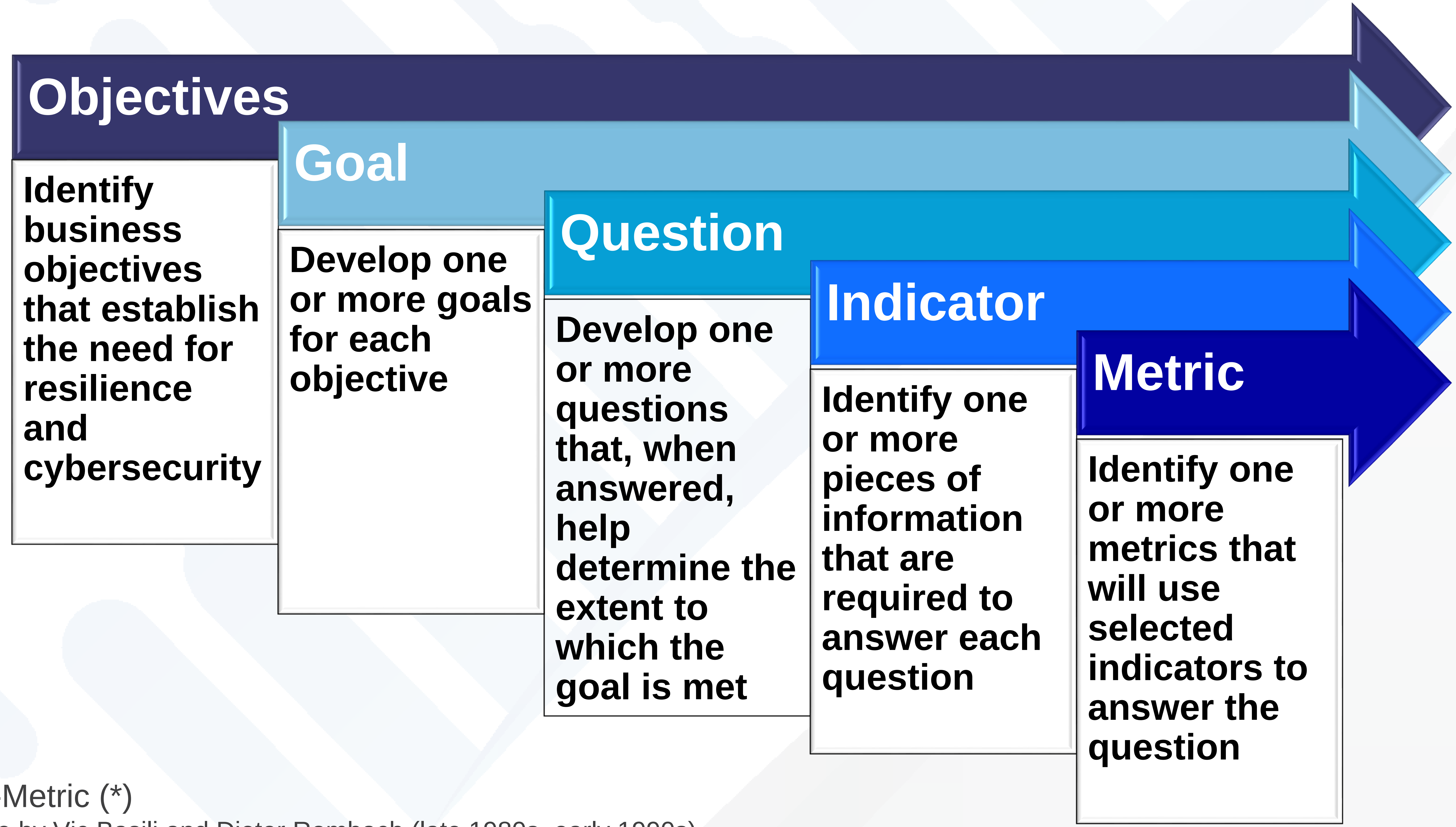
"[Our metrics are] very immature."

"[Distribution Statement A] Approved for public release and unlimited distribution."

Goal
Question
Indicator
Metric

"[Distribution Statement A] Approved for public release and unlimited distribution."

