# Let’s be reasonable!

Pragmatic approach to measuring Digital Transformation and DevSecOps.

**Trac Bannon**
Senior Principal
Advanced Software Innovation Center

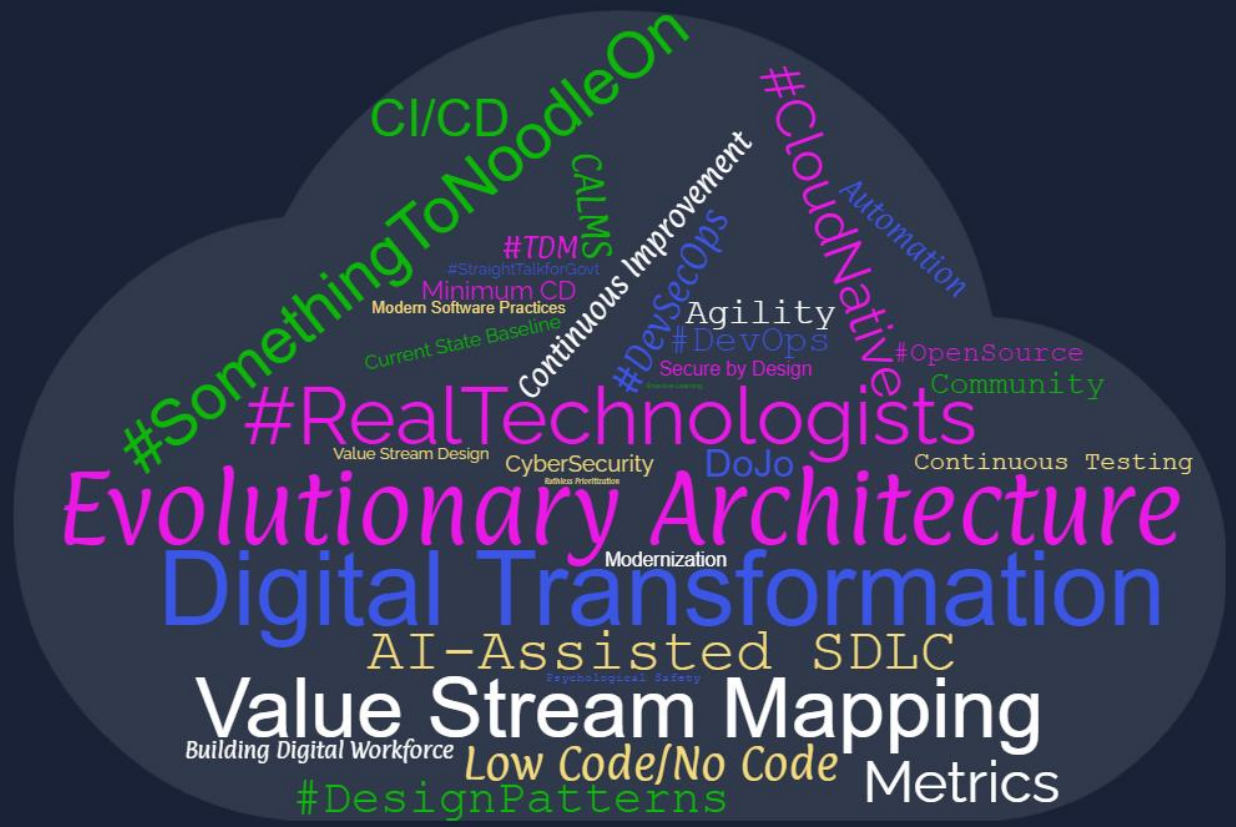
# Who Am I?

/trās/

# Tracy L. Bannon

("Trac")

Software architect | engineer | mentor | community leader




vsm consortium Influencer

AMBASSADOR DevOps Institute ADVANCING THE HUMANS OF DEVOPS

IEEE SENIOR MEMBER



MITRE

# Digital Transformation

- More that a catchy way of saying “move to the cloud” or “doing agile”
- Integration of digital technology into all areas of business or mission
- It’s a survival issue
- Adapt and adopt at speed
- Incorporates focus on customers, automation, and “radical housecleaning”
- It’s a culture change that requires continually challenging status quo, experimentation, and getting comfortable with failure

