Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 NOV 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Measuring What Matters	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
; ; Stewart /Julia Allen KatieValdez /MichelleYoung /Lisa	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**130**	

Measuring What Matters

ISACA Information Security Risk Management Conference
November 18, 2014
Measurement Workshop
Topic 1 Context

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0001662

Workshop agenda

Topic 1	Set context
Topic 2	Select objectives
Topic 3	Goal-Question-Indicator-Metric (GQIM) overview
Topic 4	Objectives to goals
Topic 5	Goals to questions
Topic 6	Questions to indicators
Topic 7	Indicators to metrics
Topic 8	The big picture: putting it all in context

Topic 1: Set context

Objectives and expectations

Organizational challenges

Why do you want to measure?

Measurement defined

Getting started

Deriving metrics from objectives

- Introduction to the Goal-Question-Indicator-Metric (GQIM) method

Objectives and Expectations

Workshop abstract

It is critical to measure the right things in order to make better-informed decisions, take the appropriate actions, and change behaviors. But how do senior leaders and managers figure out what those right things are?

Public and private organizations today often base cyber risk management decisions on fear, uncertainty, and doubt (FUD) and the latest attack; compliance mandates such as HIPAA, FISMA, SOX and PCI; and security risk frameworks that typically have little to do with the way the rest of the organization measures risk and prioritizes operational risk management activities.

CFOs, Enterprise Risk Management Officers, Internal Audit Directors, and CISOs need information risk management approaches that align with business objectives.

A measurement approach tied to strategic and business objectives ensures that planning, budgeting, and the allocation of operational resources are focused on what matters most to the organization. In addition, a shift to such an approach helps to identify metrics that are expensive to collect and may not be worth the investment.

Participants in this workshop will use their real world business objectives to develop applicable goals, questions, indicators, and actionable metrics that they can take back to their organization to improve their ability to manage operational risk and resilience.

Learning objectives

1. Participants are expected to provide one or more business objectives from which metrics will be derived. Based on a defined business objective, select a few essential goals that are required to achieve this objective.
2. Formulate one or more questions for each goal in learning objective 1. The answers to these questions help determine the extent to which the goal is being achieved.
3. Identify one or more indicators for each question. An indicator is data and information that are used to answer each question.
4. Using indicators, determine what number, percentage, mean or other metric can help answer each question.
5. Understand the elements of a measurement program and how to get one started.

Confidentiality & non-attribution agreement

In order to support free and open communications, the following provisions are agreed:

1. All information gathered through or derived from any materials, discussions, or interviews will be treated by all participants as confidential.
2. No information gathered through or derived from any materials, discussions, or interviews will be discussed or reported to anyone who did not attend the measurement workshop with attribution to individuals or organizations without the explicit permission of those individual or organizations.

Workshop expectations

This session

- does not cover specific technical security metrics
- does cover strategic metrics and their importance

Why you might want to stay for this session anyway -

if you are interested in

- determining what to measure in support of business objectives
- identifying risks and gaps in your current measurement processes
- selecting and implementing practices and controls tied to business objectives
- a method for developing metrics that will help you do these things

Why are you here?

What if I don’t have any strategic objectives?

Organizational Challenges

Operating under risk and uncertainty

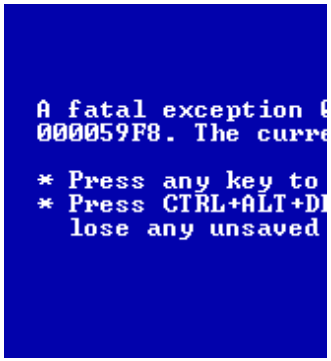
Operational risk

A form of risk emanating from day-to-day business operations

The potential failure to achieve mission objectives

Typically categorized as follows:

Inadvertent or deliberate actions of people



Systems and technology failures

Failed internal processes

External events

Is there an upside to operational risk?

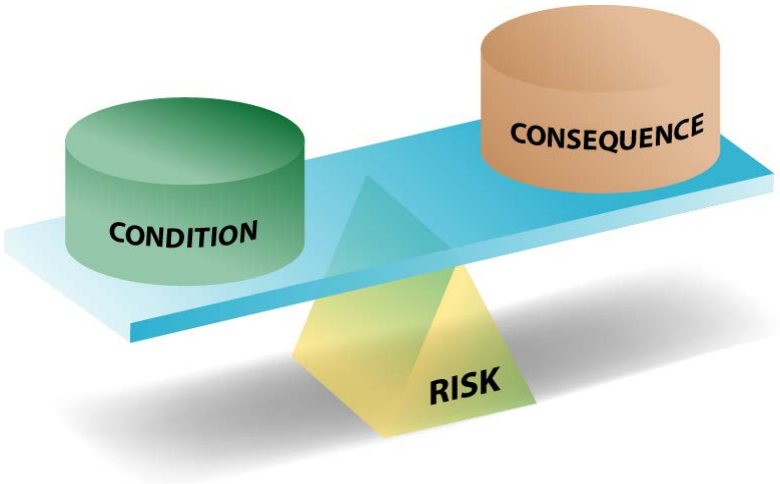
Market risks and credit risks have the possibility of an upside, or reward, to accepting the risks

Operational risk is a by-product of conducting business and is primarily concerned with reducing exposure or hazard.

Organizations do not exist to take explicit operational risks

Security is an Operational Risk Management (ORM) activity

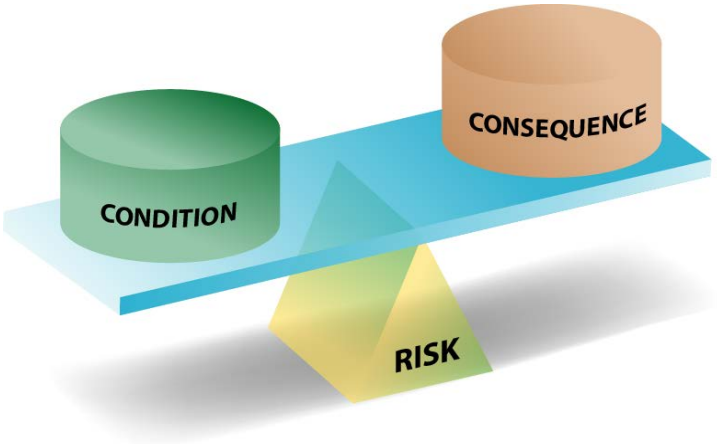
The aim of these "security" activities is ultimately to manage operational risk.



- Managing firewall rule-sets
- Installing access controls to facilities
- Limiting access to intellectual property or confidential information
- Confirming identity and privileges

Business continuity and disaster recovery are ORM activities

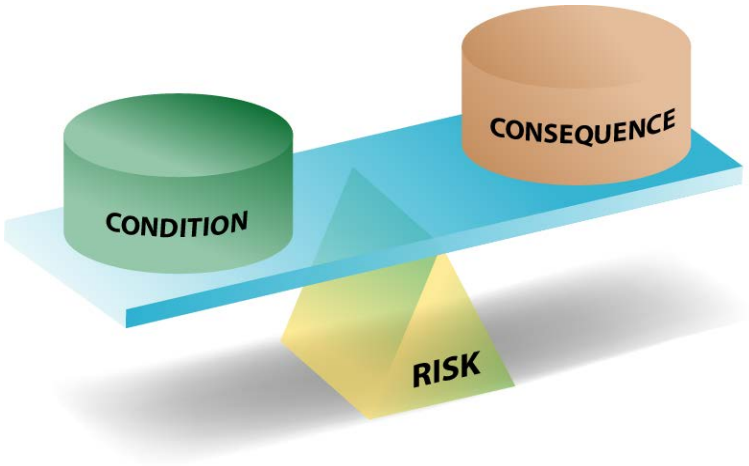
The aim of these "continuity" activities is also to manage operational risk.



- Limit unwanted effects of realized risk
- Ensure availability and recoverability
- Developing business continuity and disaster recovery plans
- Manage "consequence"

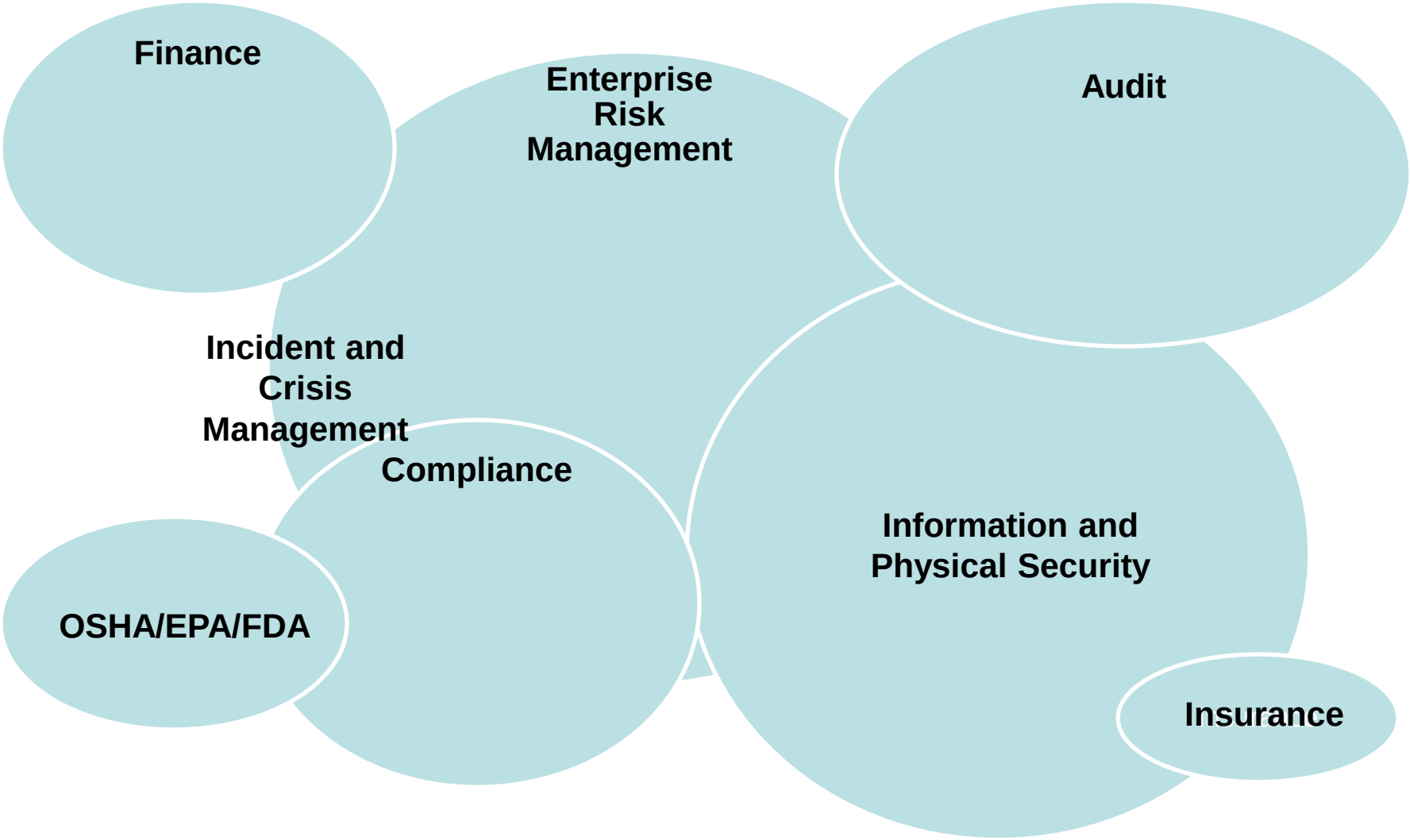
IT Operations is an ORM activity

The aim of these "operations" activities is to manage operational risk.



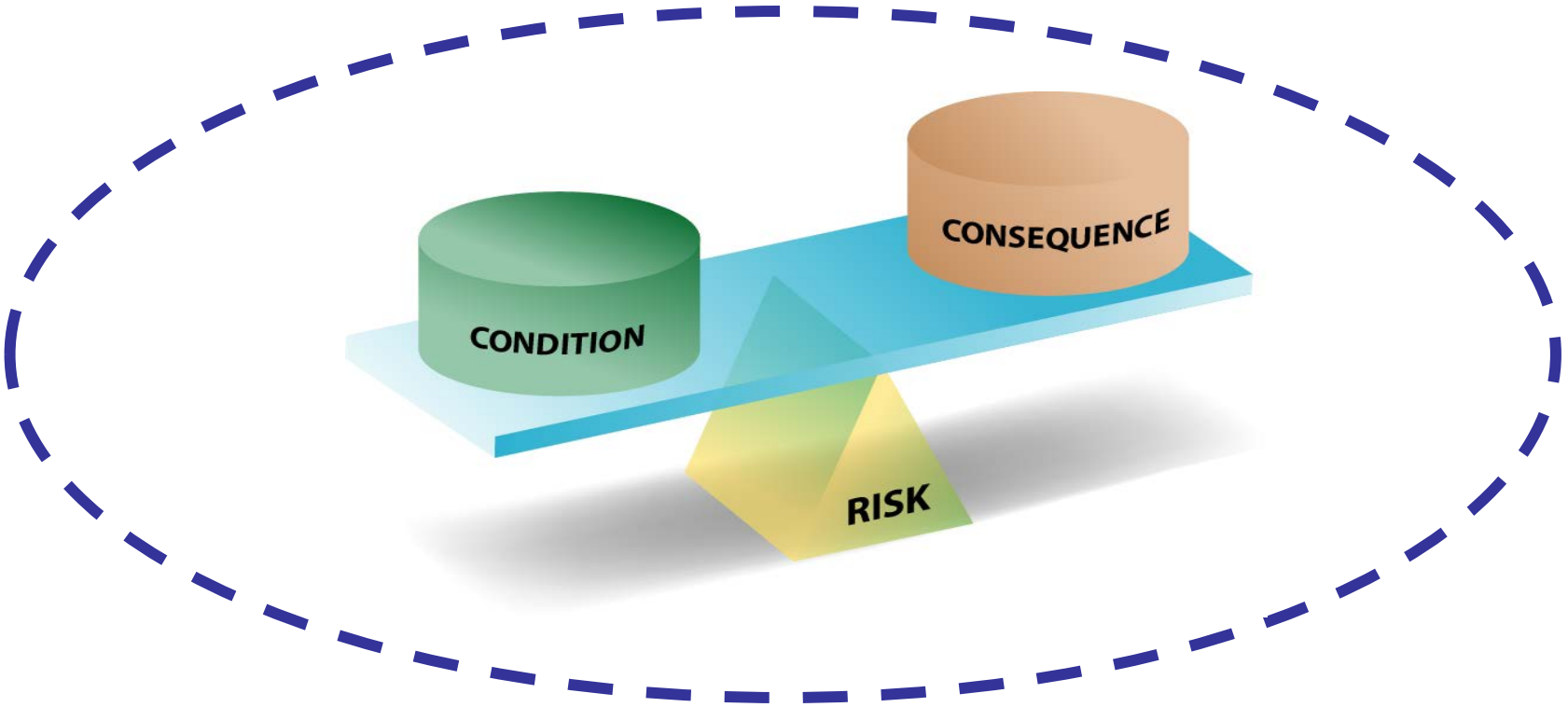
- Limit vulnerabilities and threats that originate in the technical infrastructure
- Providing appropriate access to systems & applications for staff and external entities
- Ensure availability and recoverability of technology

Risk Management areas are independent



Managing operational resilience requires a holistic approach

Managing both sides of the risk equation in alignment with business drivers and full knowledge of costs increases the resilience capability of the organization.



