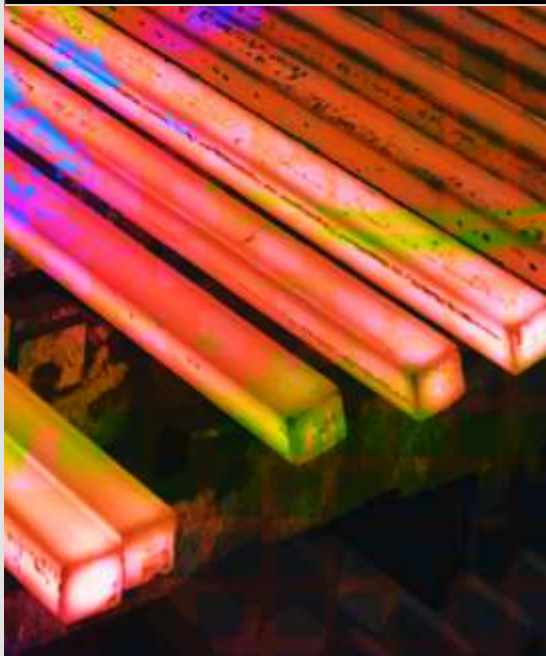
Carnegie Mellon University
Software Engineering Institute



Measurement Matters: The New Horizon for GQIM

APRIL 28, 2023

Brett Tucker, PMP, CSSBB, CISSP, CGRC
Technical Manager, Cyber Risk Management

Document Markings

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.

DM23-0373

Carnegie Mellon University – Software Engineering Institute (SEI)

Software Engineering Institute (SEI)

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

CERT – Anticipating and solving our nation's cybersecurity challenges

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

Agenda

Carnegie Mellon University Software Engineering Institute

The Need for Measurement in Cybersecurity
- **Measurement of Risk and Resilience**

A Brief Review of GQIM
- **The Gaps of GQIM**
- **New Considerations**

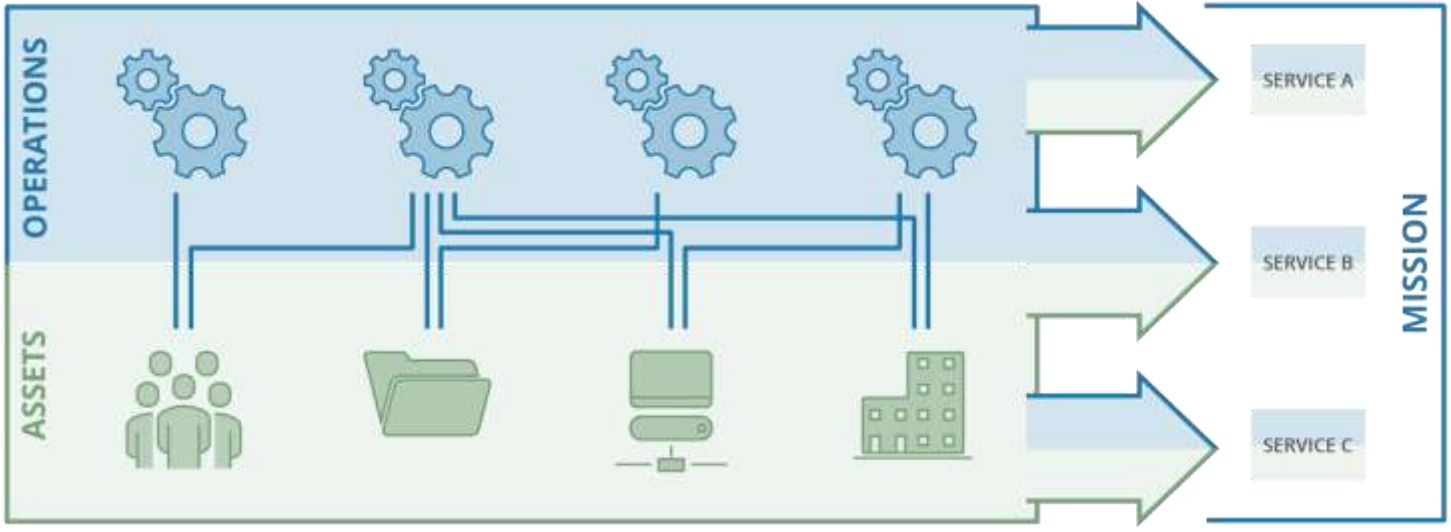
Looking to the Future
- **Next Steps**

Measurement Matters: The New Horizon for GQIM

The Need for Measurement in Cybersecurity

Carnegie Mellon University
Software Engineering Institute

Assets Support Critical Services



Assets derive their value from their importance in meeting the critical services that achieve the organization's mission.

