KROLL

The Missing Pieces

To Building and Adopting AppSec Capabilities

January 2023

Introduction

Jon Shapransky

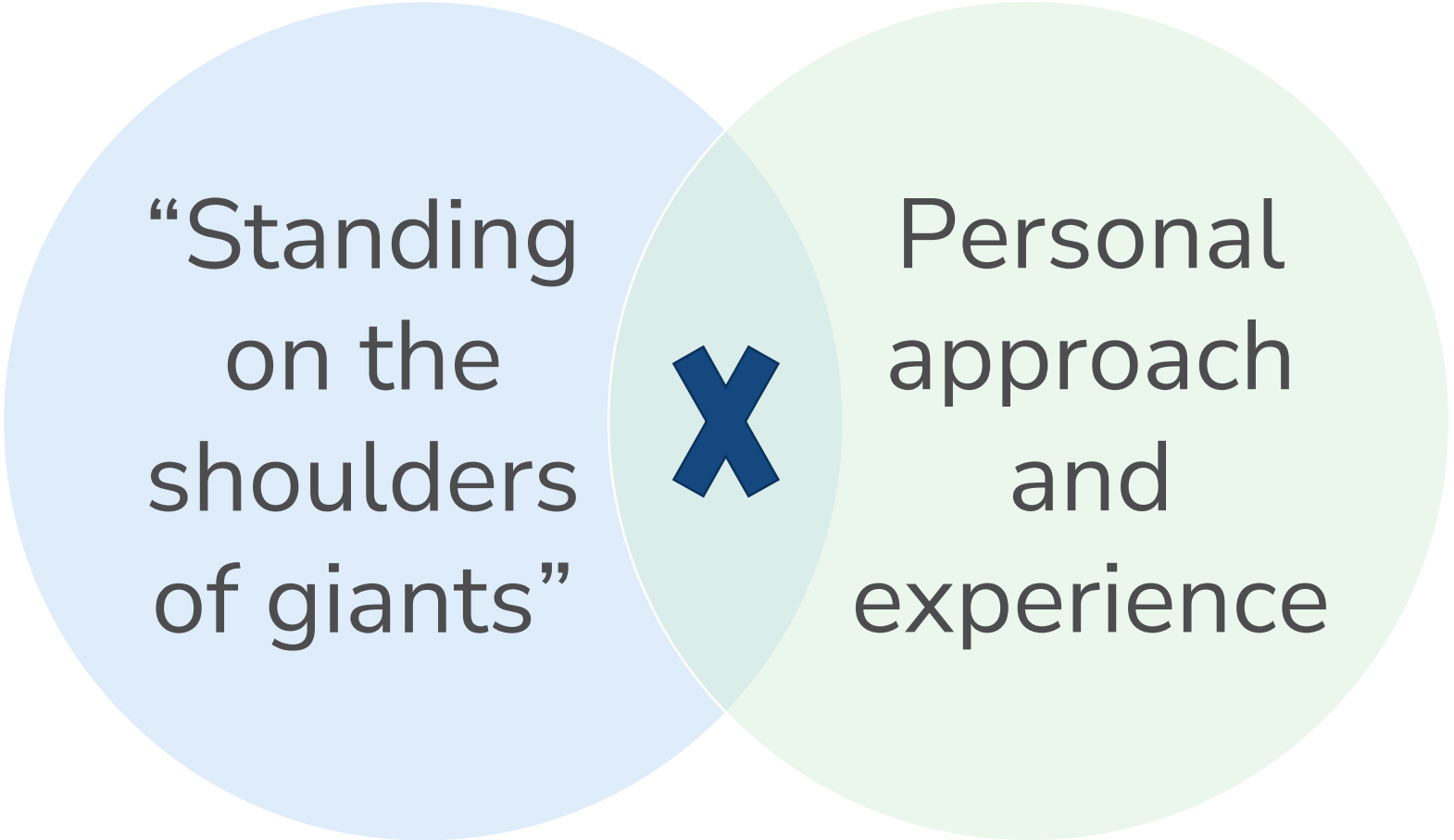
Technical Principal Consultant

Note: The above photo was taken in the “before times”.

- Technical Principal Consultant @ Kroll.
- 10+ years in security and consulting.
- Worked with public and private sector clients from startups to Fortune 100s across a variety of industries and countries.
- Presently focused on helping clients build Application Security/Product Security programs and capabilities.

KROLL

What is this talk?



Quick show of hands…

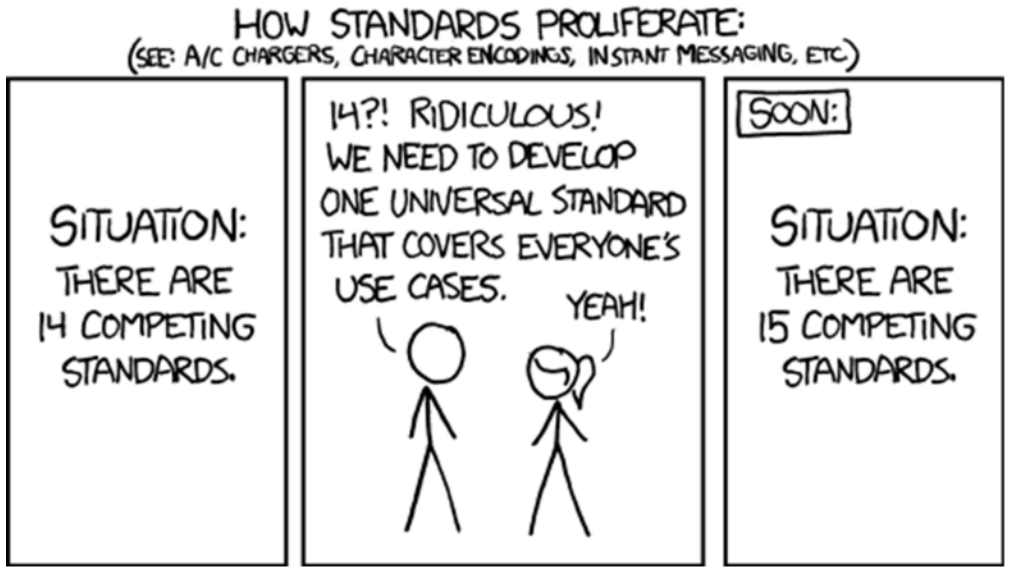
- We bought this tool X years ago and nobody is using it (and the renewal is coming up).
- The audit said we should be doing X so we bought a tool for X but we are not seeing any results.
- X is supposed to be “self-service”, but nobody has adopted it.
- We are supposed to do X, but we are not sure how or who is responsible.
- Our policy says that we must do X, but it’s often forgotten, not done, or performed too late to provide value and just causes frustrations for everyone.
- We have a team that does X, but their process isn’t “agile”, and they take too long to respond and provide their input.