Auditing vs. risk management

Looking back vs. looking forward

Stop asking “What are the top risks I should be worried about?”

Barriers and challenges

What current barriers do you face in establishing, managing, and/or executing a measurement program?

What challenges do you face in identifying meaningful metrics within your organization?

What have you done to try to overcome these barriers and challenges?

Why Do You Want to Measure?

How secure am I?

When asked:

- How secure am I?
- Am I secure enough?
- How secure do I need to be?

What does this mean?

- How secure am I compared to my competition?
- Am I managing my risks well?
- Do I need to spend more $$ on security or risk management? If so, on what?
- What are the PR and legal impacts of a data breach?

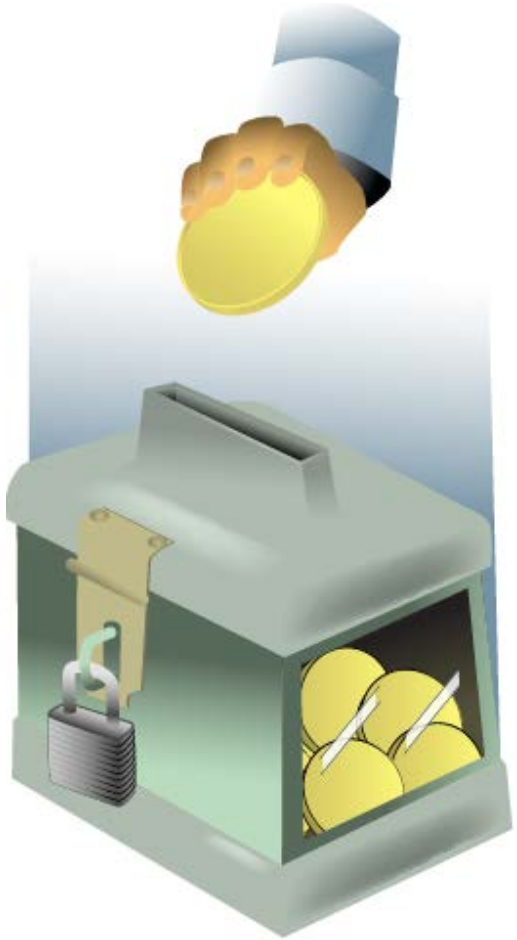
Key questions

What should I be measuring to determine if I am meeting my performance objectives for security?

- Do I know what these are? Do they reflect today's realities?

What is the business value of being more secure?

- Of a specific security investment?



So what? Why do you care?

This is the most important question.

If I had this metric: (*)

- What decisions would it inform?
- What actions would I take based on it?
- What behaviors would it affect?
- What would improvement look like?
- What would its value be in comparison to other metrics?

(*) informed by Douglas Hubbard, *How to Measure Anything*, John Wiley & Sons, 2010

What are you measuring today? -1

Some typical technical metrics

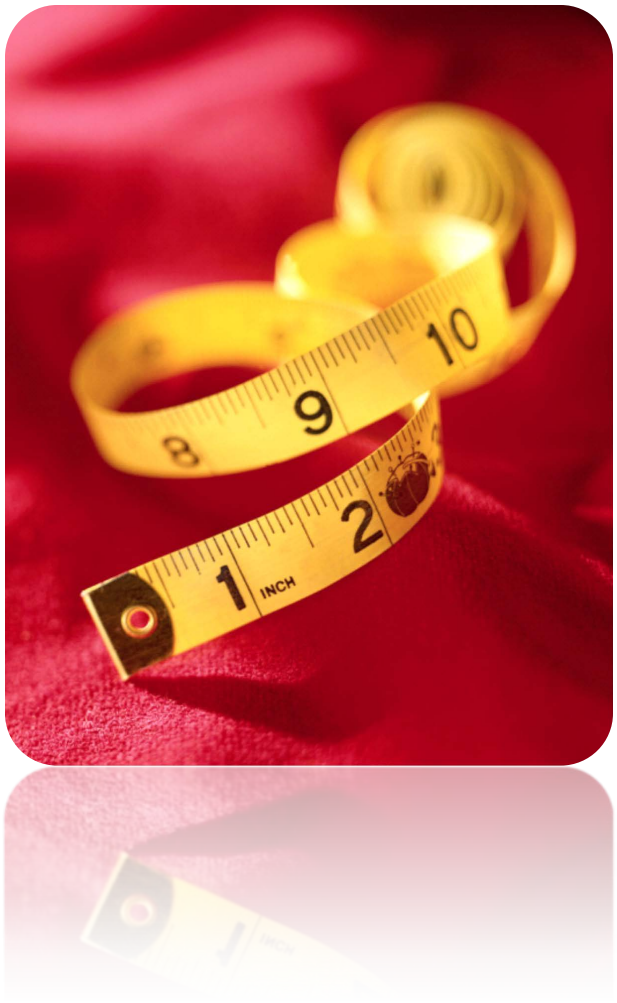
- % of assets (systems, devices) patched
  - min/mean/max time from patch release to patch implementation
- % of scanned assets not found in the CMDB
  - Goal: 100% of assets inventoried in CMDB and reflect standard configurations
- % of devices/assets regularly scanned by anti-virus software
- number of incidents reported/closed
  - number of incidents with a known solution (patch) that was not applied
- % of assets subject to ingress/egress filtering

What are you measuring today? -2

Some typical strategic/business metrics

- % of senior executives who have documented security objectives that are reviewed as part of the performance management review process
- % of security policies that are met (no violations; all exceptions approved)
- difference in planned vs. actual to perform security activities/actions/investments
  - schedule
  - resources
  - cost
- % of staff who have been assessed to determine if training has been effective commensurate with their job responsibilities

Why measure?



- Demonstrate that the security program has measurable business value
- Speak to decision makers in their language
- Answer key questions
- Demonstrate that control objectives are (and continue to be) met
- Justify new investments; improve
- Use trends to help predict future events

Who, what, where, when, why, how?

Who is the metric for? Who are the stakeholders? Who collects the measurement data?

What is being measured?

Where is the data/information stored?

When/how frequently are the metrics collected?

Why is the metric important (vs. others)?

- The most meaningful information is conveyed by reporting trends over time vs. point in time metrics.

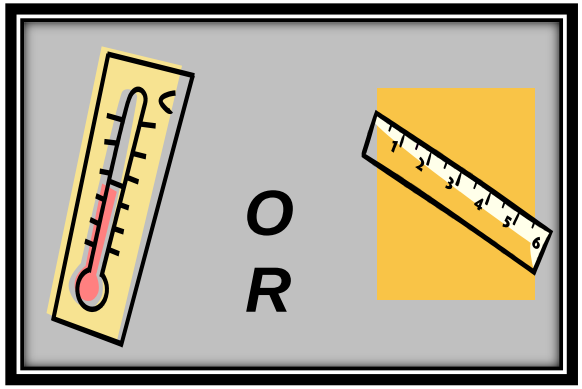
How is the data collected? How is the metric presented? How is the metric used?

Measurement Defined

Terminology (*)

Measure vs. metric

- I had 2 eggs for breakfast this morning
- It's 90 degrees in Las Vegas, NV
- This workshop is 8 hours long

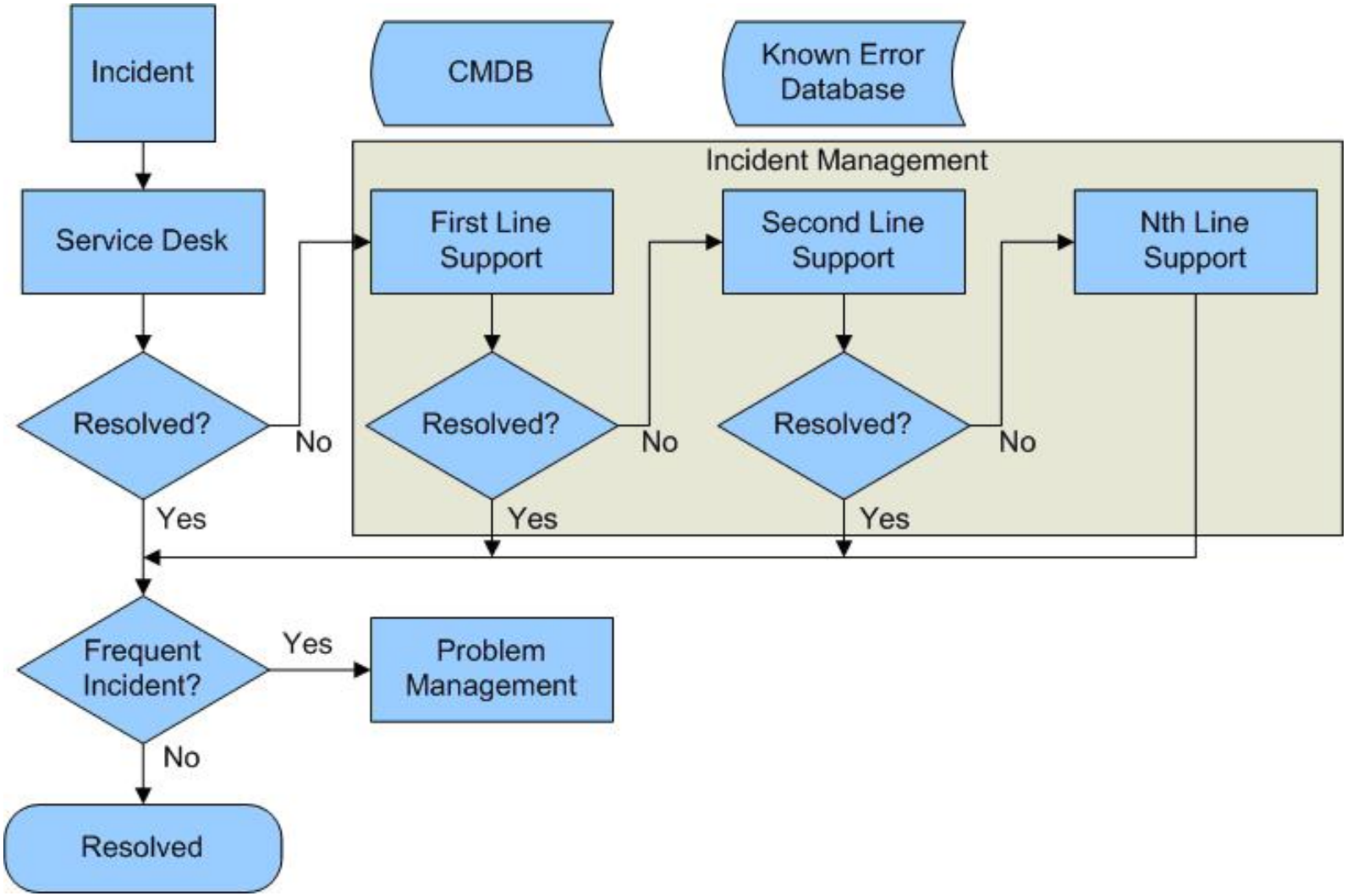


A measure (or measurement) is the value of a specific characteristic of a given entity (collected data).

A metric is the aggregation of one or more measures to create a piece of business intelligence, in context.

(*) Visualize This! Meaningful Metrics for Managing Risk. Session GRC-F02, RSA Conference 2014.

Technical vs. process metrics



Types of process metrics

Implementation

- Is this process/activity/practice being performed?

Effectiveness (aka outcome)

- How good is the work product or outcome of the process/activity/practice? Does it achieve the intended result?

Process performance

- Is the process performing as expected? Is it efficient? Can it be planned? Is it predictive? Is it in control?

Maturity models

A maturity model reflects known, commonly used practices in a domain.

Maturity models exist for software development, service delivery, acquisition, managing people, operational resilience, and other domains.

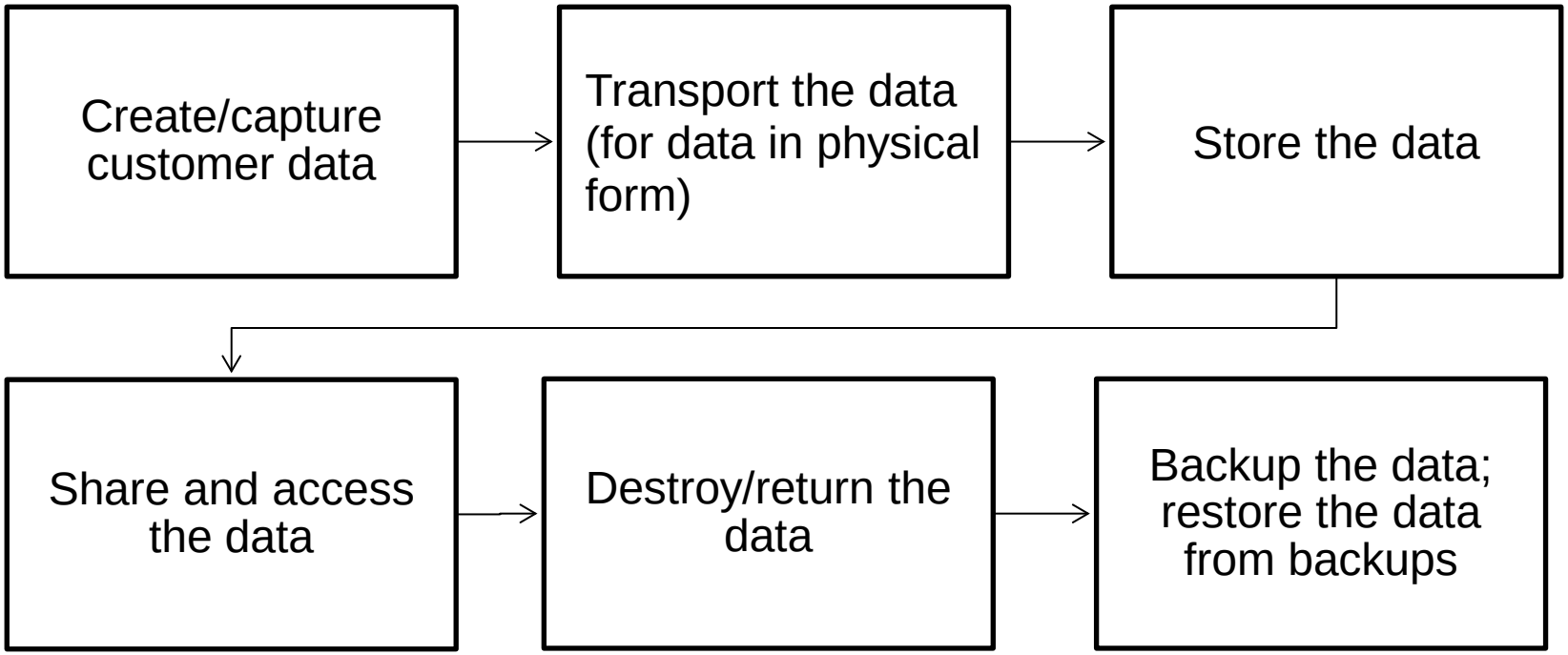
Examples of maturity models are COBIT, CMMI, ITIL, and CERT-RMM.