# Elements of Digital Transformation

CUSTOMER EXPERIENCE

OPERATIONAL AGILITY

CULTURE AND LEADERSHIP

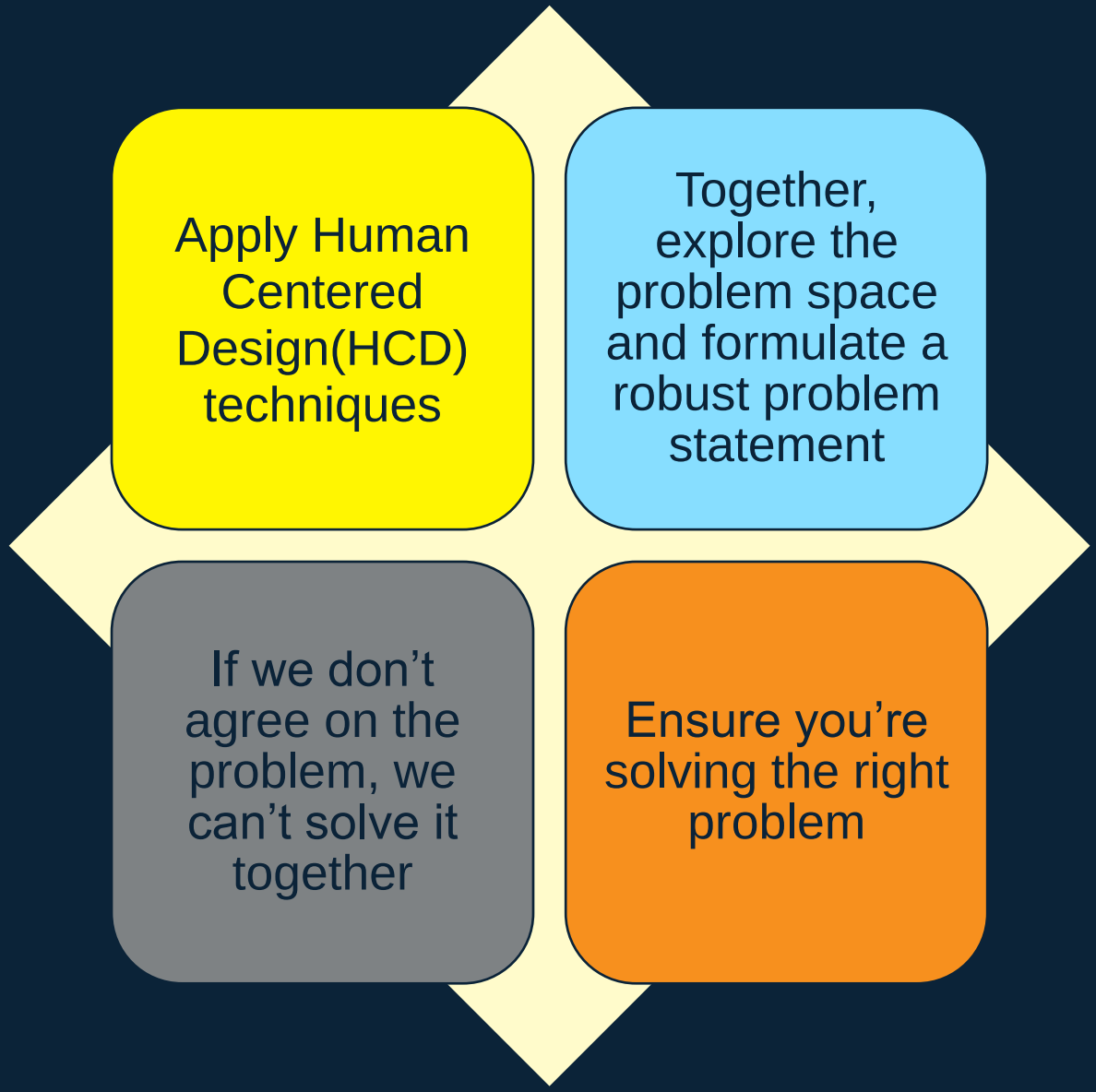
WORKFORCE ENABLEMENT

DIGITAL TECHNOLOGY INTEGRATION

MITRE

# Continuous Improvement Mindset

# Start by problem framing



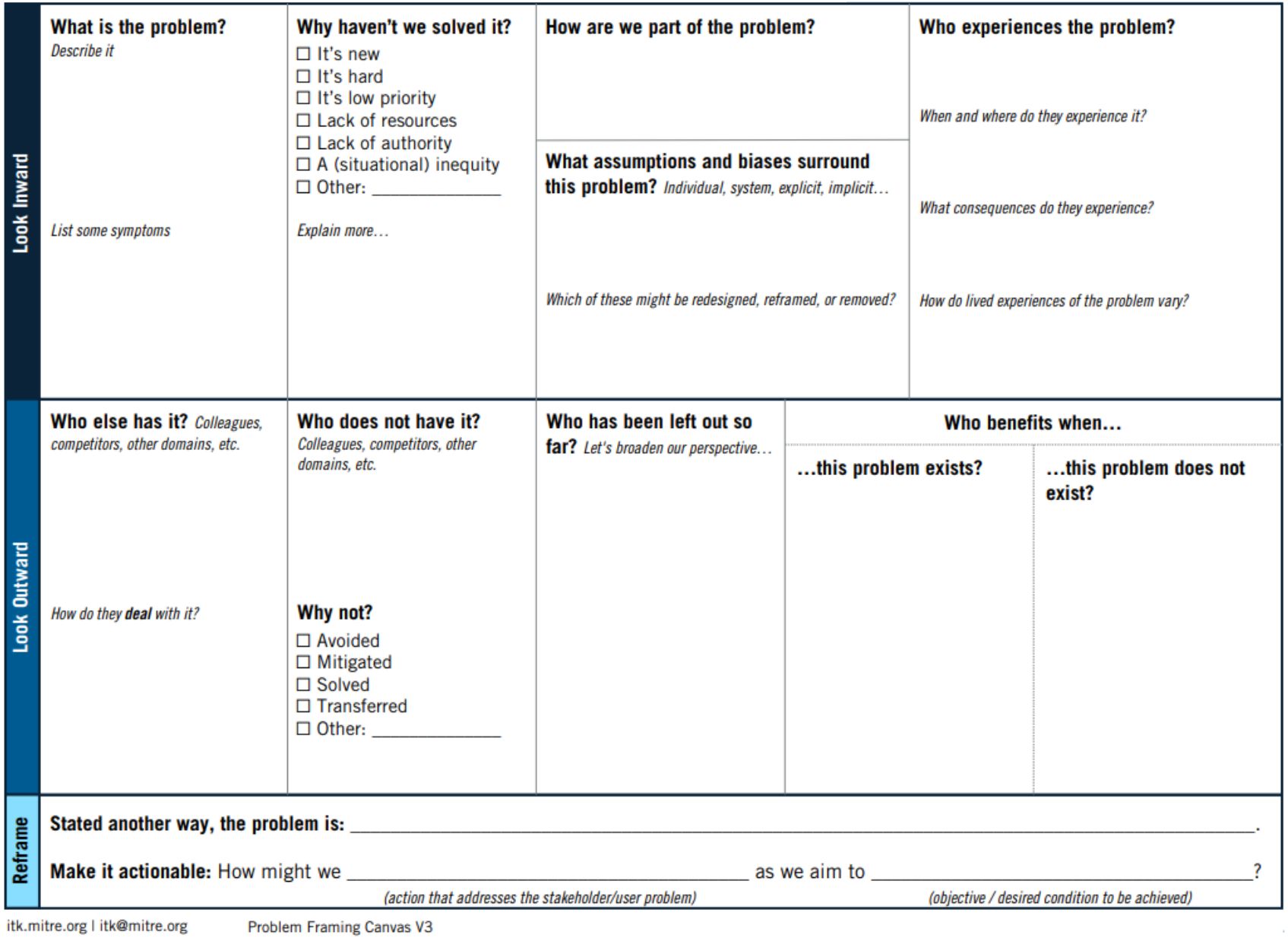

✓ Driving to a shared problem statement.

# Problem Framing Canvas:

## Defining the Right Problem

- 30-second exercise if team is on same page!
- May require some collaborative conversations with other folks to broaden your perspective.