Why this talk?

- A problem unidentified is a problem unresolved… and I think we have a problem.
- Organizations heavily invest and rely on tools and technology to fill capability gaps but fail at successful adoption. This results in:
  - Spending hundreds of thousands, if not millions, of dollars annually without realizing any benefits.
  - A demonstrable unresolved capability gap.
- When we fail to plan we plan to fail.
- Hope is not a strategy.

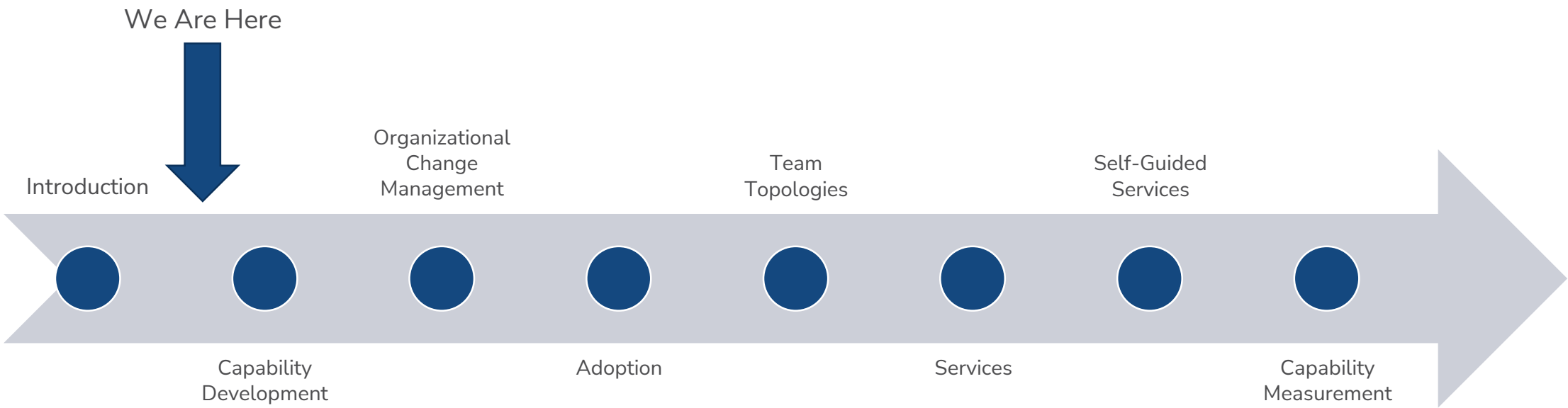
Why this talk?

- OWASP SAMM, BSIMM, NIST SSDF, NIST CSF, ISO 27034, Etc.
- We are told what we need or should be doing (i.e., industry “best practices”).
- We are told the technical how-to. (i.e., how to threat model or penetration test, etc.)
- We know the tools that help support capabilities.
- But… How should these all be implemented as capabilities? How do we get these things adopted?



Source: *https://xkcd.com/927/*

Our Journey Today



Goal for Today (Takeaways)

- A mental framework that enables you to:
  - Think about how to approach developing or improving capabilities.
  - Understand capability and service adoption.
  - Understand how team structure and interactions affect adoption.
  - Consider a different way to measure success when developing and improving capabilities that focus more on successful adoption first, results second.