Defined process

A defined process describes the activities and tasks necessary to consistently perform work in a predictable, repeatable, measurable manner.

Example: Protecting customer data

A process for protecting customer data draws upon current experiences, improved by relevant COBIT, ITIL, CMMI, or CERT-RMM specific practices.



Getting Started

To get started

Identify sponsors and key stakeholders

Define security objectives and key questions

Determine information that informs these

- What information do you already have?
- What information do you need to collect?
- What is the value of collecting additional information?

Define and vet a small number of key metrics

Collect, analyze, report, refine

Leverage an existing measurement program

Set up a measurement program

1. Define
   - measurement objectives including audiences and key stakeholders
   - metrics (5-10 based on the metric template)
   - key roles to collect, analyze, and report these metrics
   - data collection and storage methods and tools
   - analysis methods and procedures
2. Collect measurement data
3. Analyze measurement data
4. Store data and results in a secure manner
5. Report results
6. Start small
   - data collection
   - analysis procedures
   - number of metrics
   - number of participating business units

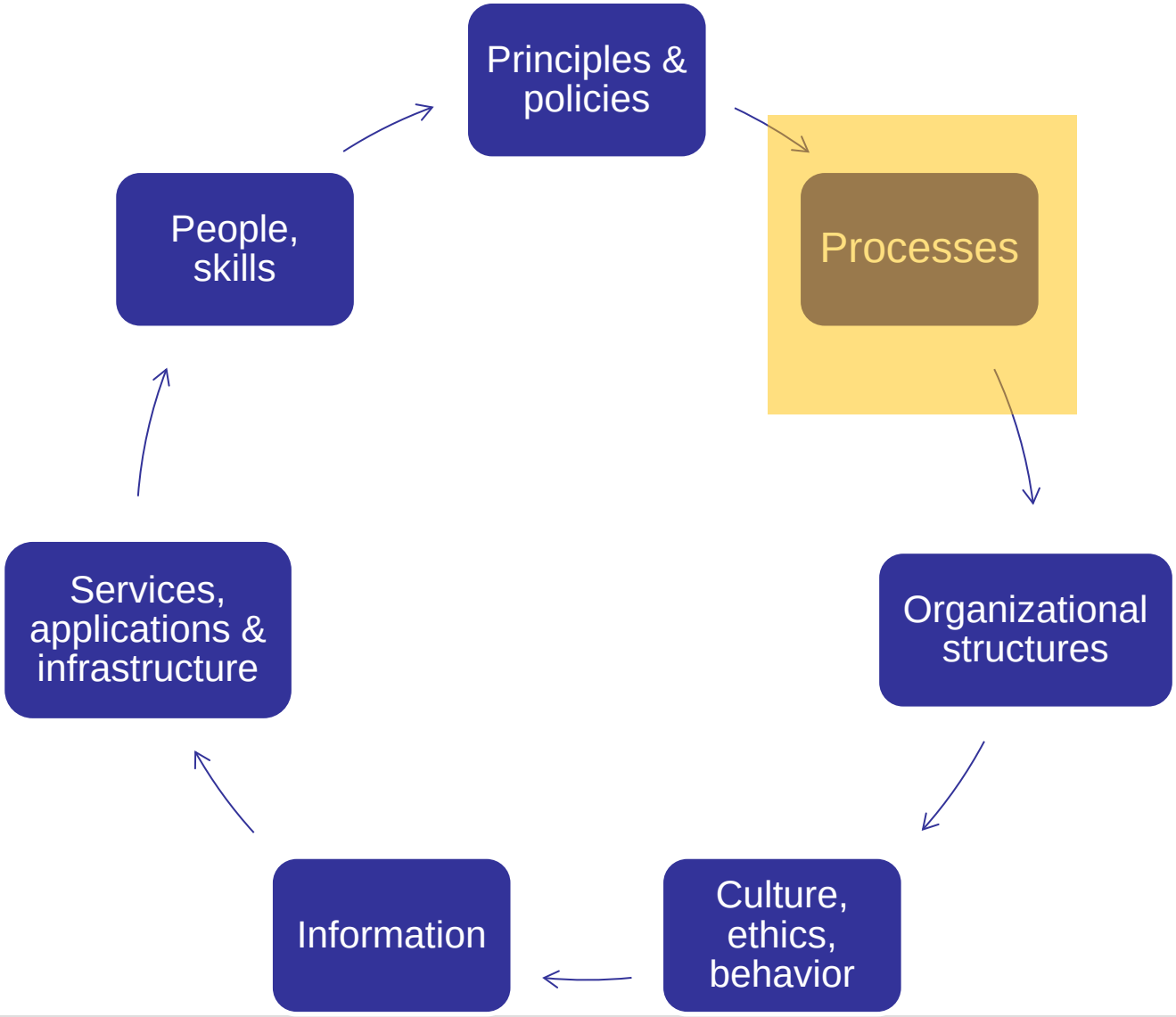
Risk quantification

Building a risk quantification method or program is by definition “measuring” something.

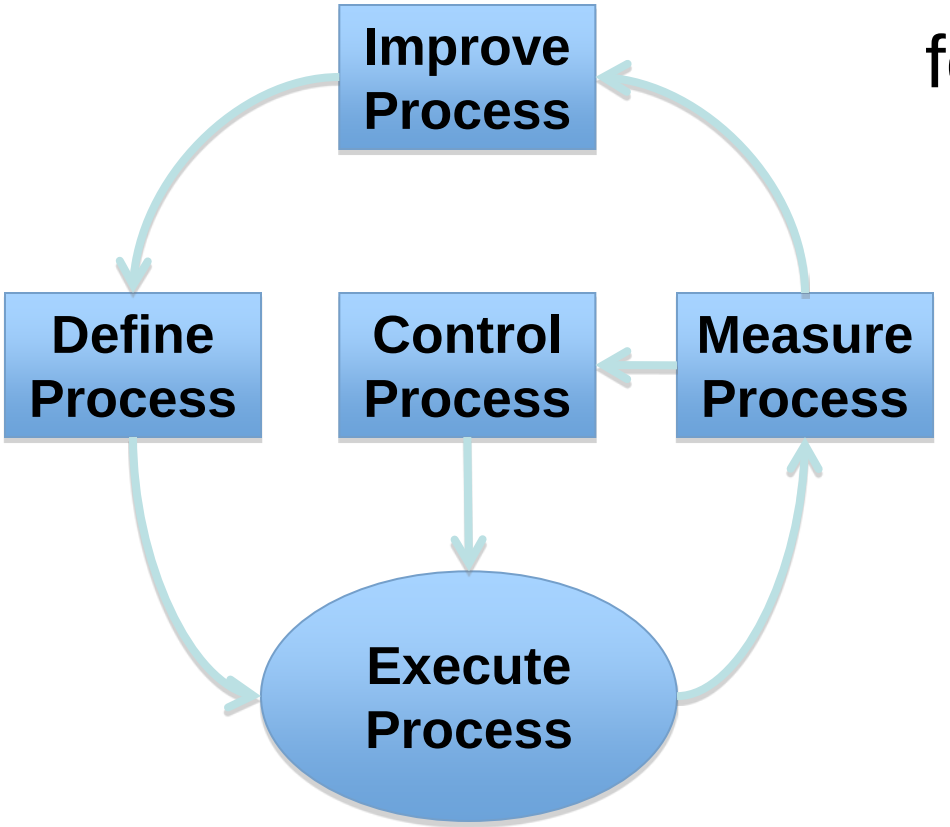
There are foundational elements that need to be in place for a successful risk quantification program:

- Business objectives and goals
- Method & Program
- A set of questions that can be answered with the data; “clean” data
- Process and workflow; roles and responsibilities
- Results that are generated from data – minimizes “gaming” and provides context to compare results.
- Governance and oversight of the method and program

COBIT 5 enablers



Managing a process

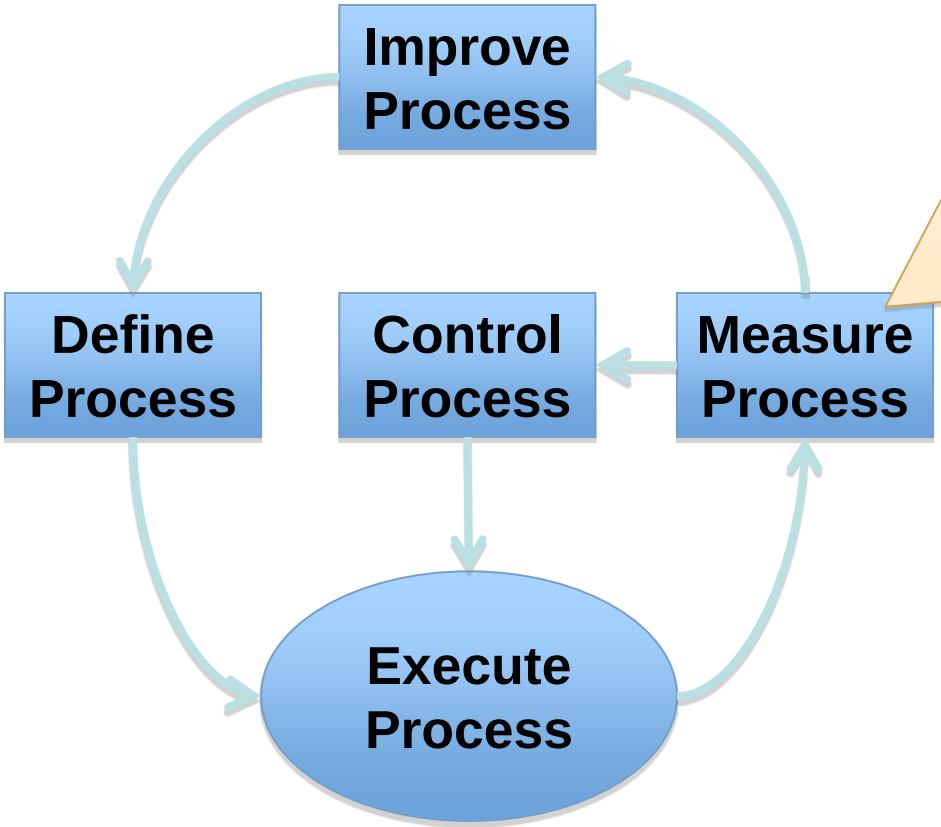


Four key responsibilities for managing a process:

1. Define the process
2. Measure the process
3. Control the process (stabilize so that results are predictable)
4. Improve the process

Florac & Carleton, *Measuring the Software Process*, Addison-Wesley, 1999

Measuring a process



1. **Collect data that measures performance**
2. **Analyze performance**
3. **Retain & use data**
   - **Assess process stability**
   - **Predict cost & performance**
   - **Establish baselines**
   - **Identify improvements**

Florac & Carleton, *Measuring the Software Process*, Addison-Wesley, 1999

Cost-effective vs. cost-benefit

Cost-benefit – for a given decision, one particular option has both a cost and a benefit.

- This type of information may not be available on day one when building a measurement program.

Cost-effective – desired result or objective achieved by money spent.

- Generally, this is a better representation of an information security and risk management program.

Deriving Metrics from Objectives – GQIM

Background

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)

(*) [Allen 2010]

Key questions

Not “What metrics should I use?”

“What do I want to know or learn?”

Alternatives:

- What decisions do I want to inform?
- What actions do I want to take?
- What behaviors do I want to change?

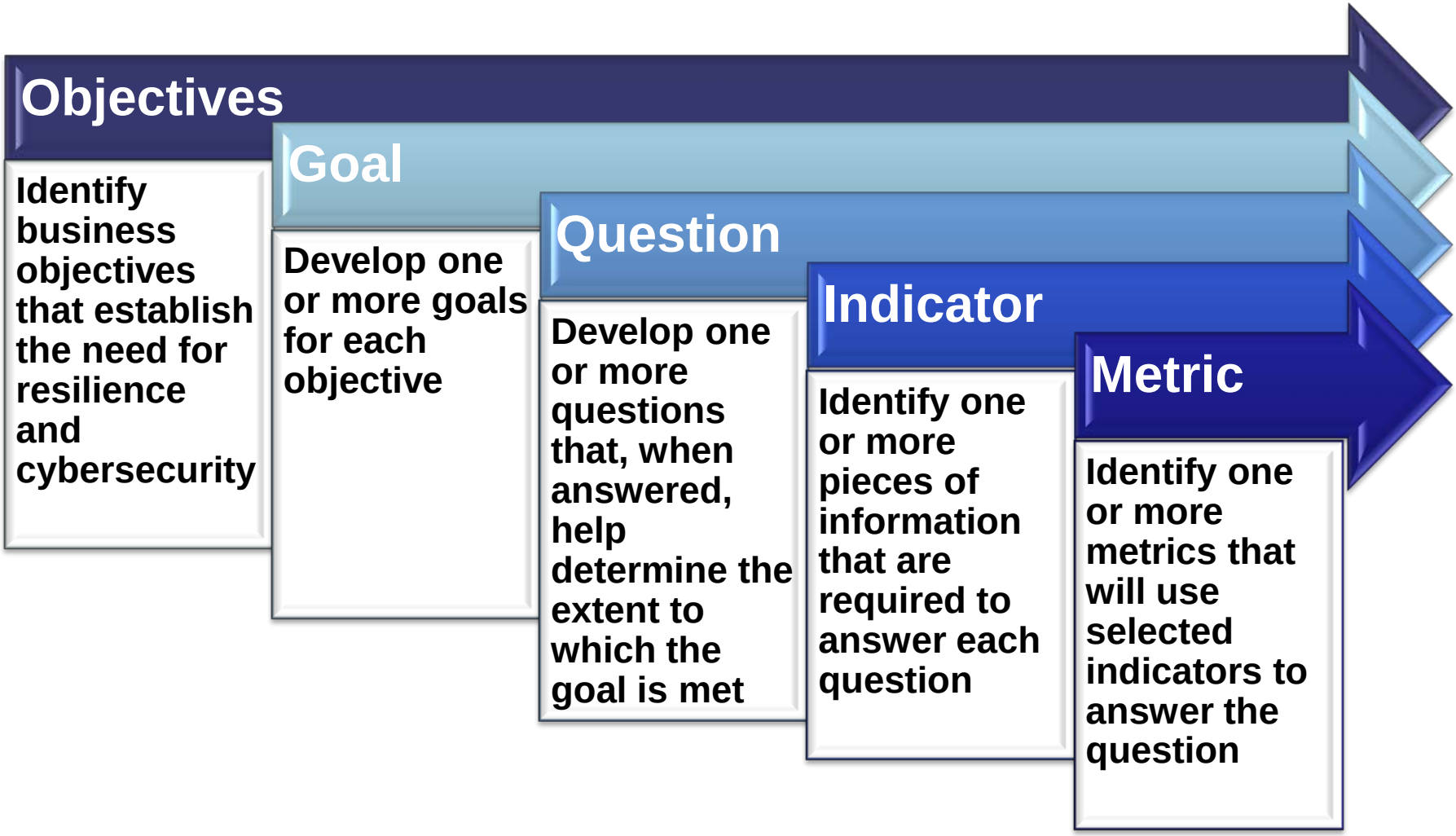
Purpose

Use a defined, repeatable method to derive meaningful metrics that directly support the achievement of business objectives