The GQIM Process



Objectives

Identify business objectives that establish the need for resilience and cybersecurity

Goal

Develop one or more goals for each objective

Question

Develop one or more questions that, when answered, help determine the extent to which the goal is met

Indicator

Identify one or more pieces of information that are required to answer each question

Metric

Identify one or more metrics that will use selected indicators to answer the question

Goal-Question-Metric (*)

- Early work done by Vic Basili and Dieter Rombach (late 1980s, early 1990s)

Goal-Question-Indicator-Metric (*)

- SEI work in software engineering (late 1990s, early 2000) and operational resilience (2010 to present)

"[Distribution Statement A] Approved for public release and unlimited distribution."

GQIM for Incident Management

"[Distribution Statement A] Approved for public release and unlimited distribution."

Example: Incident Management Objective to Goals

Objectives	Goals
Restore the service as quickly as possible and minimize disruption	Improve the process for investigation of incidents
	Improve the process for remediation of incidents
	Increase automation for incident investigation and remediation
Manage the incident during its entire lifecycle	Improve the reporting process for events/incidents
	Improve the process for detection of events
	Improve the process of hand-off/escalation of incidents

Objectives and Goals derived from ITIL

Example: Incident Management Goals to Questions

Goal	Questions
Improve the process for detection of events	Is there a defined process for the detection of events?
	Is the process for detection of events documented?
	Do we have tools for event detection?
	Are events being detected?
	Are there events not being detected?
	Is there a tool for reporting events?
	Is the information for detected events documented?
	Is staff trained on detecting events?

Example: Incident Management Questions to Indicators

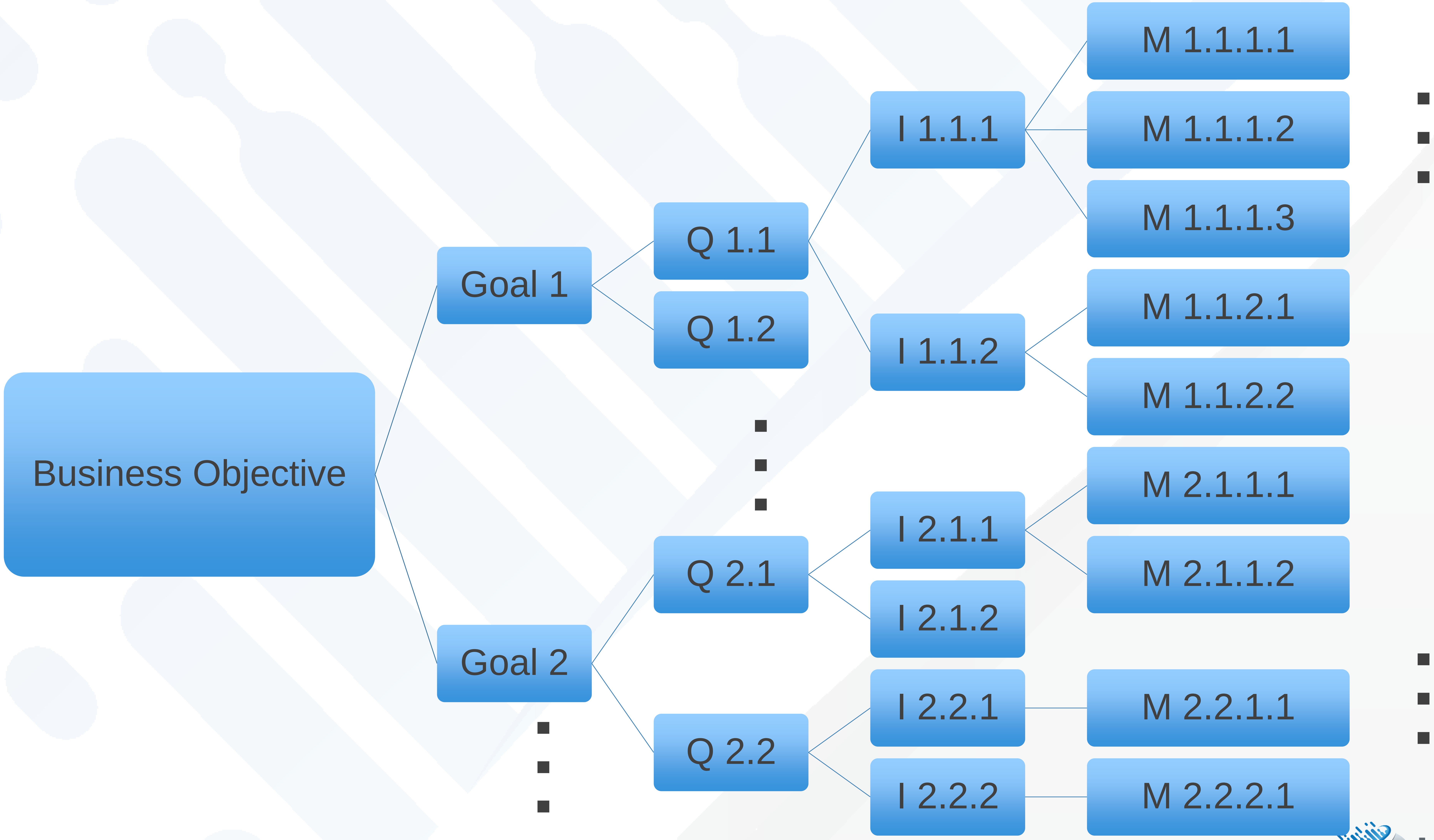
Question	Indicators
Do we have tools for event detection?	Tools Inventory
	Tool requirements for event detection are documented
Are there events not detected?	Late detection is indicated
	New alerts
	Gaps in investigation capabilities
Is the information for detected events documented?	There is a defined template for event reports
	Tickets are created/reviewed