Capability Development

KROLL

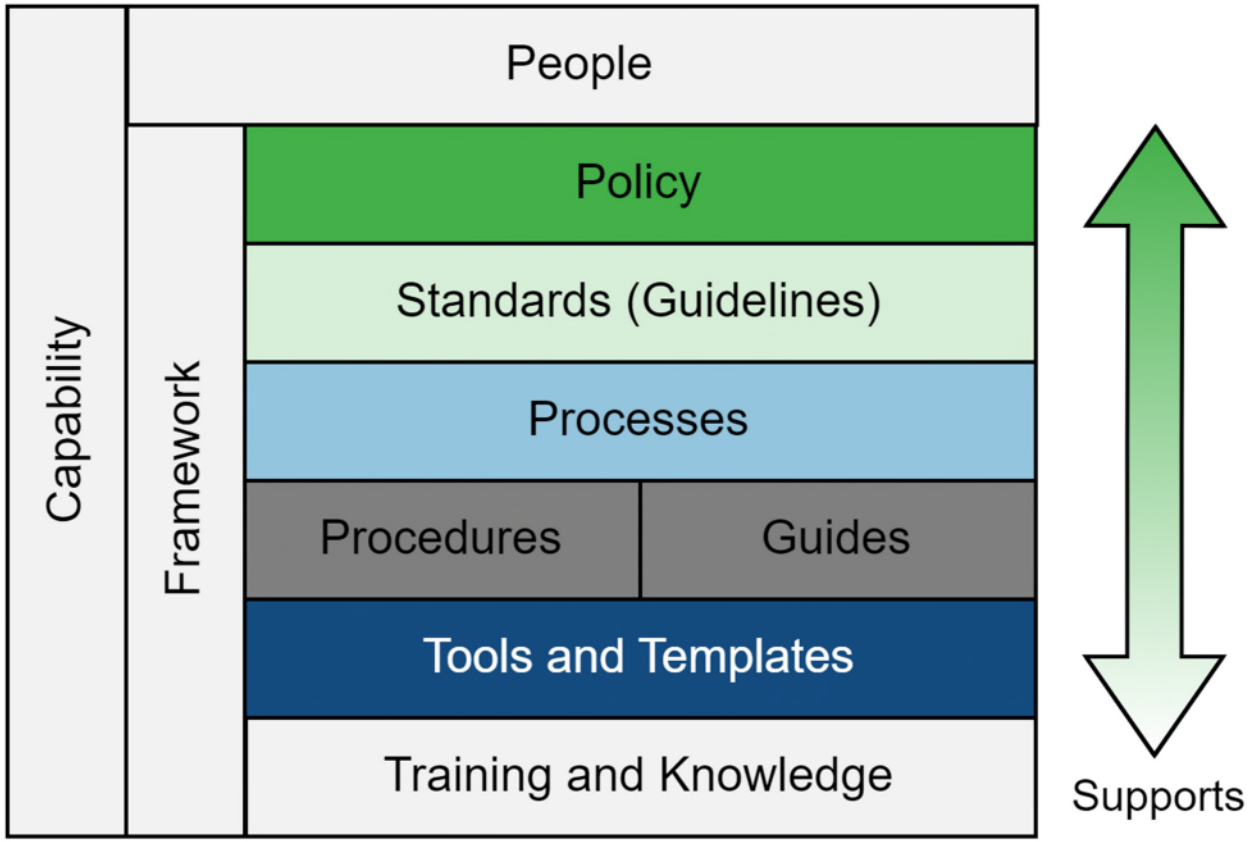
What is a Capability?

- A capability is “the ability or power to do something.”- Cambridge Dictionary
- Any activity that is supported and enabled through:
  - People
  - Process
  - Procedure
  - Technology
- Application Security capabilities are practices and processes that help us identify and/or reduce risks to improve security.
- A tool is not a capability; it only supports capabilities.

Example of AppSec Capabilities

- Examples within Application Security include:
  - Threat Modelling
  - Security Architecture Review
  - Secure Coding
  - Security Testing (Automated and Manual)
  - Risk Assessments
  - Code Review
  - Security Training
  - Vulnerability Management
  - Risk Management

Capability Framework



Capability Development Goals

- A good target CMMI maturity level is “Defined”.
- Build solid foundations to adequately support the capability:
  - Having the right people
  - Having the right governance
    - Policy
    - Standards
    - Processes and Procedures
    - Guides
  - Having the right tools
  - Having the right processes and technology integrations and automations

Capability Development Approach

Capability Development Approach

Discover | Plan | Build | Pilot | Refine | Launch

- Conduct stakeholder interviews to understand the current state and desired future state (vision).
- Conduct user experience interviews to identify current issues, challenges, pain points and opportunities for improvement.
- Review current toolset and associated documentation.
- Review current processes and procedures, configurations, usage, etc.
- Identify technology and development environment.
- Gather and define business and technical requirements.
- Understand business drivers, goals, and objectives.
- Identify dependencies and gaps.

Capability Development Approach

Discover | **Plan** | Build | Pilot | Refine | Launch

- Identify and define the definition and purpose of the capability independent of the technology and solution that will be used to support the implementation of the capability.
- Determine and define the scope and applicability including any conditions or exclusions.
- Identify the goals, objectives, and supporting metrics.
- Identify the desired future, vision, state.
- Identify program and capability enablers.
- Design capability and program architecture (i.e., processes, procedures, integrations, etc.).
- Identify and define change management plan(s).
- Identify and define an implementation roadmap.

Capability Development Approach

- Design and develop the capability framework and documentation (e.g., policies, processes, procedures, templates, etc.).
- Design and develop supporting resources (e.g., training, knowledge base content, guides, etc.).
- Tool evaluation and selection.
- Tool deep-dive to build in-depth knowledge and understand full features and capabilities.
- Identify opportunities to refine and optimize tool usage and procedures to meet capability goals.
- Develop required supporting change management communications and material.

Capability Development Approach

- Identifying between 5 and 10 teams to work with and support the pilot.
- Execute capability processes and procedures from team onboarding, training, through to execution and support.
- Conduct the pilot over a defined period to allow development teams and stakeholder groups time to adopt the new capability and provide feedback (i.e., 3 months).
- Collect feedback and adjust as-needed.

Capability Development Approach

- Deliberately and actively seeking feedback from teams involved in the pilot.
- Adjusting processes, procedures, tools, training, and related documentation based on feedback.

Capability Development Approach

- The final stage of capability development is the launch.
- Launching does not represent the end but instead represents a shift from development activities into implementation and operational activities.
- Scaling the capability beyond the pilot teams to the teams and systems in scope.
- Involves executing the implementation strategy and associated change management plan(s).
  - Performing outreach.
  - Socialization of the capability and raising awareness.
  - Onboarding teams and performing training.
  - Fully supporting the implementation and integration of the capabilities.
  - Following up to confirm that progress is going well and actively solving challenges.

Capability Development Summary and Takeaways

- An AppSec capability is any activity or practice that helps us identify and/or reduce risks to improve security.
- A tool is not a capability.
- Capabilities involve people, process(es), procedure(s), and technology.
- A good target maturity level is “defined” and therefore should include some, or all, of the capability framework.
- The development approach can be broken down into 6 phases to help us methodically plan, design, and implement capabilities to achieve a higher likelihood of success and adoption.