As a result, be able to:

- demonstrate the business value of each metric (and thus justify the cost for its collection and reporting)
- defend such metrics in comparison to others
- add metrics, update metrics, and retire metrics as business objectives change
- ultimately, inform business decisions, take appropriate action, and change behaviors

GQIM process



Questions

References

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

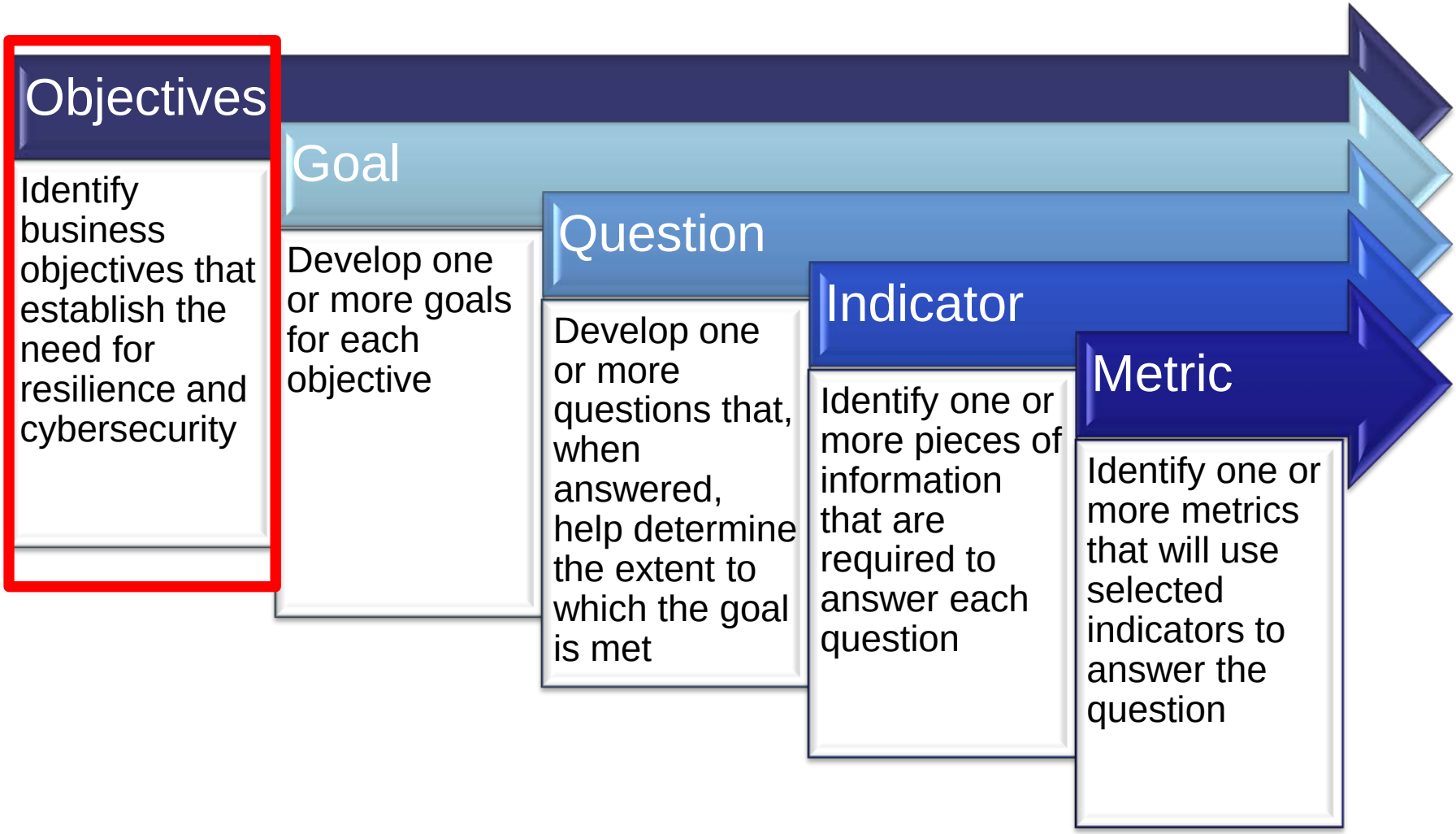
Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, September 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9401

http://blogs.gartner.com/paul-proctor/2013/10/15/please-stop-asking-me-for-a-list-of-your-top-risks-aka-everyone-wants-a-pony/

http://blogs.gartner.com/paul-proctor/2013/08/11/no-one-cares-about-your-security-metrics-and-you-are-to-blame/

Topic 2: Select Objectives

GQIM process



Approach

State a business objective

- Ideally your business objective supports a stated strategic objective
- **Ensure that** [*business unit, service, product, supply chain, technology, data center*] **is** …
  - *available to meet a specified customer or revenue growth objective*
  - *unavailable for no more than some stated period of time, number of transactions, other units of measure*
  - *fully compliant with [law, regulation, standard] so as not to incur [z] penalties*

SMART(ER) criteria for objectives

S: Specific

M: Measurable

A: Achievable

R: Relevant (Results-based; Realistic)

T: Time-bound

E: Evaluated

R: Reviewed

Discuss objectives with your group

State your business objective and why you chose it

Provide feedback to your group members

Facilitators will provide feedback

Choose one objective to report

Questions

Topic 3: Goal-Question-Indicator-Metric Method Overview

Key takeaways

Understand a 5-step method for deriving metrics from business objectives

- applied to example scenarios

Be able to apply this method to your business objective(s)

- using provided templates

Identify at least one metric that you can use immediately

Be able to better communicate with business leaders in their language

Assess the utility of currently reported metrics

Topics

Overview

Objectives to goals

- Incident management and Forbes scenarios

Goals to questions

Questions to indicators

Indicators to metrics

Overview

Background

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)

Additional tailoring of the method for use by the U.S. Department of Homeland Security (2013 to present)

(*) [Allen 2010]

Key questions

Not “What metrics should I use?”

“What do I want to know or learn?”

Alternatives:

- What decisions do I want to inform?
- What actions do I want to take?
- What behaviors do I want to change?

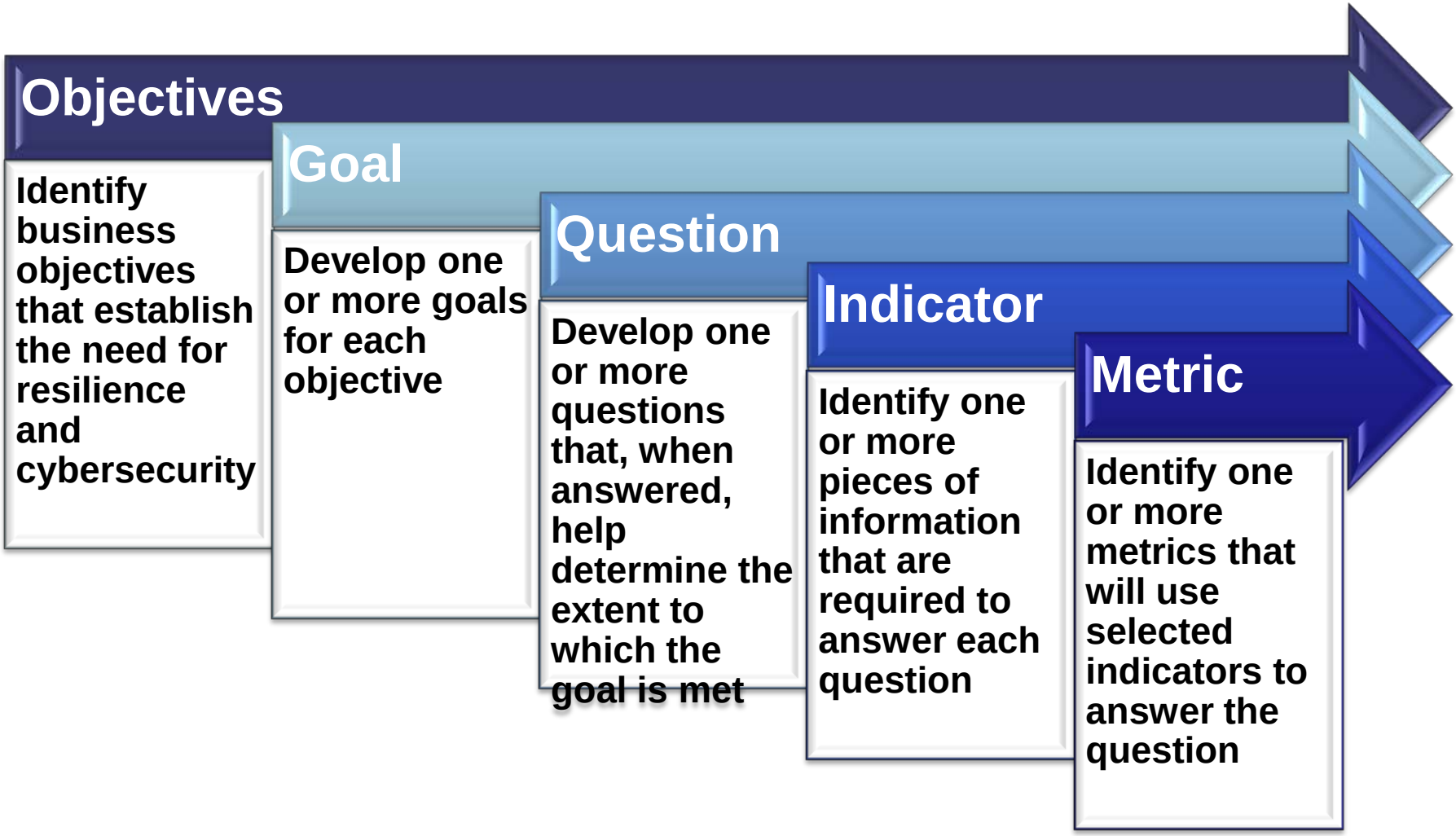
Purpose

Use a defined, repeatable method to derive meaningful metrics that directly support the achievement of business objectives

As a result, be able to:

- demonstrate the business value of each metric (and thus justify the cost for its collection and reporting)
- defend such metrics in comparison to others
- add metrics, update metrics, and retire metrics as business objectives change
- ultimately, inform business decisions, take appropriate action, and change behaviors

GQIM process



Objectives to goals

Approach

State a business objective

Define one or more goals that are required to achieve the stated objective

Goal: the end toward which effort is directed

- Fewer are better
- Essential (high leverage/high payoff) vs. complete coverage
  - Judgment informed by stakeholder review

Last 2 statements apply to each step in the GQIM method

Objectives to goals

What are meaningful actions to take to achieve the objective?

Which actions are most important?

- 2-3 that are essential, high leverage, high payoff

Carry forward and further refine key terms from the objective in the goals

Ask "If I achieve this goal, will I be able to demonstrate substantive progress in achieving the objective?"

Objectives to goals – healthy teeth

Objective	Goal
Ensure your kid's teeth are healthy	**G1:** Ensure your kid has everything needed to brush their teeth. **G2:** Ensure your kid is brushing their teeth at least twice daily.

Goals to questions

Goals to questions -1

What are meaningful questions to answer to determine if the goal is being achieved?

- Requires subject matter expertise

Which questions are most important?

Carry forward and further refine key terms from the goal in the question

Ask "If I answer this question, will I be able to demonstrate substantive progress in achieving the goal?"

Goals to questions -2

Useful questions are in the form of:

- *What is the process for . . . (better than "How does the organization . . .")*
  - —leads to implementation metrics
- *How effective is . . .*
  - —leads to effectiveness metrics
  - —most desirable but need implementation metrics first

Goal to questions – healthy teeth



Goal	Question
G1: Ensure your kid has everything needed to brush their teeth.	**Q1:** Do they have a good toothbrush? **Q2:** Do they know how to brush properly?
G2: Ensure your kid is brushing their teeth at least twice daily.	**Q1:** Do they show you their clean teeth?

Questions to indicators

Questions to indicators

What data (and sometimes in what form) do I need to answer the question?

- Can add more data granularity than called for in the question

Which data is most important?

Carry forward and further refine key terms from the question in the indicators

Ask “If I have this data, will I be able to answer some aspect of the question?”

Questions to indicators – healthy teeth



Goals	Questions	Indicators
G1	**Q2:** Do they know how to brush properly?	**Q2.I1:** Demonstration of use **Q2.I2:** Issues found during dental check-ups
G2	**Q1:** Do they show you their clean teeth?	**Q1.I1:** Evidence that tooth brushing has occurred

Indicators to metrics

Indicators to metrics

Using the indicator data, what number, percentage, mean, or other metric can I collect/calculate to help answer the question?

- a percentage presumes 2 numbers are available so you don't need to list the number as a metric if the percentage is based on it

Which metrics are most important?

Ask "Do I need additional data (more indicators)?"

Ask "If I report this metric (over time), will it provide the greatest insight possible to answer the questions from which it derives?"

Indicators to metrics – healthy teeth

Goals	Indicators	Metrics
G1	**Q2.I2:** Issues found during dental check-ups	**I2.M1:** Number of cavities **I2.M2:** Instances of gingivitis
G2	**Q1.I1:** Evidence that tooth brushing has occurred	**I1.M1:** Smell of breath **I1.M2:** Condition of toothbrush (wet vs. dry)

Iterate

Put yourself in the role of the decision maker who will receive these metrics reports

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

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

- What decision needs to be made (including where to invest)?
- What action(s) needs to be taken next? By whom?
- What behavior needs to change? For whom?
- Are we improving or getting worse? Why?
- Do I need to keep collecting this metric (in comparison to others)? If so, for how long? If not, what is a better metric?

Collect, interpret, refine, improve

Forbes scenario

Forbes scenario

On 13 Feb 2014, a single, successful spear phishing email set in motion a very public compromise of Forbes.com.

The Syrian Electronic Army leveraged the variety of social media accounts that the Forbes staffers and contributors have to leap-frog from their email accounts to the publication's blog and social media platforms.

All passwords across multiple platforms were forced to be reset and Forbes.com and its WordPress platform were taken offline several times over 2 days.