Consider Third-Party Providers Too!

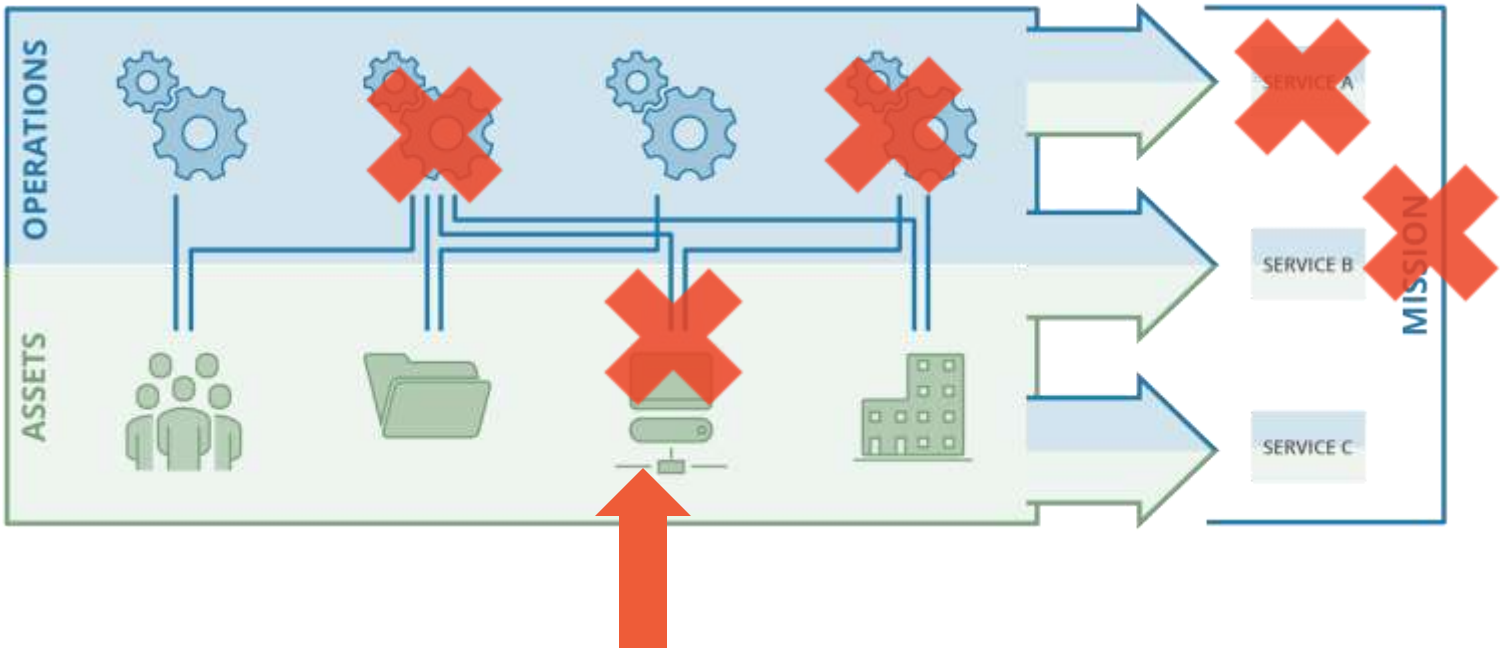
People: those who operate and monitor the service

Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed

Disruption of Assets Can Lead to Mission Failure



Realized Operational Risk Resulting in Asset Disruption

Good risk management practice leads to operational resilience.

How do you know if you are resilient enough?

Set goals and measure progress…

Measurement Matters: The New Horizon for GQIM

A Brief Review of GQIM

Carnegie Mellon University
Software Engineering Institute

Designing a Meaningful Metric

WHO
is the metric for?

WHAT
is being measured?