Organizational Change Management

KROLL

Organizational Change Management

- Application Security practices and capabilities requires a greater focus on people and processes than on IT.
- Organizational Change Management is not the same as IT Change Management.
- Methodologies to consider:
  - Prosci ADKAR
  - Lewin's 3-Stage Model of Change
  - Kotter's Eight Steps for Leading Organizational Change
  - McKinsey 7-S Model
  - Appreciative Inquiry
  - Nudge Theory

Adoption

KROLL

Defining Adoption

- Adoption is **“the process of starting to use a new method, system, law, etc.”** or **“the process of starting to use a new product or service”** – Cambridge Dictionary Business English

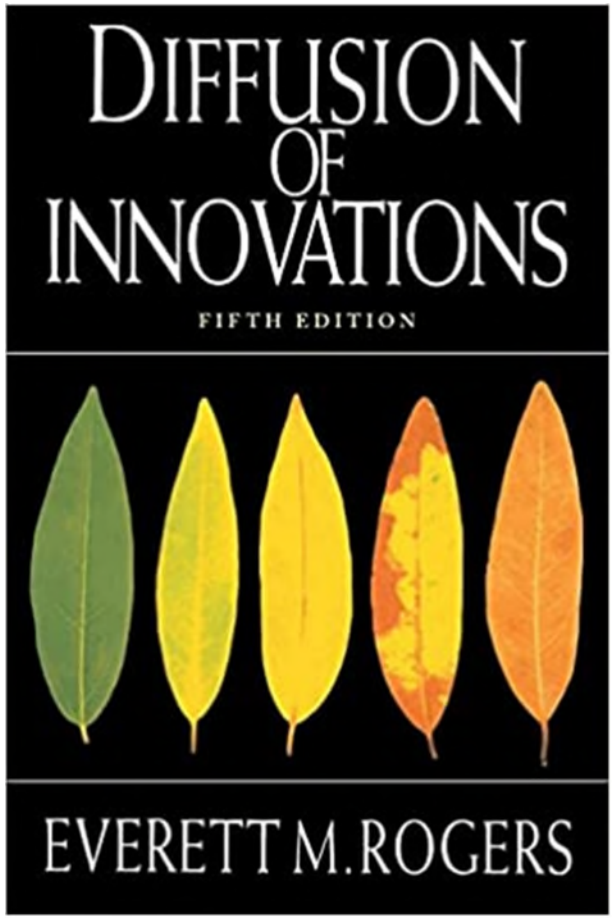
- Key word in this definition “use”.

Source: *https://dictionary.cambridge.org/dictionary/english/adoption?q=Adoption*

Adoption

- Adoption is enabled through a process of diffusion.

- **“Diffusion is the process in which an innovation is communicated through certain channels over time among members of a social system. It is a special type of communication, in that the messages are concerned with new ideas. Communication is a process in which participants create and share information with one another in order to reach a mutual understanding.”**
  – Everett M. Rogers (page 5)



Process of Diffusion

Four Elements

KROLL

1. The Innovation

- **“An innovation is an idea, practice, or object that is perceived as new by an individual or other unit of adoption.”** – Everett M. Rogers (page 12)
- Five attributes influencing rate of adoption:
    1. Relative advantage
    2. Compatibility
    3. Complexity
    4. Trialability
    5. Observability

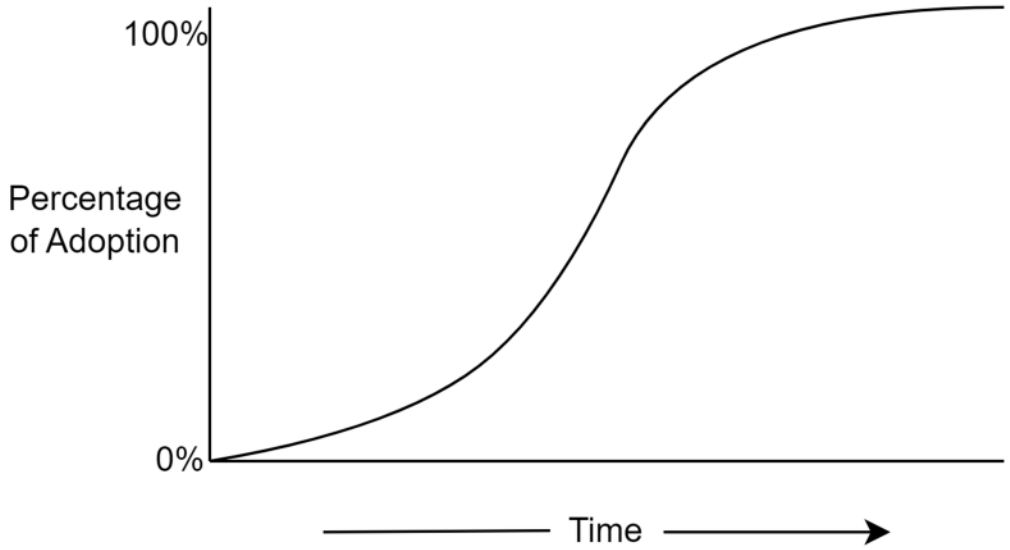
2. Communication Channels

- **“A communication channel is the means by which messages get from one individual to another.”** – Everett M. Rogers (page 18)
- Information and knowledge exchange is critical to adopting new ideas.
- Communication channels enable the exchange and may include:
  - In person discussion or meetings
  - Email or IM
  - Internal newsletter or other mass communication
  - Knowledge-base or Wiki