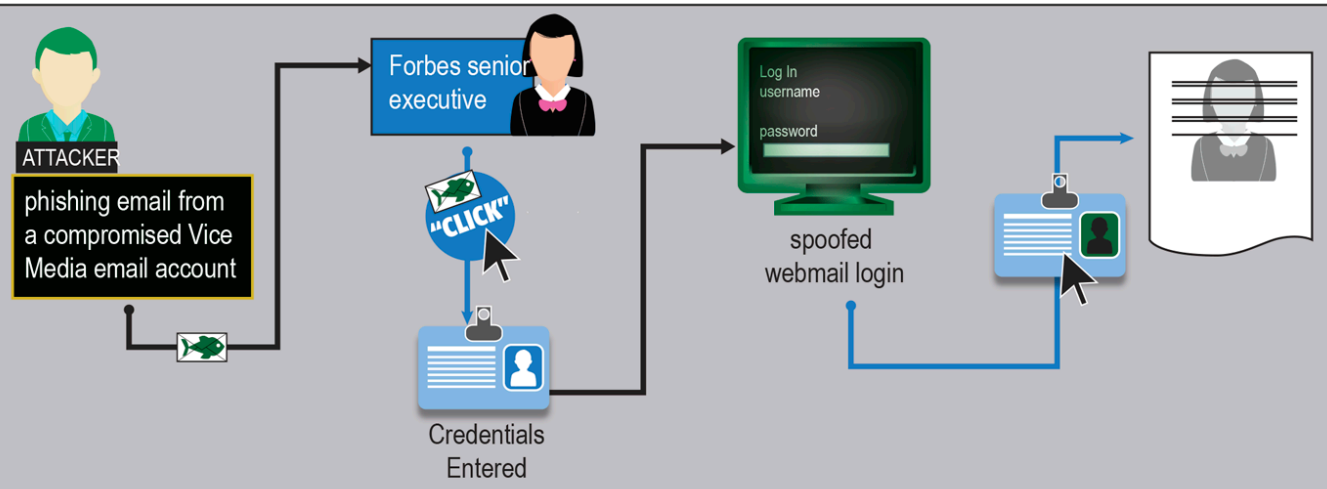
Forbes has focused on building unique content and a publishing model for the social media era in an open and secure platform…So what happened?

The DAY the Syrian Electronic Army Hacked Forbes

On February 13, 2014, a single, successful spear phishing email set in motion a very public compromise of Forbes.com, the website of the influential business and financial publication. The Syrian Electronic Army, apparently in retribution for earlier Forbes stories on Syria, leveraged the social expectations of Forbes staffers and leap-frogged from their email accounts to the publication's blog and social media platforms.

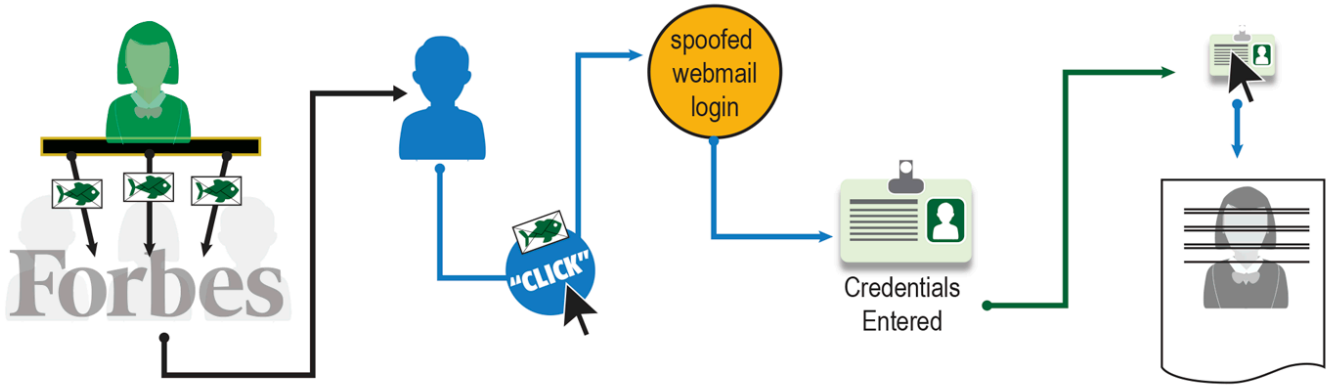
Thursday, 6:15am

A Forbes senior executive receives a phishing email from a compromised Vice Media account concerning a fake Reuters story about Forbes. She clicks the link, which opens a spoofed webmail login page, and enters her email credentials.



7:45am

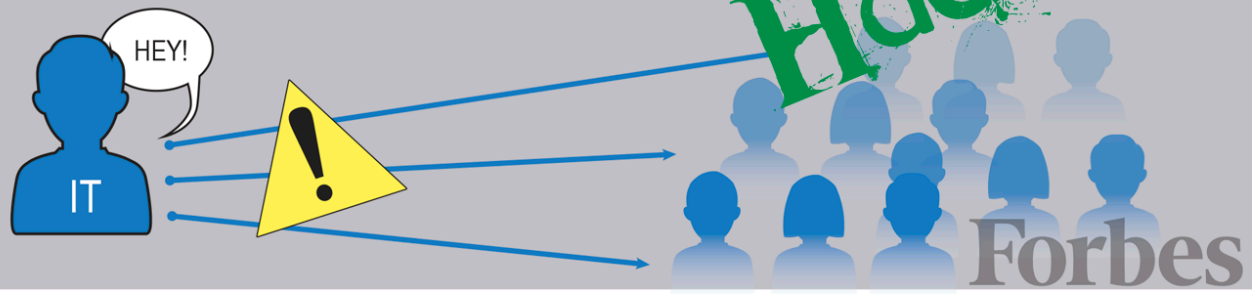
The attackers use the senior executive's compromised account to send more phishing emails to Forbes staff. The appearance of the executive as the sender deceives a staffer with super-administrator privileges on Forbes' WordPress platform, and he clicks on the malicious link and enters his email credentials.



The DAY the Syrian Electronic Army Hacked Forbes

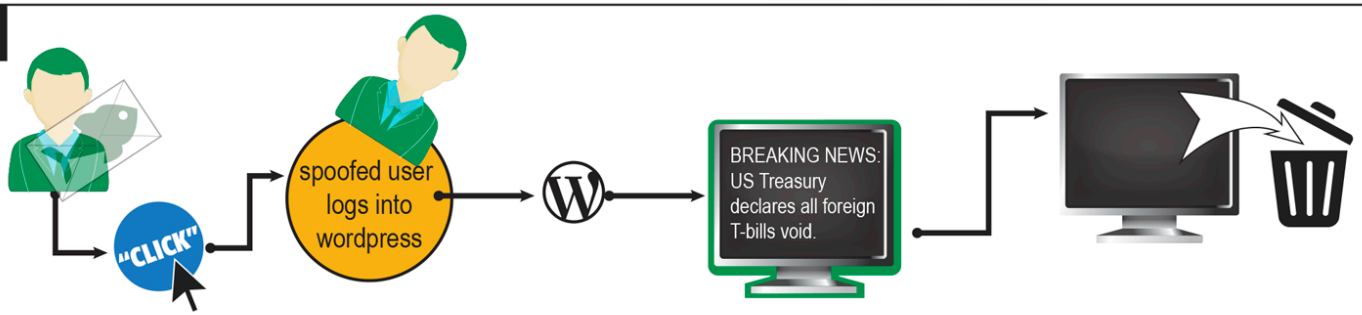
8:15am

A Forbes IT administrator warns staffers about the phishing attempts.



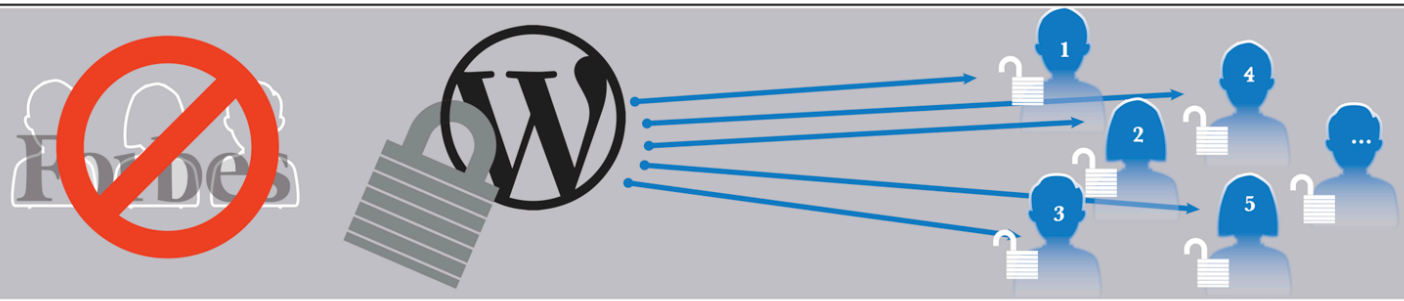
10:00 am

A financial reporter clicks the link in the phishing email but does not enter his credentials on the subsequent login page. Returning to his blog, WordPress prompts him to log in again. Almost immediately after he logged in, two new posts with false information appeared on his blog.



10:15am

Forbes locks all users out of its WordPress site and resets the credentials of its super-administrators and phishing victims one by one, by phone or in person to avoid further compromise.



6:00 pm

Forbes reopens the site to users.

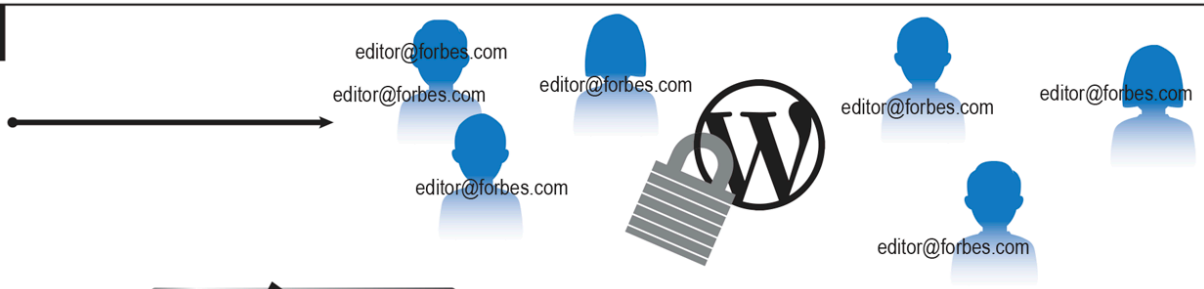
The DAY the Syrian Electronic Army Hacked Forbes

7:00 pm

The attackers use the email credentials stolen from the staffer at 7:45 a.m. to again trigger the WordPress "forgot password" function and access the same WordPress super-administrator account and deface a Forbes editor's blog, adding the headline "The Syrian Electronic Army Was Here." Forbes also believes the attackers compromised other Forbes social networking accounts.

7:10 pm

Forbes locks down the site again and changes back the compromised WordPress credentials to its users' email addresses.



Midnight

Forbes reopens the site to users.

The attackers, perhaps using Forbes' social networking account logins, again compromise the WordPress super-administrator account and deface six Forbes blog pages with the phrase "Hacked By The Syrian Electronic Army." Forbes staffers' personal Twitter accounts linked to WordPress propagate this message.

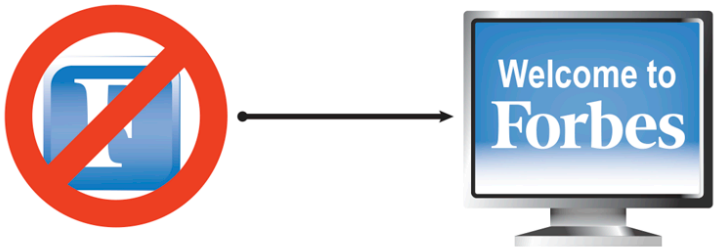
The DAY the Syrian Electronic Army Hacked Forbes

3:40am

Forbes locks down the site again.

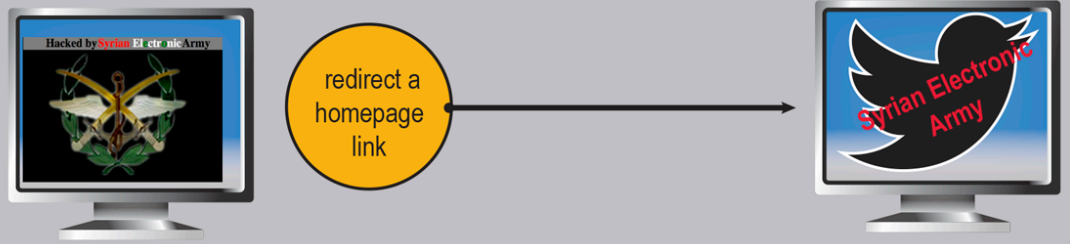
7:30 am

Forbes disables social account logins and reopens the site.



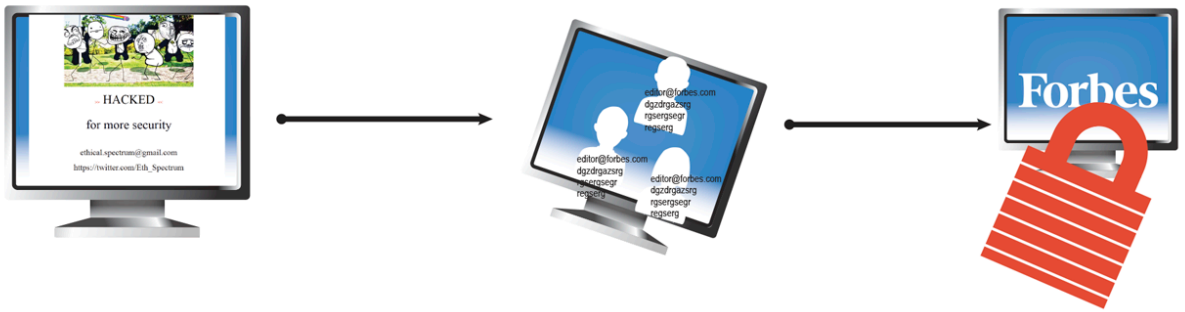
8:00 am

Using a method that remains unclear, the attackers compromise another editor's WordPress account and replace Forbes' WordPress theme with one displaying a stylized Syrian flag and the Syrian Electronic Army's logo. They also redirect a homepage link to the attackers' Twitter feed.



11:30 am

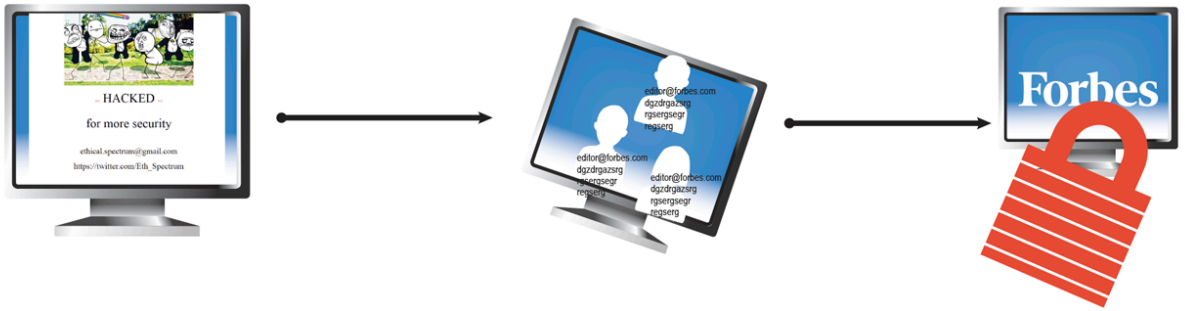
Forbes administrators receive email from the hacker Ethical Spectrum, apparently not connected to the Syrian Electronic Army, saying that he or she had stolen the database of Forbes usernames, emails, and passwords and demanding what appeared to be a ransom. The email included a screen shot of a few users' hashed credentials and passwords. Forbes locks down the site again and calls the FBI.