- Requires a facilitator who knows how to lead the discussion to help the team
  - broaden their thinking
  - understand assumptions & biases they inherently bring with them,
  - think of non-primary populations/stakeholders that may be impacted

[https://itk.mitre.org/toolkit-tools/problem-framing/](https://itk.mitre.org/toolkit-tools/problem-framing/)



# Get a clear view of the current state

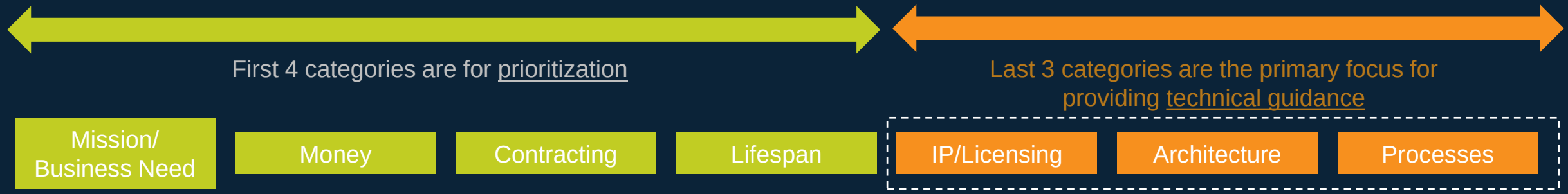
- Often, focus is on technology
- There *can* be quick wins in adopting DevSecOps principles
- Take time to understand all 7 categories of factors that reflect current state…