3. Time

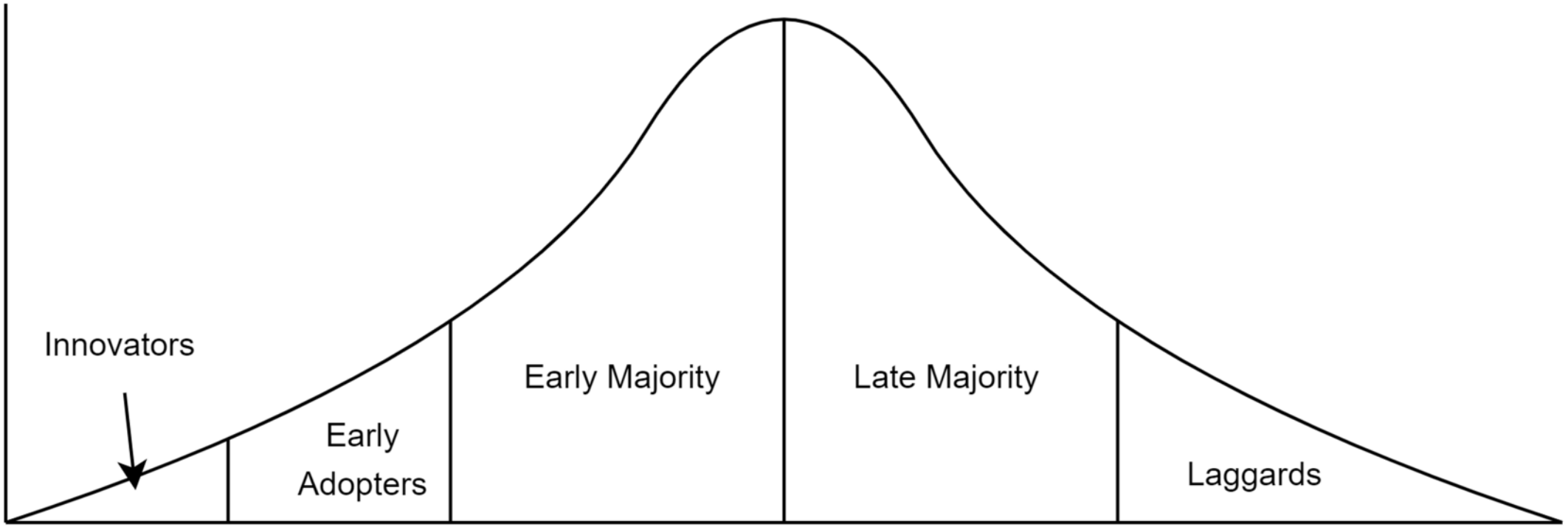
- **"... is involved in diffusion in (1) the innovation-decision process by which an individual passes from first knowledge of an innovation through its adoption or rejection, (2) the innovativeness of an individual or other unit of adoption (that is, the relative earliness/lateness with which an innovation is adopted) compared with other members of a system, and (3) an innovation's rate of adoption in a system, usually measured as the number of members of the system who adopt the innovation in a given time period."**

  – Everett M. Rogers (page 20)



Source: *A modified version of Figure 1-2. The Diffusion Process (Rogers, 2003, p. 11)*

3. Time – Adopter Categorization



Source: *A modified version of Figure 7-3. Adopter Categorization on the Basis of Innovativeness (Rogers, 2003, p. 281)*

3. Time – Innovation-Decision Process

- Five steps in the innovation-decision process:
    1. Knowledge
    2. Persuasion
    3. Decision
    4. Implementation
    5. Confirmation

3. Time – Types of Knowledge About a Change

- **Awareness-knowledge** stems from the information that an innovation exists.
- **How-to-knowledge** stems from the information necessary to use an innovation properly.
- **Principles-knowledge** stems from the information about the functioning principles underlying how an innovation works.

4. A Social System

- **“A social system is defined as a set of interrelated units that are engaged in joint problem solving to accomplish a common goal. The members or units of a social system may be individuals, informal groups, organizations, and/or subsystems.”**

  – Everett M. Rogers (page 23)

Controlling Rate of Adoption and Factors in Change Success

- Success in securing adoption is positively related to…
  - The extent of **change-agent effort** in contacting clients.
  - **Client orientation**. Change agents that have a closer rapport with their clients enjoy higher credibility in the eyes of their clients and base their diffusion activities primarily on clients' needs.
  - The degree to which a diffusion program is **compatible with clients' needs**.
  - **Change agent empathy** for clients.

Adoption Summary and Takeaways

- We can help others help us by doing the work necessary to achieve the desired level of adoption.
- Using the Process of Diffusion
  - We can increase adoption success by considering the the five attributes influencing rate of adoption and creating a favourable environment to enable adoption.
  - A capability cannot be adopted without awareness and knowledge about the capability which requires communication.
  - Adoption takes time and adopters go through an innovation-decision process. Supporting this process is critical.
  - Knowledge is a key part of this process and different groups and adopters require different levels of knowledge.
- Adopter categories help explain why some easily adopt new practices while others resist.
- Our pilots are best suited for Innovators and Early Adopters to help us with testing changes and provide early and observable results.

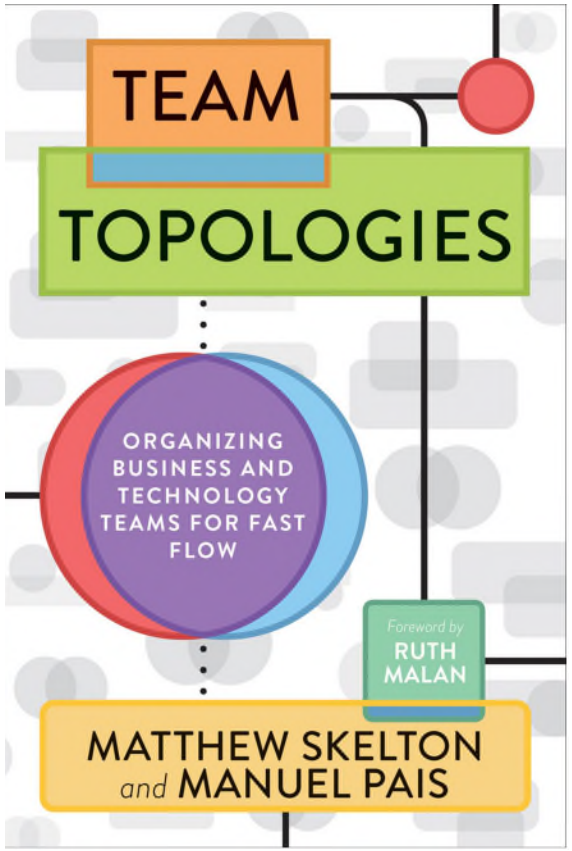
Team Topology

KROLL

Team Topology

- **“Team Topologies: Organizing Business and Technology Teams for Fast Flow”**

  Matthew Skelton and Manuel Pais (2019)