"[Distribution Statement A] Approved for public release and unlimited distribution."

Example: Incident Management Indicators to Metrics

Indicators	Metrics
Tools inventory	Elapsed time since the tools inventory was updated
Tool requirements for event detection are documented	% of unfulfilled requirements for tool detection
	% of tools generating expected reports
	Number of out of date/unauthorized tools in operation
Late detection is indicated	Number of events that are detected “late”
New Alerts	Number of events that were not previously considered suspicious
Tickets are created/reviewed	% of tickets that get flagged in Q/A

GQIM Visual Example



"[Distribution Statement A] Approved for public release and unlimited distribution."

Iterate, Iterate, and Iterate

Put yourself in the role of the decision maker

“If I have this metric, will I have a better understanding of progress (or not) toward achieving my goals and objectives?”

Will this metric help me answer one or more of these questions:

- What decision(s) or action(s) needs to be made? By whom?
- Are we improving or getting worse? Why?
- Do I need to keep collecting this metric?

Collect, interpret, refine, improve

Technical vs. Process Metrics

Technical metrics

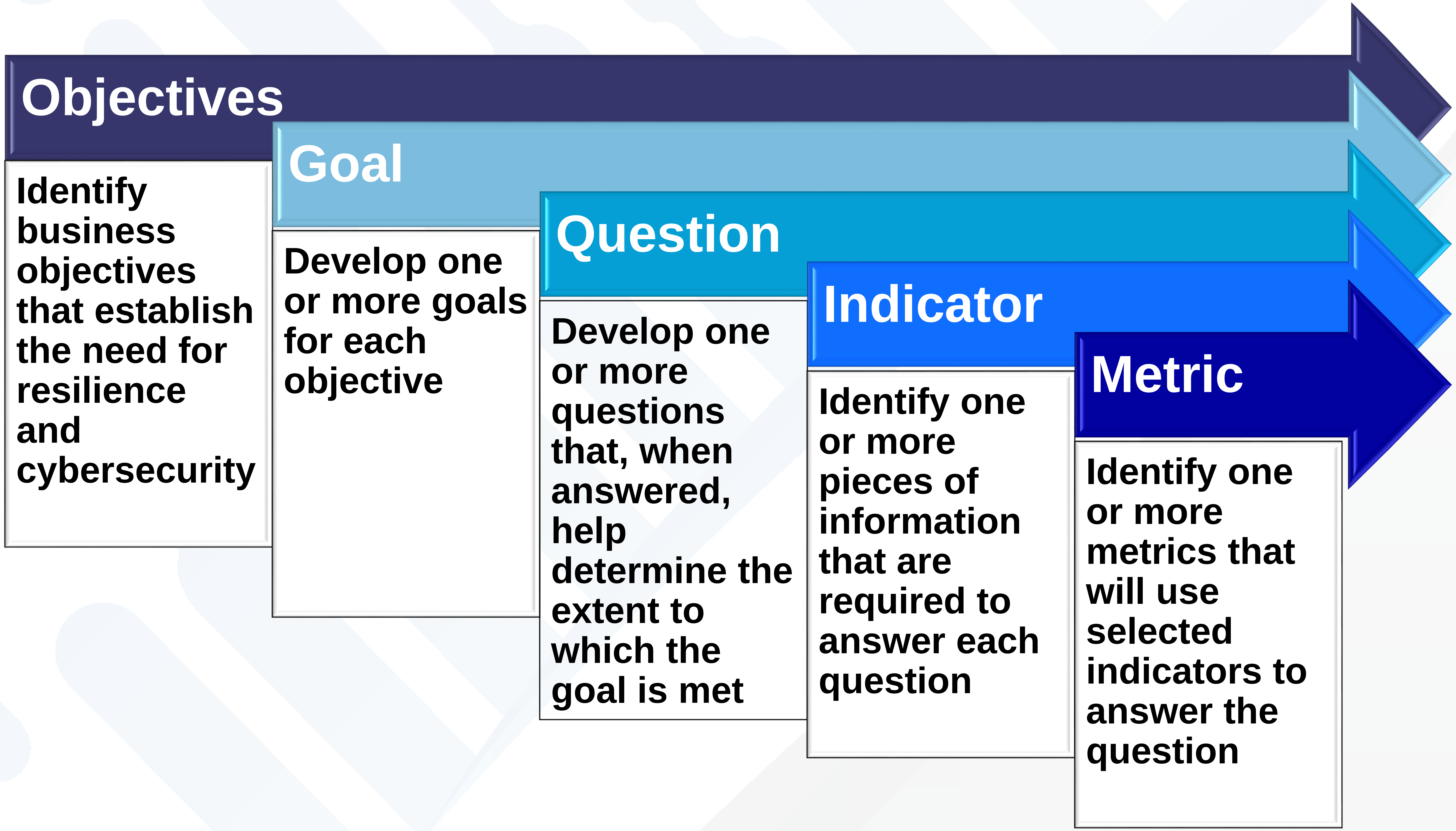
Measure controls implemented through technology

Process metrics

Measure a series of activities and tasks that produce a work product or that lead to a particular outcome

- Implementation
- Effectiveness
- Process Performance

The GQIM Process



Objectives

Identify business objectives that establish the need for resilience and cybersecurity

Goal

Develop one or more goals for each objective

Question