The DAY the Syrian Electronic Army

11:30 am

Forbes administrators receive email from the hacker Ethical Spectrum, apparently not connected to the Syrian Electronic Army, saying that he or she had stolen the database of Forbes usernames, emails, and passwords and demanding what appeared to be a ransom. The email included a screen shot of a few users' hashed credentials and passwords. Forbes locks down the site again and calls the FBI.



12:35 am

Via Twitter, the Syrian Electronic Army announces its attack on Forbes and later offers to sell the Forbes user database. On Friday night, the attackers publish the database.

Forbes scenario objective examples

Strategic

- Provide a content and publishing model for the era of social media that is both open and secure.

Business

- OB1: Increase user awareness on potential threats and the appropriate responses to social engineering and phishing tactics
- OB4: Improve the public's and users' confidence in the ability of Forbes.com to operate securely and to protect user privacy

Topics 4-7: Goal-Question-Indicator-Metric Method Work Sessions

Topics

Objectives to goals

Goals to questions

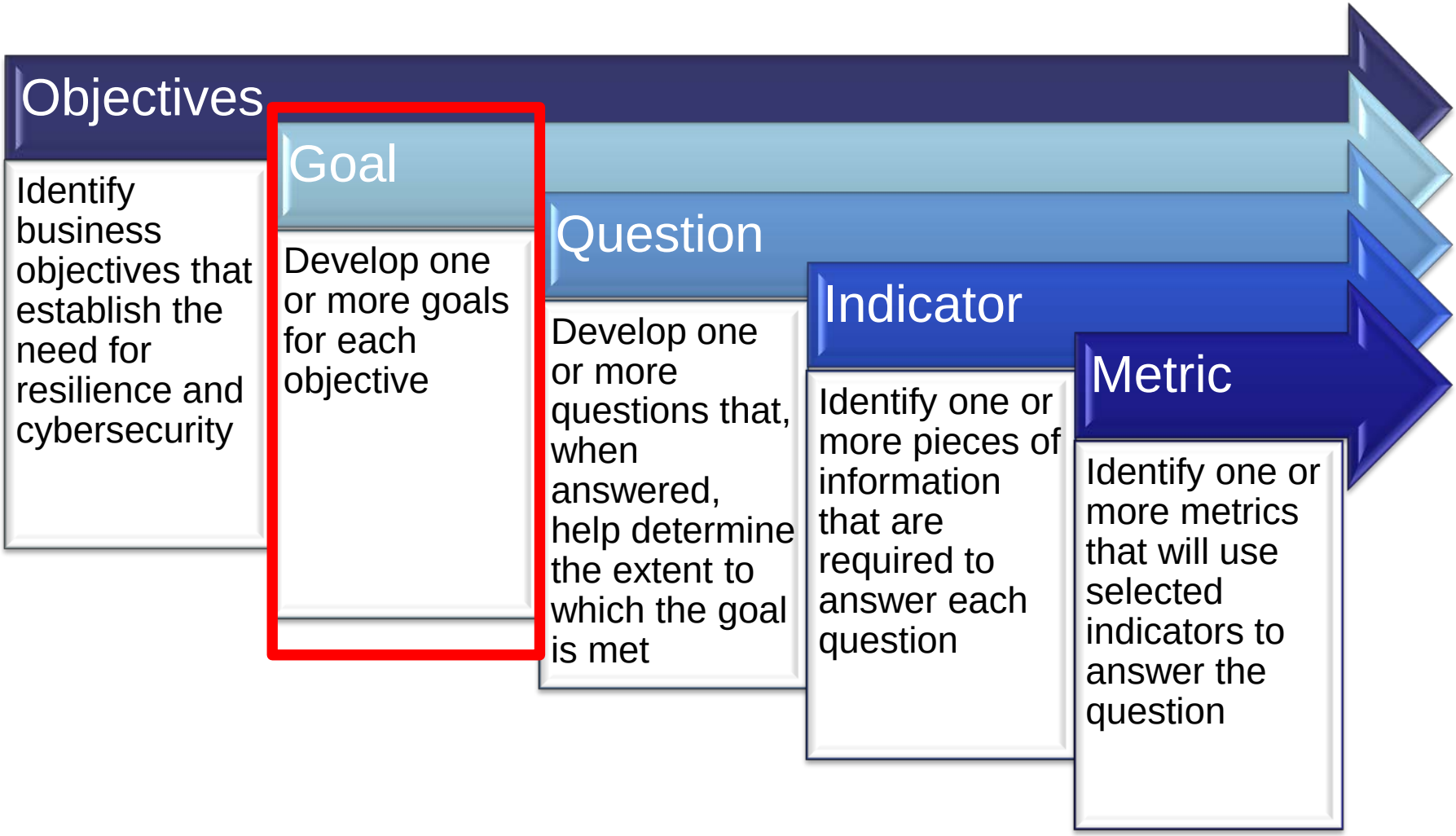
Questions to indicators

Indicators to metrics

- Template for defining metrics

Topic 4:
Objectives to goals

GQIM process



Objectives to goals

What are meaningful actions to take to achieve the objective?

Which actions are most important?

- 2-3 that are essential, high leverage, high payoff

Carry forward and further refine key terms from the objective in the goals

Ask "If I achieve this goal, will I be able to demonstrate substantive progress in achieving the objective?"

Objective to goals – incident management example

Objective	Goal
Mitigate the risks of business disruption and loss resulting from cybersecurity incidents (with impact threshold > [x])	*Operate a cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.* • *enterprise and operational unit levels*
	Others?

Objective to operational risks – IM example

Objective	Risk
Mitigate the risks of business disruption and loss resulting from cybersecurity incidents (with impact threshold > [x])	*A successful cybersecurity incident (condition) is not detected (event), resulting in impact exceeding threshold [x] (consequence).*
	Others?

Objective to goals – Forbes scenario

Objective	Goals
OB1: Increase user awareness on potential threats and the appropriate responses to social engineering and phishing tactics	**OB1.G1:** Ensure all users are trained at least bi-annually on new cybersecurity threats and appropriate responses
	OB1.G2: *Ensure users whose accounts are compromised do not succumb to the same attack(s) again (randomly tested for one year following a compromise)*
	Others?

Objective to goals template

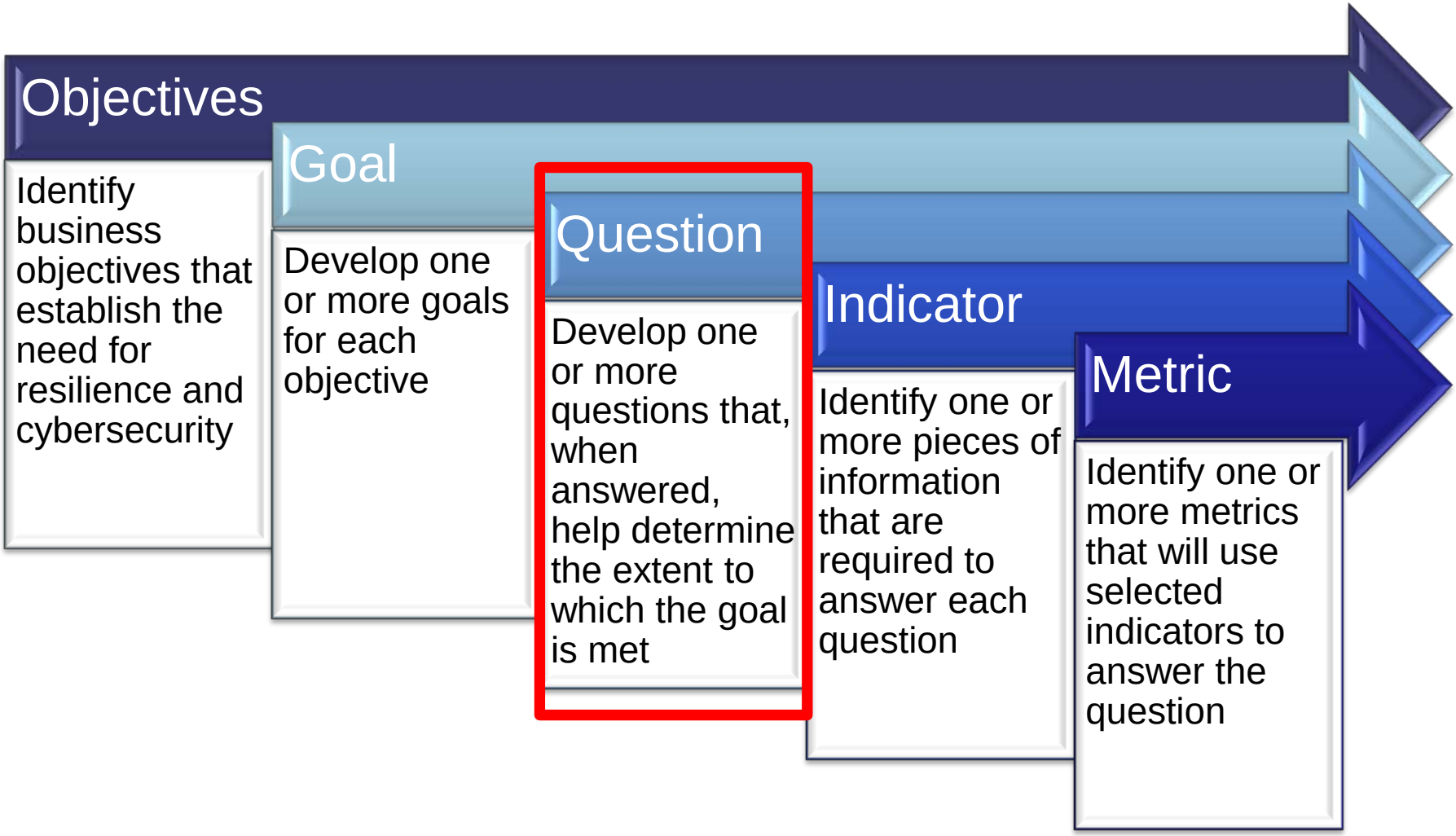
Objective	Goals

Objective to operational risks template

Objective	Risks

Topic 5:
Goals to questions

GQIM process



Goals to questions -1

What are meaningful questions to answer to determine if the goal is being achieved?

- Requires subject matter expertise

Which questions are most important?

Carry forward and further refine key terms from the goal in the question

Ask "If I answer this question, will I be able to demonstrate substantive progress in achieving the goal?"

Goals to questions -2

Useful questions are in the form of:

- *What is the process for . . . (better than "How does the organization . . .")*
  - —leads to implementation metrics
- *How effective is . . .*
  - —leads to effectiveness metrics
  - —most desirable but need implementation metrics first

Goal to questions – IM example

Goal	Questions
G1: Operate a cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.	***Q1:*** *What is the process by which suspicious events are detected and declared as incidents?*
	Q2: What is the criteria for escalating high-impact incidents? To whom?
	Q3: What steps are taken to respond to incidents? Minimize impact caused by incidents?
	Others?

Goal to questions – Forbes scenario

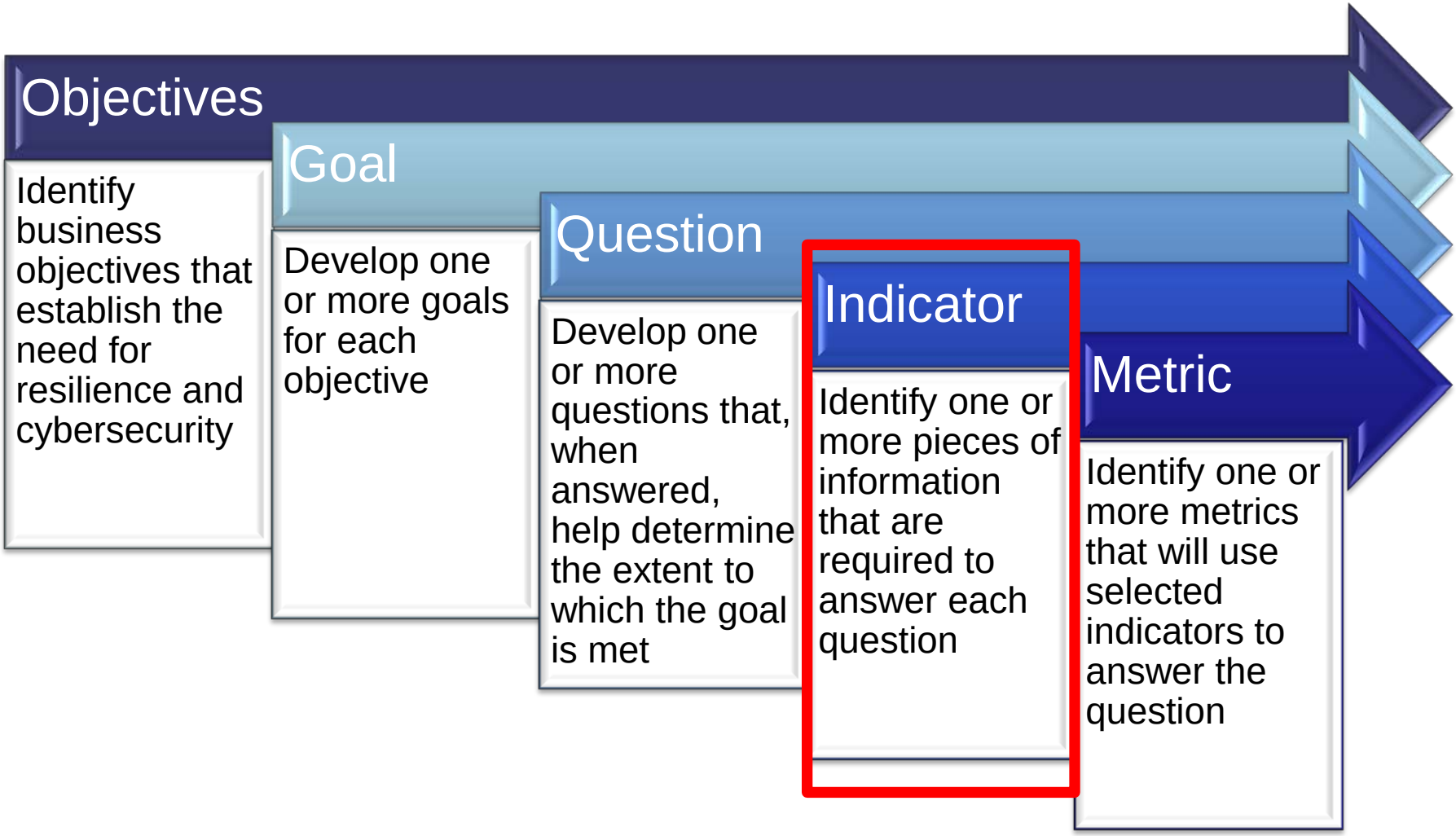
Goal	Questions
OB1.G2: Ensure users whose accounts are compromised do not succumb to the same attack(s) again (randomly tested for one year following a compromise)	***OB1.G2.Q1:*** *What is the process for identifying recurring compromised accounts?*
	OB1.G2.Q2: What is the process for implementing random testing of compromised accounts?
	Others?