Why Think About Team Topology?

- **“Team Topologies clarifies team purpose and responsibilities, increasing the effectiveness of their interrelationships.”** – Skelton and Pais (page 2)
- Changes how view ourselves as components in a larger system.
- Changes how we approach achieving our collective goals and objectives.
- Helps us better understand our teams’ priorities and focus helping better manage our cognitive load (team capacity) and become more aware of the cognitive load of others.

Topologies According to Skelton and Pais

Stream-Aligned

Enabling

Complicated-Subsystem

Platform

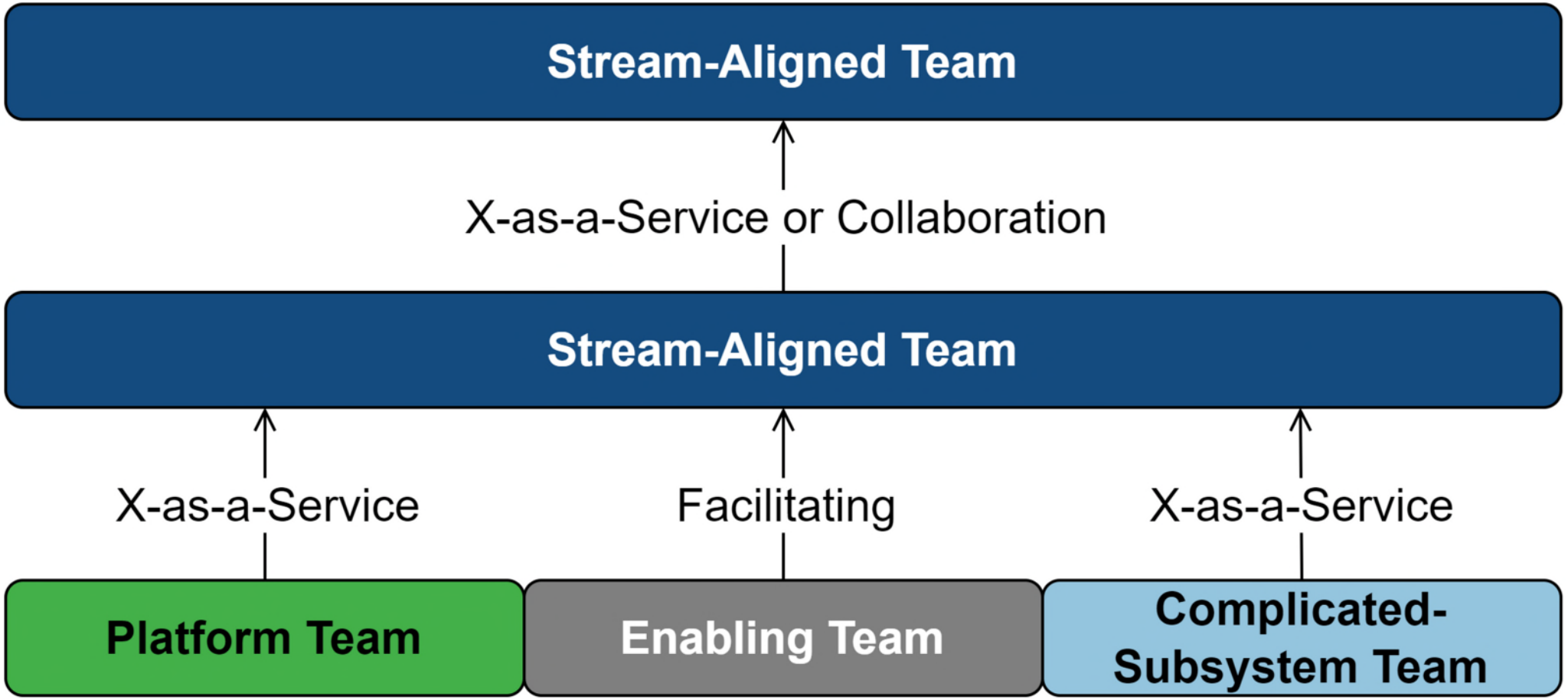
Interaction Modes

Collaboration

X-as-a-Service

Facilitating

Topologies and Common Interaction Modes



Source: *A summarized depiction of Table 7.4: Team interaction modes of the fundamental team topologies (Skelton & Pais, 2019, p. 144)*

KROLL

Services

KROLL

Capabilities and Services

- Capabilities are often realized and delivered through services.
- Services involve interaction(s) between two parties.
- One acts as a service provider, whether internal or external, and the other the customer consuming the service.

