

VALUE DRIVEN SECURITY

Roadmapping to Business Alignment

By Avi Douglan

BLUF:

Don't be generic

Map the value streams

Focus on what actually matters

I am... **Avi Douglen**








Researcher / Consultant / Architect / Advisor

AviD@BounceSecurity.com

Socials: [@sec_tigger](https://twitter.com/sec_tigger)

He / Him

Product Security Consulting  **Bounce**
SECURITY

- OWASP Israel Leader 
- Global Board of Directors 
- Privacy Reference Project Leader 
- Moderator [Security.StackExchange](https://security.stackexchange.com) 
- Co-Author, TM Manifesto 



Agenda

- Does security really matter?
 - *“Best Practices” and other generic guidance*
- Going on a journey
 - *Discovering the real goals and challenges*
- Strategic approach
 - *Wardley maps*
- Value Driven Roadmapping

Does Security Really Matter?

“Best Practices” and other generic guidance

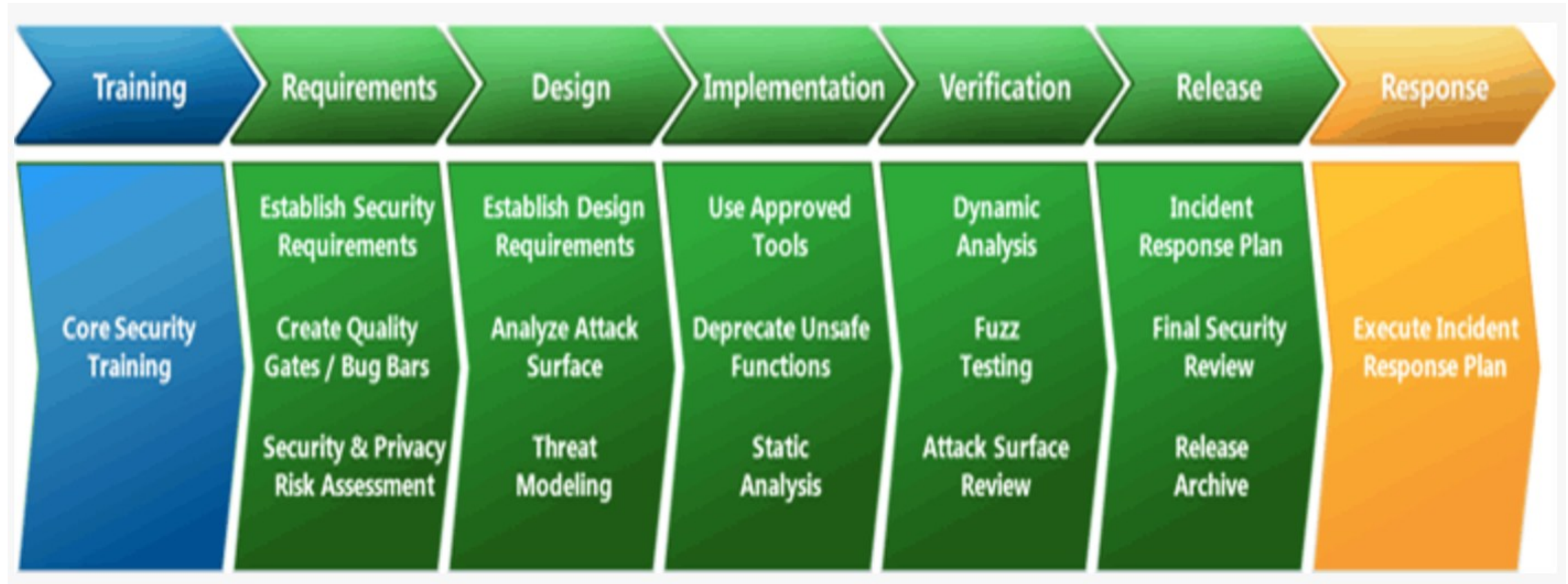
The Impact of Security

- Of course (!!)
- Of course (!!) we all need security
- Thought experiment: what does security actually do?
 - *“No one sees if you’re doing a good job”*
 - *No attacks == good security?*
- Is security merely insurance?
 - *Cost of doing business? Corporate tax?*

The Impact of Security

- Or can security actually add real value...
 - *More efficient development?*
 - *Quicker sales?*
 - *Reputation-based marketing?*
 - *Premium features?*
 - *Or yes, even risk management*
- Answer: IT DEPENDS.