Goal to questions template

Goal	Questions
	1. 2. 3.
	1. 2. 3.
	1. 2. 3.

Topic 6:
Questions to indicators

GQIM process



Questions to indicators

What data (and sometimes in what form) do I need to answer the question?

- Can add more data granularity than called for in the question

Which data is most important?

Carry forward and further refine key terms from the question in the indicators

Ask "If I have this data, will I be able to answer some aspect of the question?"

Question to indicators – IM example

Goal	Question	Indicators
G1	**Q1:** What is the process by which suspicious events are detected and declared as incidents?	***Q1.I1:*** *process and criteria for detecting and triaging suspicious events*
		Q1.I2: process and criteria for declaring incidents
		Q1.I3: incident categories
		Others?

Question to indicators – Forbes scenario

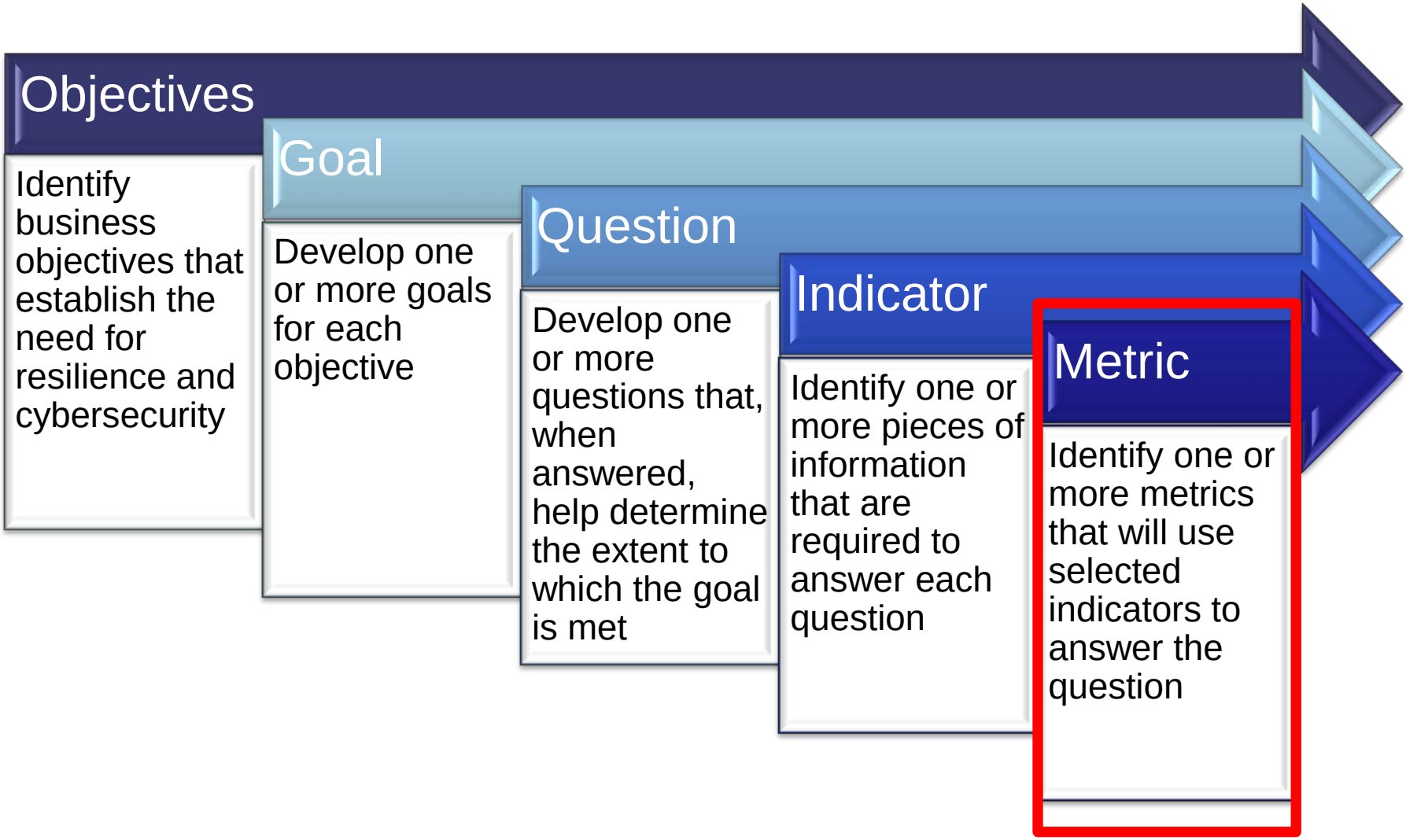
Goal	Question	Indicators
OB1.G2	**Q1:** What is the process for identifying recurring compromised accounts?	**Q1.I1:** Process for identifying recurring compromised accounts, including criteria and controls
		Q1.I2: *Security incident reports where the incident is caused by the same user account*
		Others?

Question to indicators template

Goal	Question	Indicators

Topic 7:
Indicators to metrics

GQIM process



Indicators to metrics

Using the indicator data, what number, percentage, mean, or other metric can I collect/calculate to help answer the question?

- a percentage presumes 2 numbers are available so you don't need to list the number as a metric if the percentage is based on it

Which metrics are most important?

Ask "Do I need additional data (more indicators)?"

Ask "If I report this metric (over time), will it provide the greatest insight possible to answer the questions from which it derives?"

Indicator to metrics – IM example

Goal	Indicator	Metrics
G1	**Q1.I1:** process and criteria for detecting and triaging suspicious events	**Q1.I1.M1:** mean time to detect suspicious events
		Q1.I1.M1: mean time to declare incidents (by incident category such as impact, for example, number of users or number of system affected)
		Others?

Indicator to metrics – Forbes scenario

Goal	Indicator	Metrics
OB1.G2	**Q1.I2:** Security incident reports where the incident is caused by the same user account	**I2.M1:** Number of user accounts that have been compromised by the same attack
		I2.M2: Mean time between similar attacks for a given user account
		Others?

Indicator to metrics template

Goal	Indicator	Metrics

Who, what, where, when, why, how

Who is the metric for? Who are the stakeholders? Who collects the measurement data?

What is being measured?

Where is the data/information stored?

When/how frequently are the metrics collected?

Why is the metric important (vs. others)?

- The most meaningful information is conveyed by reporting trends over time vs. point in time metrics.

How is the data collected? How is the metric presented? How is the metric used?

Metric template [refer to handout]

Metric name/ID

Goal

Question(s)

Related processes & procedures

Visual display

Data input(s) (data elements, data type)

Data collection (how, when, how often, by whom

Data reporting (by, to whom, when, how often)

Data storage (where, how, access control)

Stakeholders (information owner(s), collector(s), customer(s))

Algorithm or formula

Interpretation or expected value(s)

Topic 8:
The Big Picture:
Putting It All in Context

So what? Why do you care?

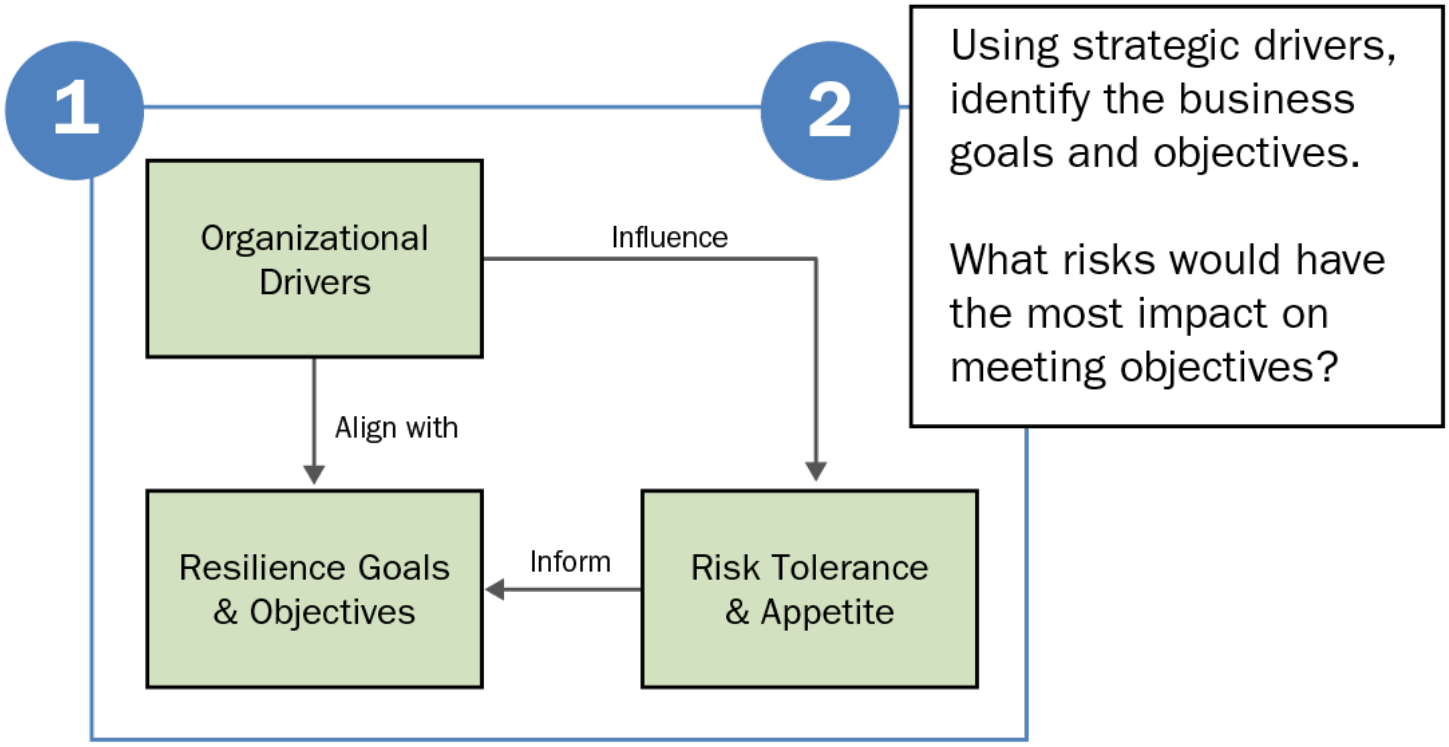
This is the most important question.

If I had this metric: (*)

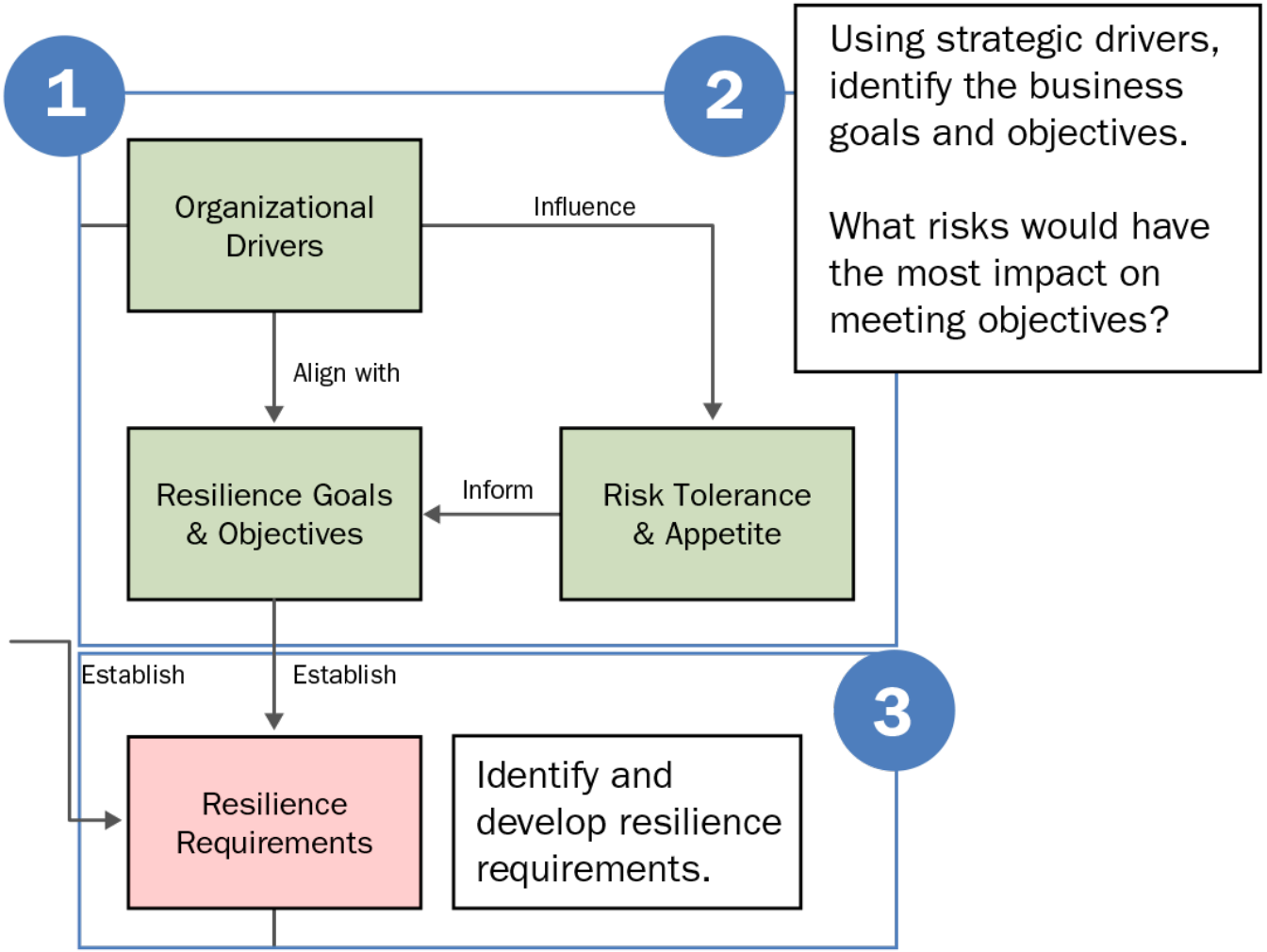
- What decisions would it inform?
- What actions would I take based on it?
- What behaviors would it affect?
- What would improvement look like?
- What would its value be in comparison to other metrics?