Definition of Service

- **“The application of specialized competences (knowledge and skills) through deeds, processes, and performances for the benefit of another entity or the entity itself”**

  – Adam Tacy (2021)

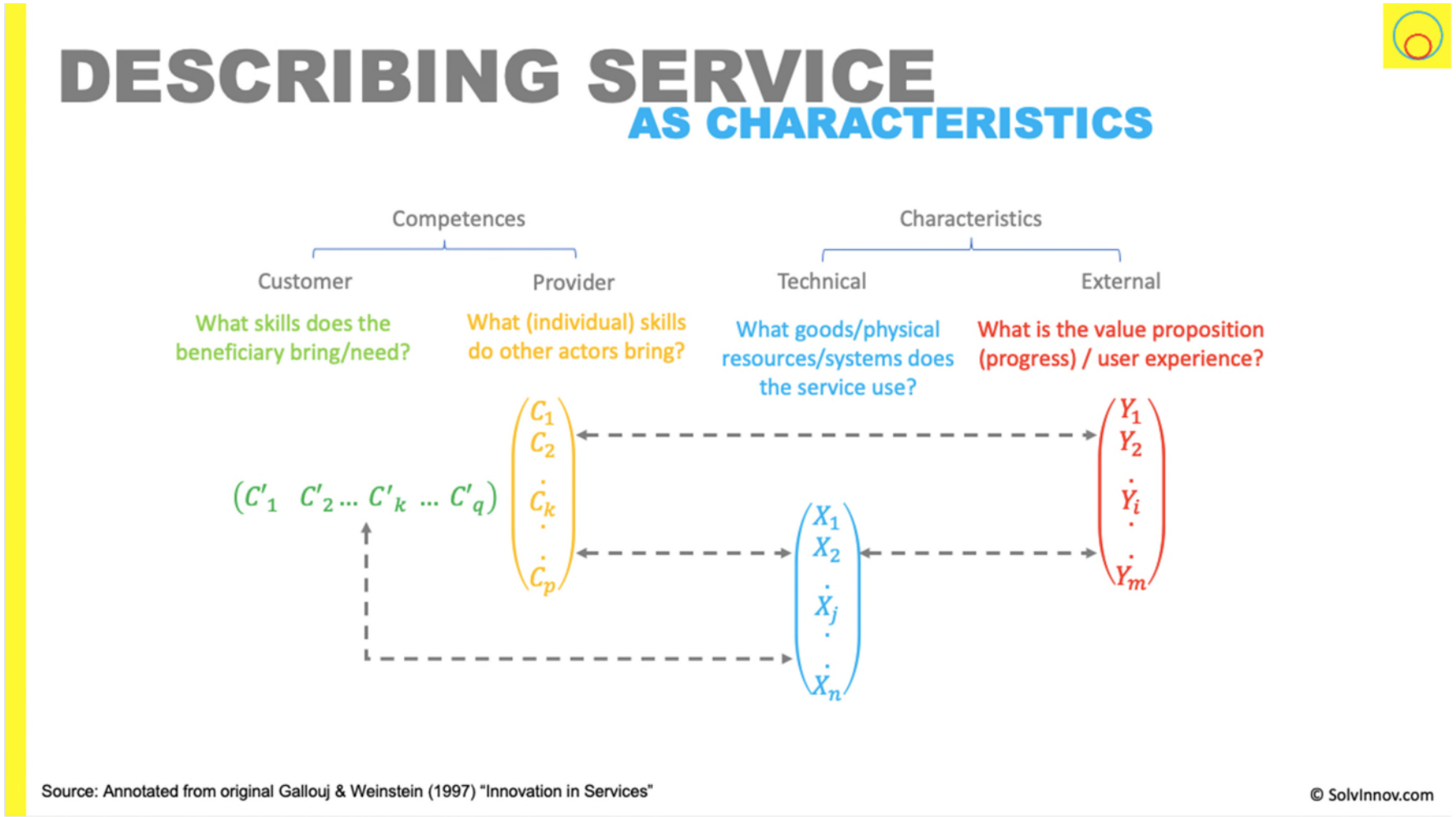
- **“A service is a process consisting of a series of more or less intangible activities that normally, but not necessarily always, take place in interactions between the customer and service employee and/or physical resources or goods and/or systems of the service provider, which are provided as solutions to customer problems.”**

  – Christian Grönroos (2000)

Quick Tangent…

- There is a great website (https://solvinnov.com/) by Dr. Adam Tacy that contains articles/blogs, summaries, and references to related material and many of the material I've used in this section and throughout presentation.
- Dr. Tacy has referenced and cited their material which is very useful and refreshing in a world of unsourced blog material.

Describing Service as Characteristics

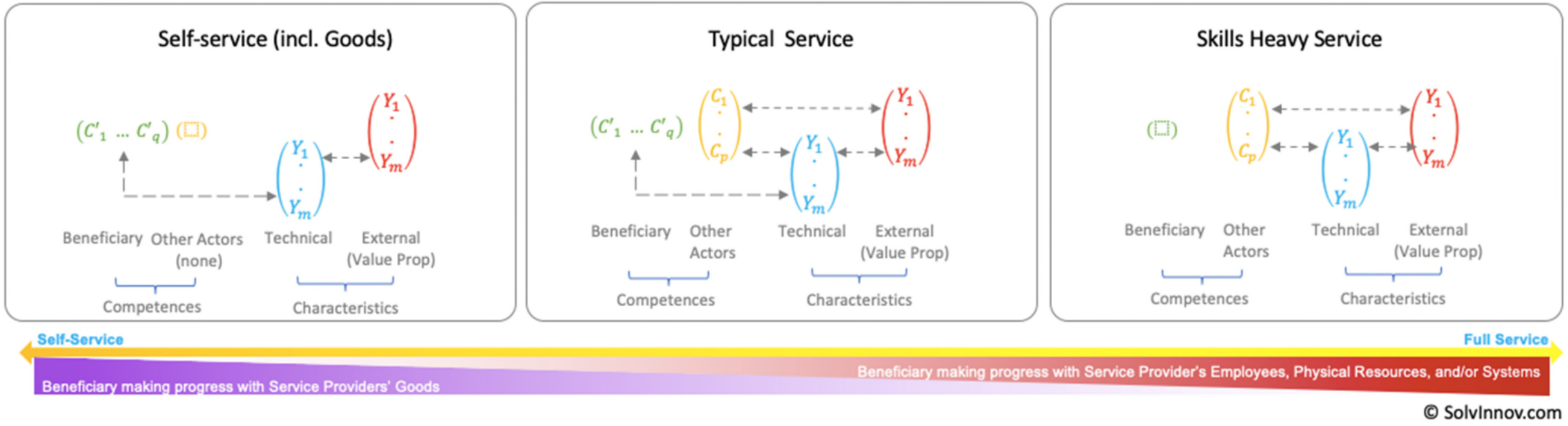


Source: *https://solvinnov.com/a-model-for-describing-a-service-and-better-still-systematically-discovering-services-innovations/*