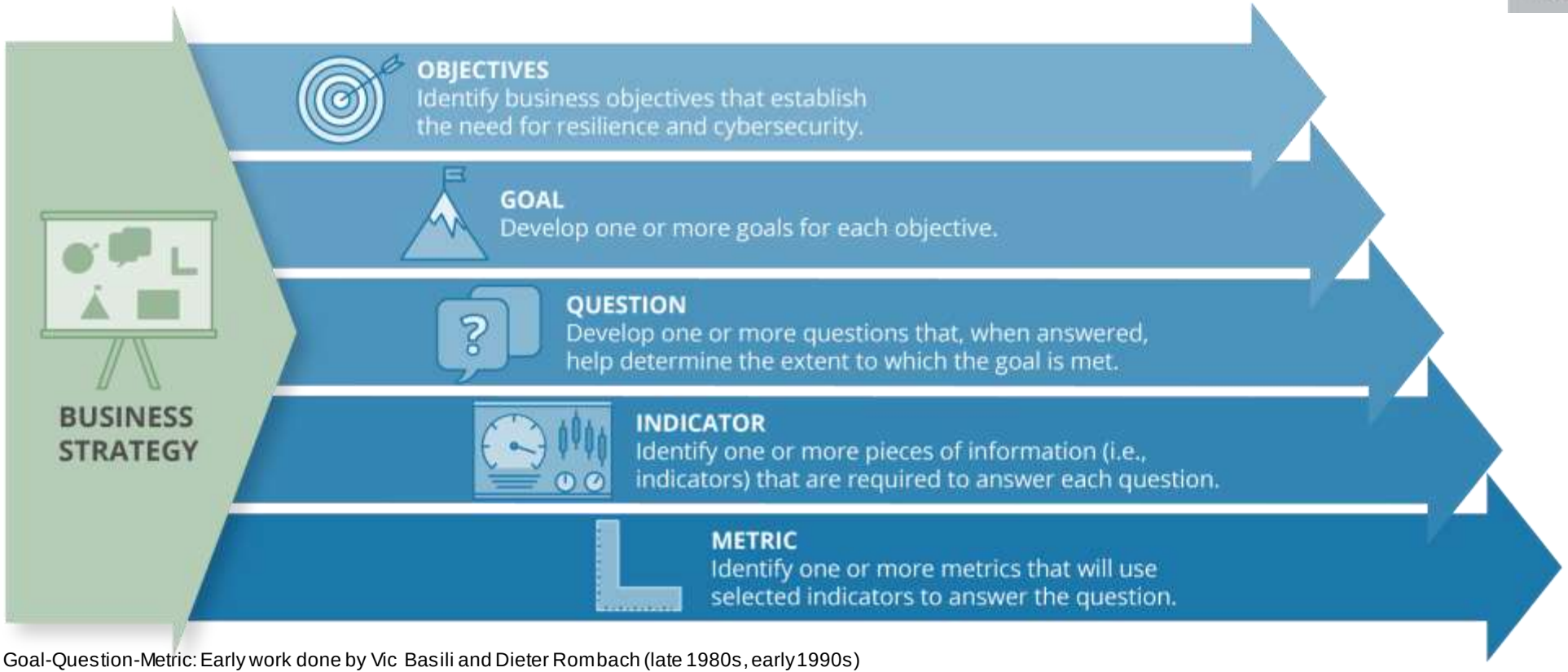
WHERE
is the data/information stored?

WHEN/HOW
frequently are the metrics collected?

WHY
is the metric important?

HOW
is the data collected and used?

GQIM as a Process



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's) and resilience (2010 to present)

Measurement Matters: The New Horizon for GQIM

Looking to the Future

Carnegie Mellon University
Software Engineering Institute

It's Not Easy – Challenges Still Exist

Organizations struggle with metrics.

- Regulatory requirements
  - where strategy and regulation collide
- Limited coordination with leadership
  - requirements versus expectations
- Quality Control (QC)
  - who, what, when, and how for data and analysis
- Metrics
  - Metrics are what organizations need.
  - Now that you measured it, what is the tolerance?
  - How do you convey the message?

Advancing the Science – Updates to GQIM

There is no plan to change the fundamental process.

There are several additional considerations to overcome gaps:

- History of “Measuring What Matters”
- Simple process – straight forward approach
- Not much of a consideration for building context

The mindset is evolving from “Measuring What Matters” to
“**Measuring Matters**.”

- Keeping the process but adding social engineering aspects

New Features for “Measuring Matters”

Changing the way people think about metrics and measures of performance

- Do not just “report” **data**; leaders need **information**.
- Risk-based decision-making means **informed** decisions.

Some of these ideas may add rigor to the process. However,

- Metrics will be more effective for informing decisions.
- Crawl-Walk-Run development enables an iterative approach.
- Building cultural context should provide better connections to stakeholders and enhance the value of the measures developed.

A Brief Overview of What Is to Come

- Introducing cultural considerations during implementation
- Improving the governance discussion
- Changing the way people think about measurement, metrics, and information
- Using stronger use-case examples
- Scaling considerations that expand beyond organizational context
- Taking a direction that supports facilitation with process questions
- Establishing a programmatic standard for building and implementing measures

Contact Information

Brett A. Tucker, PMP, CSSBB, CISSP, CGRC
Technical Manager, Cyber Risk Management

Telephone: +1 412.268.6682
Email: info@sei.cmu.edu