Generic Security Practices



Generic Security Practices

- There is a LOT to do
- Not all of it applies
- Not optimized for specific environment
- Diminishing returns

Governance

Strategy and Metrics

Create and
promote

Measure and
improve

Stream A

Stream B

Design

Threat Assessment

Application
risk profile

Threat
modeling

Stream A

Stream B

Implementation

Secure Build

Build
process

Software
dependencies

Stream A

Stream B

Verification

Architecture Assessment

Architecture
validation

Architecture
mitigation

Stream A

Stream B

Operations

Incident Management

Incident
detection

Incident
response

Stream A

Stream B

Policy and Compliance

Policy &
standards

Compliance
management

Stream A

Stream B

Security Requirements

Software
requirements

Supplier
security

Stream A

Stream B

Secure Deployment

Deployment
process

Secret
management

Stream A

Stream B

Requirements-driven Testing

Control
verification

Misuse/abuse
testing

Stream A

Stream B

Environment Management

Configuration
hardening

Patch and
update

Stream A

Stream B

Education and Guidance

Training and
awareness

Organization
and culture

Stream A

Stream B

Secure Architecture

Architecture
design

Technology
management

Stream A

Stream B

Defect Management

Defect
tracking

Metrics and
feedback

Stream A

Stream B

Security Testing

Scalable
baseline

Deep
understanding

Stream A

Stream B

Operational Management

Data
protection

Legacy
management

Stream A

Stream B

The Fallacy of “Best Practices”

- Least common denominator
- Everyone follows them (supposedly)
- Everyone still gets hacked...
- Attackers know the best practices too
- Best practices should be followed – until you know better
 - *Beware Dunning-Kruger of course...*

Missing the Context

- What does your product do?
- How does it do it?
- Who is doing it?
- Why is this a priority?
- Where else can your product connect?

Going on a Journey

Discovering the real goals and challenges

Security as a Journey

- You need to understand where you're going!
 - *How long it will take*
 - *Where are we coming from*
 - *How much fuel (budget) you will need*
 - *What challenges face us along the way*
- Our immediate goal:
 - ***Reduce overall risk with cost-efficient tasks aligned with overall business priorities***

Customizing Security

- OWASP SAMM can give you good current status
 - *Do we need everything in it?*
 - *Non trivial effort to keep current*
- Same with every other standard...
 - *Either significantly irrelevant*
 - *Or expect to heavily customize blindly*

Customizing Security

- How should you customize your SDLC?
 - *Just do everything*
 - *Write everything in policy, implement whatever*
 - *Only what the VP R&D agrees*
 - *Measure what we can fit in %XX*
 - *Guess which tasks will be least friction*
 - *Security team will do it all*
 - *Give up*

What are we trying to achieve?

- Reduce total number of attacks this year / next release
- Reduce total impact of breaches
- Shorten window of attack for published vulnerabilities
- Optimize developer time after failed pentest
- Compliance (with regulations / customer policies)
- Protect CISO's ~~a**~~ job
- “Have an appsec program”

What will stop us?

- Executive buy-in
- Developer buy-in
- Lack of resources / time / budget
- Unsupportive culture
- Friction between R&D and Infosec (eg language)
- Misaligned priorities
- Legacy architecture

How do we get there from here?

- Start by Security and Dev working together...
 - *and product, and QA, and Devops, and and....*
- Need flexibility and willingness to change culture
- Aligning by business priorities

Strategic Approach

Wardley maps

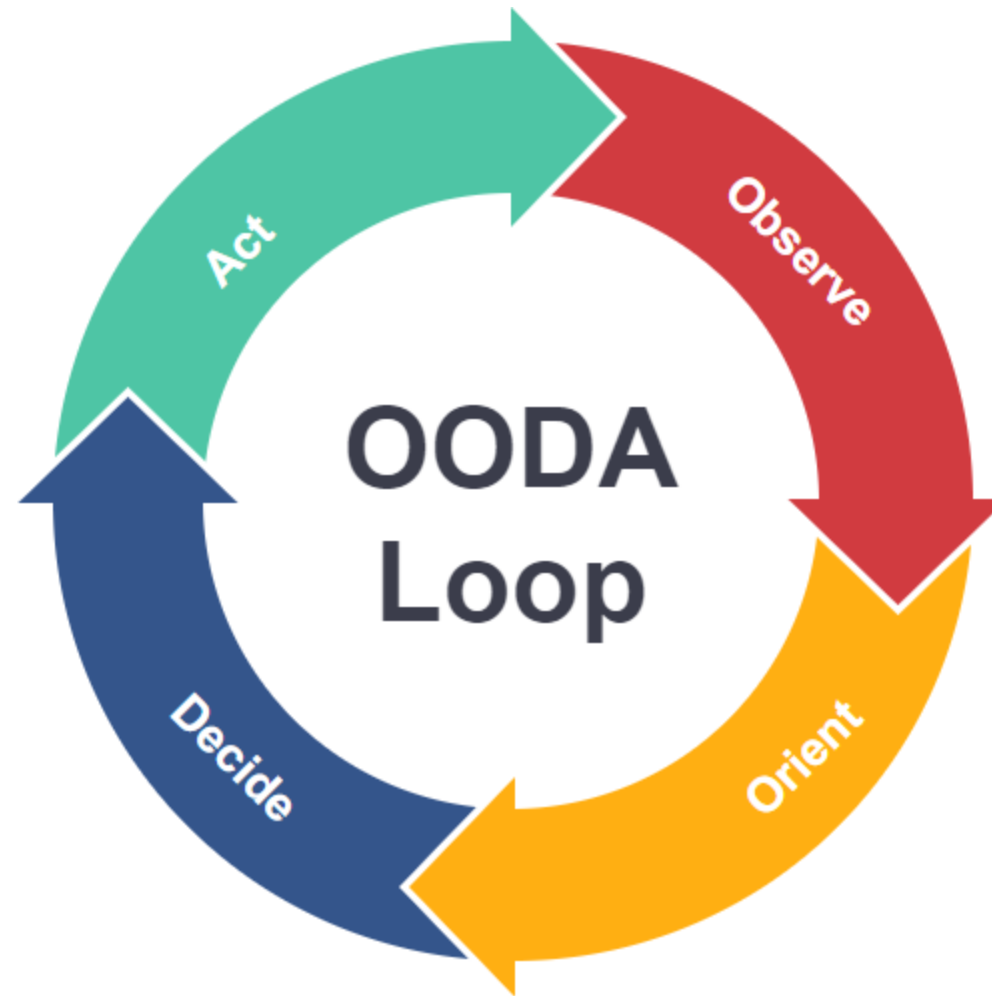
What is “strategy”?