Original Source: https://shs.hal.science/halshs-01133098/document

KROLL

Service Types



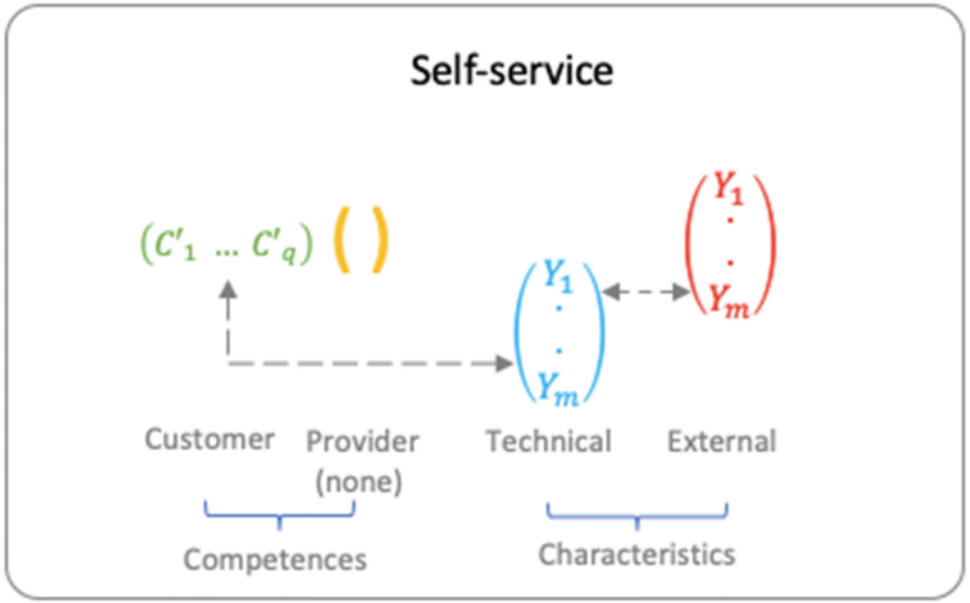
Source: *https://solvinnov.com/service-as-characteristics-examples/*

Self-Guided Services

KROLL

Self-Guided Services (Self-Service)

- Self-service is a target state of autonomy where consumers of a capability can perform the capability without the support of specialists.
- Self-service requires a platform to enable competence transfer from provider to consumer.
- Enabling adoption of a self-service capability requires
  - Awareness
  - Education and training
  - Post-training reinforcement
  - Supporting documentation
  - Tools
  - Automation
  - Support services
  - Clear guidance and expectations



Source: *https://solvinnov.com/a-model-for-describing-a-service-and-better-still-systematically-discovering-services-innovations/* ©solvinnov.com

Capability Measurement

Defining Success

KROLL

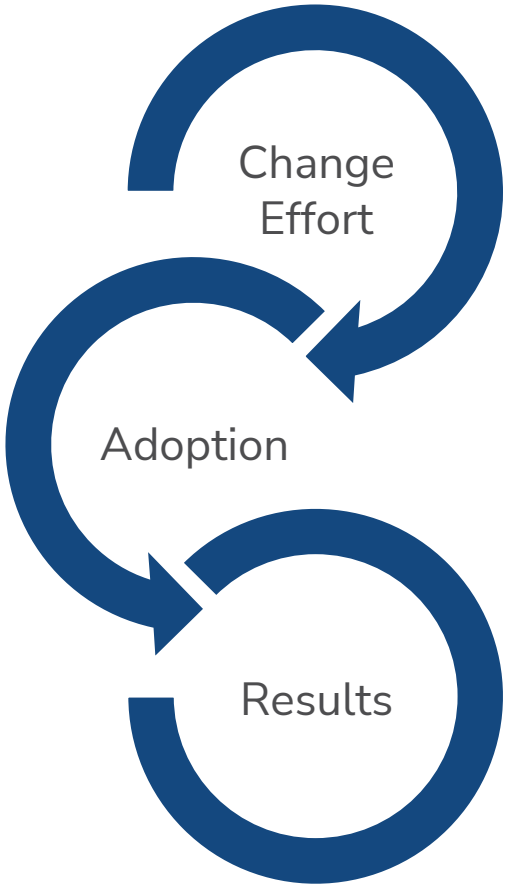
Common Results-Driven Approach

- Capabilities are frequently measured on results only informed by superficial metrics.
- Using data generally readily available in our tools.
- Examples:
  - Number of vulnerabilities identified
  - Reduction in vulnerabilities in a defined time period
  - Number of security assessments performed
- **Problem: When implementation and operationalizing a capability, results don't tell us the entire picture and therefore cannot adequately support decision making.**

If not results, then what?

- **“’Change agents’ success in securing the adoption of innovations by clients is positively related to the extent of change agent effort in contacting clients.”**

  – Everett M. Rogers (page 373)



Thank You

KROLL

For more information, please contact:

Jon Shapransky

Email: jon.shapransky@kroll.com

Twitter: @Jon.Shapransky

Mastodon: @Jon.Shapransky@infosec.exchange

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.