MITRE

# Seven Categories of Discovery

- Mission/business need
- Money
- Contracting
- Lifespan
- IP/Licensing
- Architecture
- Processes

# Holistic Information Evaluated During a Discovery Quest



# Discovery Quest Framework

## Mission/ Business Need

What is the mission capability or business need that the program provides to users?

What is the user base (size and mission)?

How mission critical is the provided capability?

## Money

What is the *current* funding situation?

How is the funding allocated to the current work efforts?

Are there additional funds needed and if so, what are they and how can they be addressed?

## Contracting

What is the current contract/subcontracting landscape?

Do they need to be renegotiated? Is there money and time to renegotiate?

Are there alternative contracting vehicles to leverage to support modern software practices?

Understand the Government/vendor relationship and possible impacts.

## Lifespan

Where is the program in its overall lifespan?

How long has the existing system been fielded?

When is divestiture?

When were they scheduled to enter sustainment?

What sorts of work need to be delivered?

Eminent replacement identified?

## IP/Licensing

What are the licensing costs for tools and software?

What is the current licensing management plan?

What types of licensing are being used? How much of the software is proprietary?

Are there legal IP challenges?

## Architecture

What is the underlying architecture for the software?

What is their technical stack dependencies?

What is the existing technical debt?

Is it organized to support modern software practices including Agility, Automations, and DevSecOps?

Interfaces and data ownership?

## Processes

What software development methodology is used?

How do requirements currently flow forward?

Are there already any DevSecOps aligned capabilities such as test automation or code scanning?

CM and governance?

**The discovery quest framework is used for both initial prioritization of programs to be reviewed as well as for creating more detailed program profiles*

Architecture does not stand alone; the ability of a program to benefit from modern software practices depends on all 7 categories

MITRE

# Discovery Quest Objectives

| Category | Objectives | Typical Supporting Documentation |
|---|---|---|
| **Mission / Business Need** | • Alternative or redundant systems to perform key mission / business functions<br>• Involved and engaged user / stakeholder base | • CONOPS<br>• System of systems analysis (CDD) |
| **Money** | • Budget for continued software improvement during sustainment<br>• Flexible expenditure of current software funding | • Program budget<br>• Commitments and obligations |
| **Contracting** | • Modular contracting; flexible contract<br>• Adaptive acquisition<br>• Stable, proven performers | • Acquisition / Contracting strategy<br>• Requirements spec / capability needs statement |
| **Lifespan** | • Low volume of new capabilities / stable feature set<br>• Iterative and incremental fielding plan leading to continuous deployment | • Program roadmaps / schedules<br>• Milestones |
| **IP/Licensing** | • Open standards<br>• Verified SBOM, continuously updated at each build<br>• Enterprise solutions for infrastructure (platform, lab, etc.) and reusable software components | • Infrastructure ”stack” diagram<br>• Tools & associated licensing<br>• SBOM & associated licensing |
| **Architecture** | • Modular, open system architecture<br>• Infrastructure that supports DevSecOps; infrastructure as code<br>• Cloud native, zero trust<br>• Defect logs/ Trouble management | • Architecture & data models<br>• ATO & interface documentation<br>• Management & automation scripts<br>• Defect logs |
| **Processes** | • Iterative and incremental system development<br>• Model-based digital engineering with shared models from requirements through operations<br>• Continuous improvement / continuous delivery (CI/CD) – including testing and monitoring<br>• Automated metrics drive continuous process improvement<br>• Localized governance (AO, CM, certification, etc.) | • SOPs, TTPs, Playbooks<br>• System Engineering Plans<br>• SW Development Plan<br>• Dashboards, performance reports |

MITRE

# Notional Current State Profile

| Improvement Area | | Strength |
|---|---|---|
| Mission Need | *Single provider of critical capability for large fielded user base* | *Small user base has access to other systems to perform key functions* |
| Money | *Insufficient to address programmatic changes* | *Budget sufficient for software modernization* |
| Contracting | *Rigid, newly renegotiated, government bears risk* | *Flexible, responsive, contractor bears risks* |
| Lifespan | *Imminent replacement, new vendor(s)* | *Lower volume of new capabilities; sufficient runway before transition* |
| IP/Licensing | *Vendor owned IP, High licensing costs, proprietary technology* | *Open or general license, full SBOM, government data rights* |
| Architecture | *Monolithic, Complex, tightly coupled, proprietary* | *Simple, scalable, modular, decoupled* |
| Processes | *Nebulous or waterfall, lack of governance, rigid* | *Well-defined, local governance, training program, agility* |