Develop one or more questions that, when answered, help determine the extent to which the goal is met

Indicator

Identify one or more pieces of information that are required to answer each question

Metric

Identify one or more metrics that will use selected indicators to answer the question

"[Distribution Statement A] Approved for public release and unlimited distribution."

CSOC Good Practices Project: Next Steps

Interview additional organizations

- Volunteers?
- Contact Katie (kcstewart@cert.org) or Jason (jfricke@cert.org)

Approach

- Qualitative → Mixed Methods (Exploratory Sequential/Sequential Explanatory)
- Case studies

Measurement Resources

- CERT Podcast: Measuring Operational Resilience
  https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34512
- CERT-RMM Measurement & Analysis website
  http://www.cert.org/resilience/research/resilience-measurement-and-analysis.cfm
- Allen, Julia; Curtis, Pamela; Gates, Linda. *Using Defined Processes as a Context for Resilience Measures* (CMU/SEI-2011-TN-029). Software Engineering Institute, Carnegie Mellon University, October 2011.
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9887
- Allen, Julia & Curtis, Pamela. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, June 2011.
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=10017
- [Allen 2010] Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, September 2010.
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9401
- Hayden, Lance. *IT Security Metrics*. McGraw-Hill Education, 2010.
- Hubbard, Douglas. *How to Measure Anything*. John Wiley & Sons, 2007.

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

"[Distribution Statement A] Approved for public release and unlimited distribution."