(*) informed by Douglas Hubbard, How to Measure Anything, John Wiley & Sons, 2010

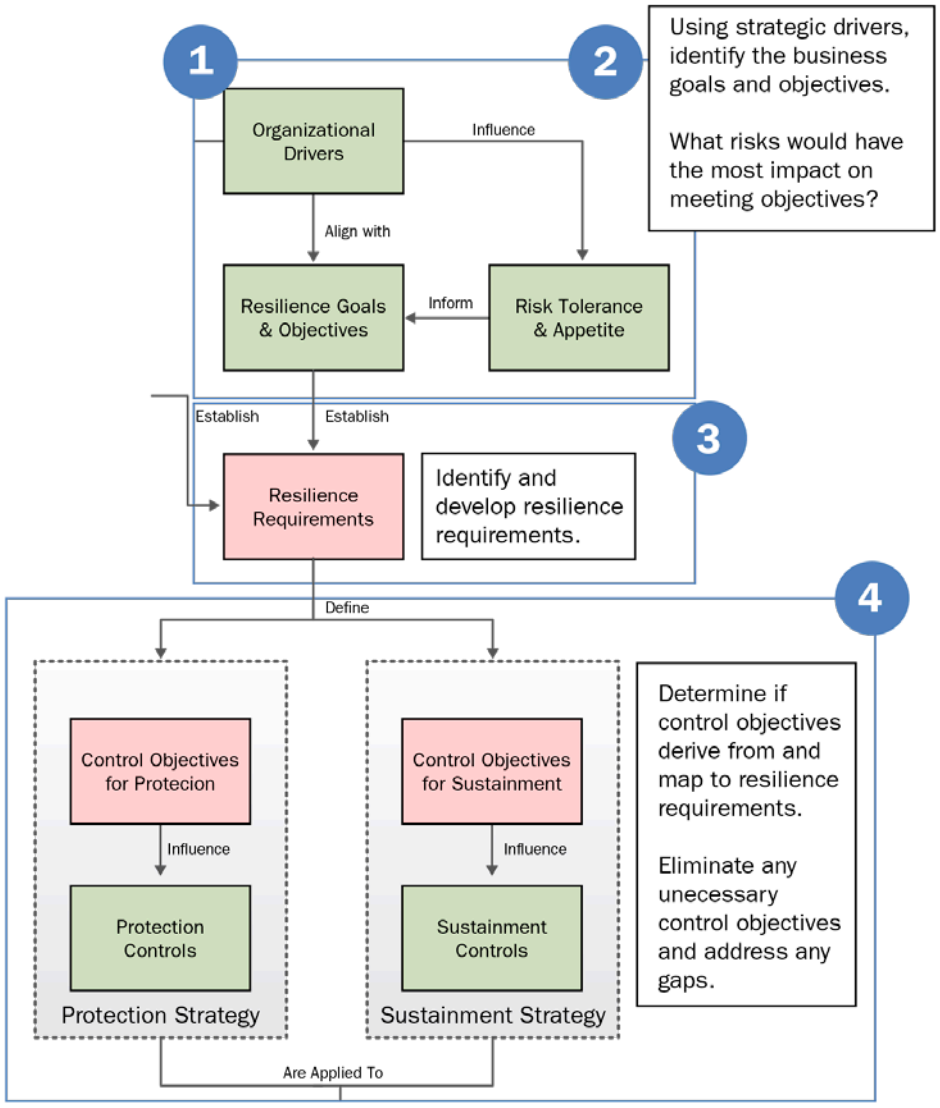
Organizational drivers



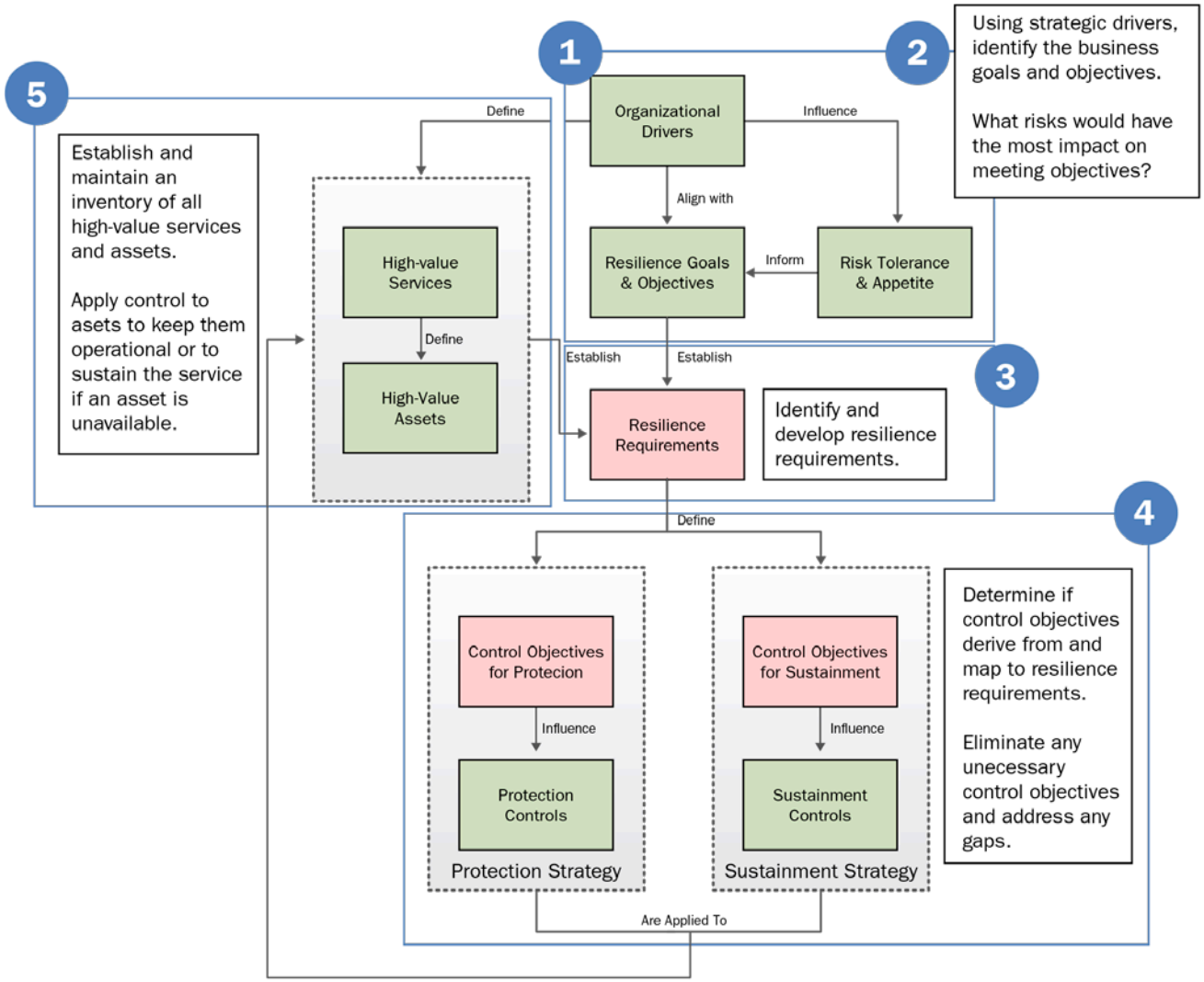
Resilience requirements



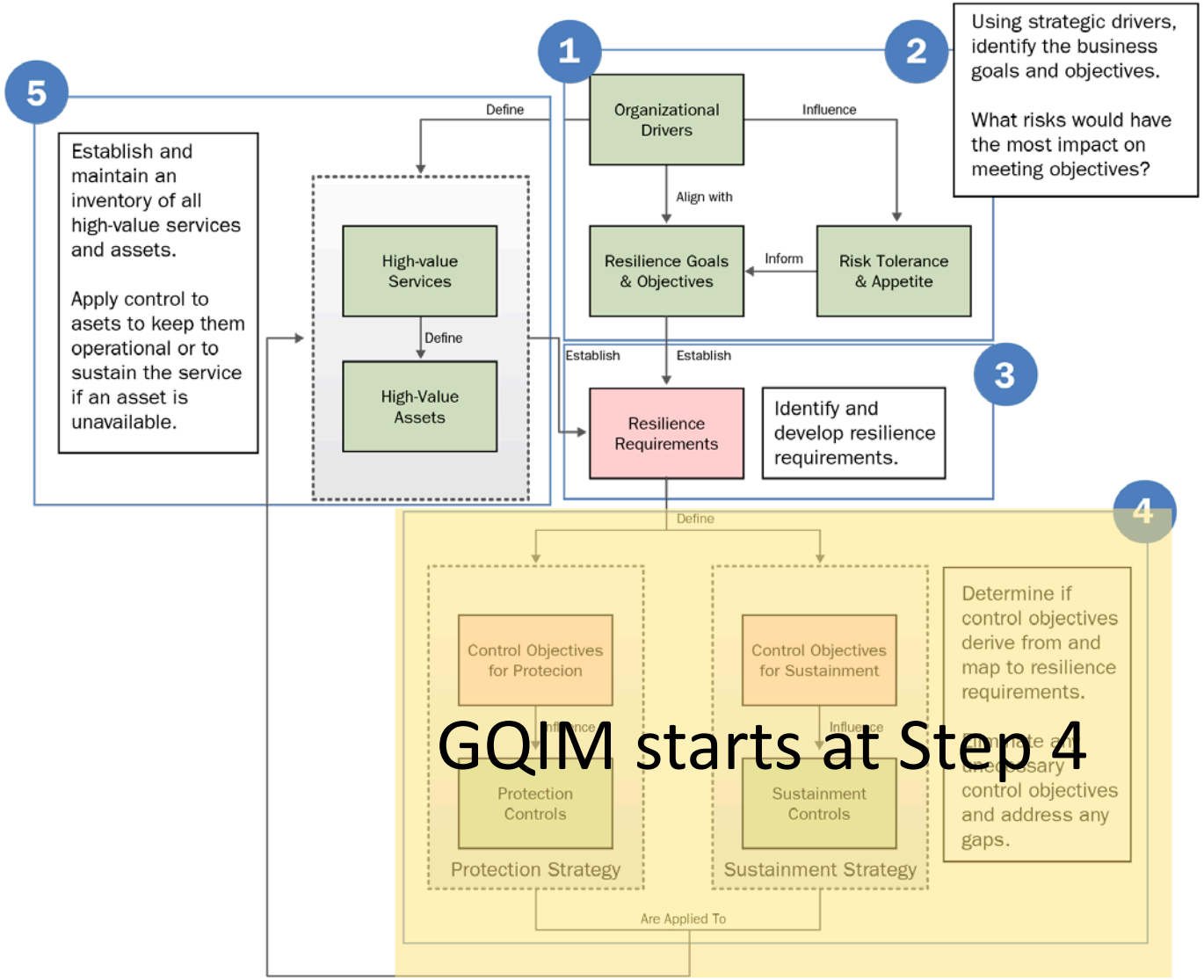
Control objectives



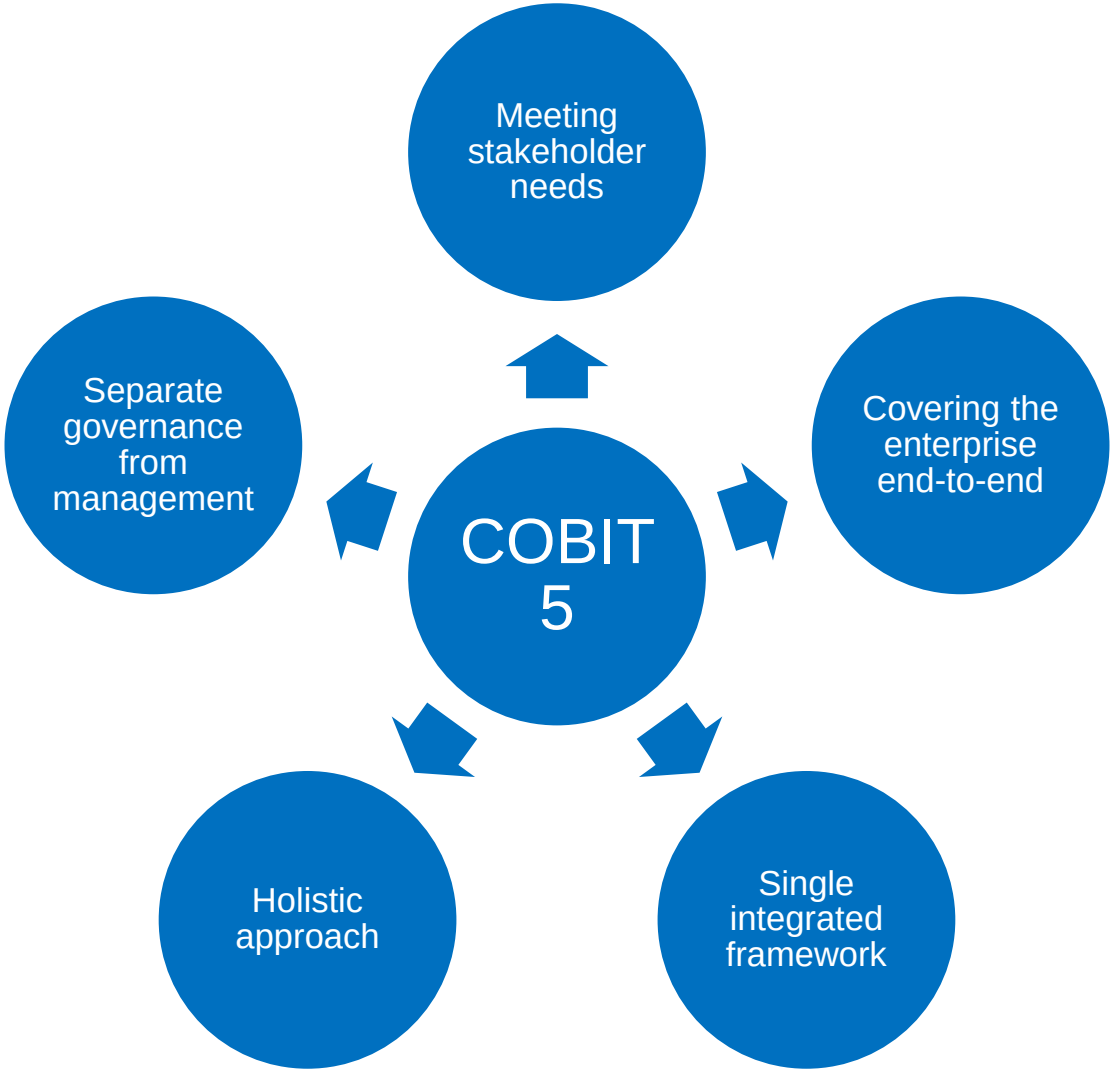
High-value services and assets



GQIM in context



GQIM measures meet COBIT5 goals



Barriers and challenges revisited

What current barriers do you face in establishing, managing, and/or executing a measurement program?

What challenges do you face in identifying meaningful metrics within your organization?

Have you identified some new/updated approaches for tackling these?

Questions


CERT
Software Engineering Institute
Carnegie Mellon University