***A program profile represents the current state of modern software practices and uses qualitative evaluation***

***The groups of factors are multi-dimensional with interdependencies***

MITRE

# Improvement Plan

**What are areas where improvements can be made?**

**Prioritize against constraints and other priorities**

**Identify specific objectives and key results**

**Define the experiment (change) to move toward the objective**

# How do we measure change and progress?

How each program improves will vary based on their unique blend of factors identified during the discovery quest

# Measures and metrics are indicators

**Keep the set of metrics and measurements small and focused**

Lagging indicators assess current state

Leading indicators predict future conditions

**Organizational metrics lay groundwork**

**Avoid team level metrics; they are intended for the team to self-regulate**

**For every measurement you must ask:**

Can we get the data?

What decision can be made using the metric?

Can we impact the metric?

# Pick specific measurements based on the goal

**What will we do differently with money?**

- Money is allocated and routed differently
- Avoid duplication or eliminated redundancy

**How does the capability change?**

- Improvement in CI/CD posture
- Observable and auditable workflow

**How does this improve our security posture?**

- CI/CD practices improve cyber security posture of the software; the pipeline can be secured
- Evaluation of full software supply chain and adoption of SBOM

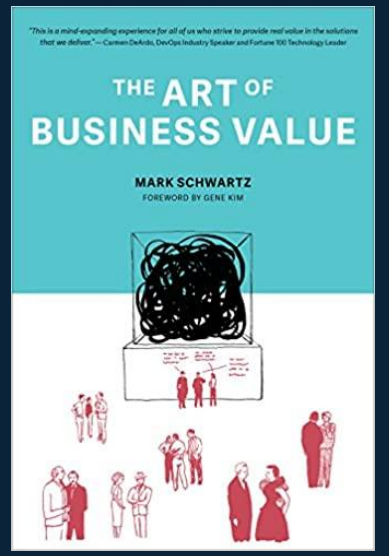
**What are our measures or indicators of improvement/success?**

- In an optimal end-state CI/CD, we would see improvements in these indicators:
  - *Faster fielding*
  - *Higher quality*
  - *More secure*
  - *Happier end-users*

MITRE

# Value goes beyond the end user or customer

While end user or customer value seems the most obvious measure, that business/mission value is unique to your context.




Mark Schwartz stated that each organization needs to identify value based on its strategies, competitors, capabilities, mission, and people.

Primary value opportunity is achieving the mission!

- ✓Are we achieving the mission value? (WHAT)
- ✓Did we get there the most effective way possible? (HOW)

# #ThoughtDiversity

Empathy and Understanding matters....otherwise it's siloed execution

It will take alignment of business and tech to provide the energy needed improve the end-to-end delivery of mission and business value

Learn from others

Leverage existing materials

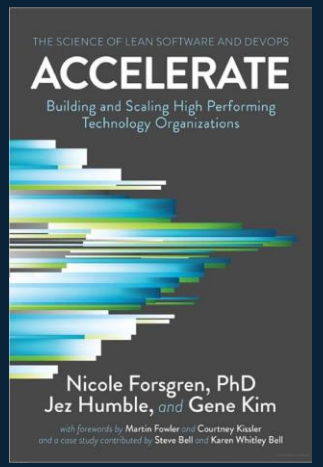
Focus on people

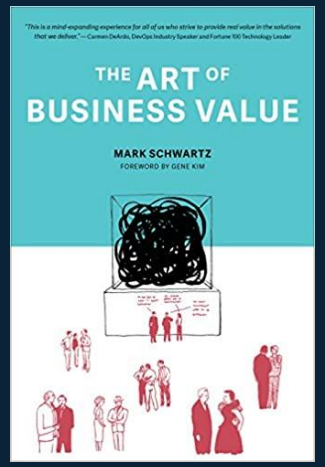
MITRE

# Resources

The Innovation Toolkit (ITK): https://itk.mitre.org/

The Value Stream Management Consortium: vsmconsortium.org




# Tracy L. Bannon

tbannon@MITRE.org

Trac@TracyBannon.tech

https://www.linkedin.com/in/tracylbannon

@TracyBannon

https://tracybannon.tech


Disclaimer: The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™