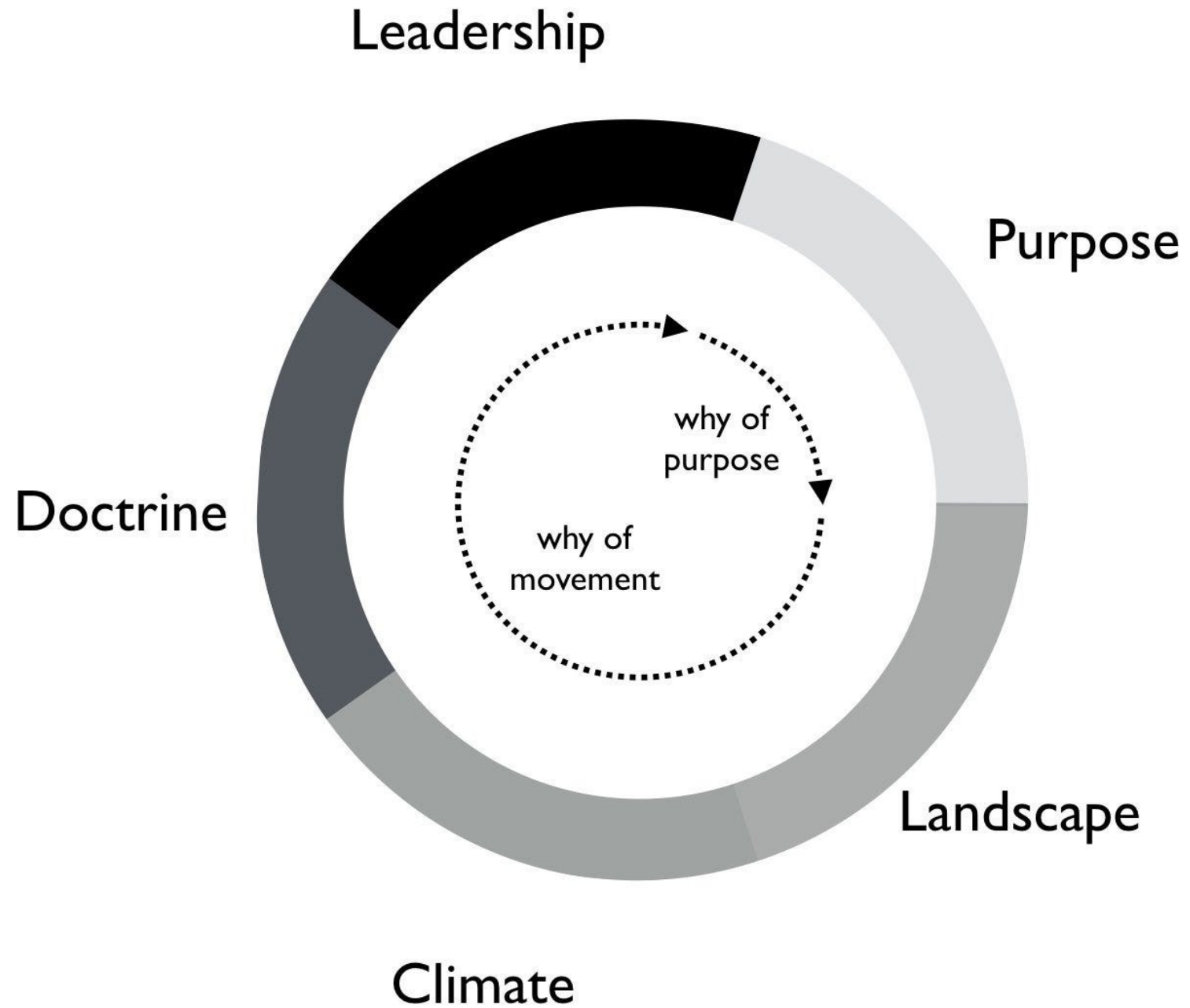
Our strategy is innovative. We will lead a self learning effort of the market through our use of large language model and hyperautomation workflows to build a human in the loop. By being both responsible and human centric, our collaborative approach will drive design thinking throughout the organization. Synergies between our value and autonomous agent will enable us to capture the upside by becoming disruptive in a sustainable world. These transformations combined with digital transformation due to our data mesh nodes will create a platform through blockchain and edge devices.

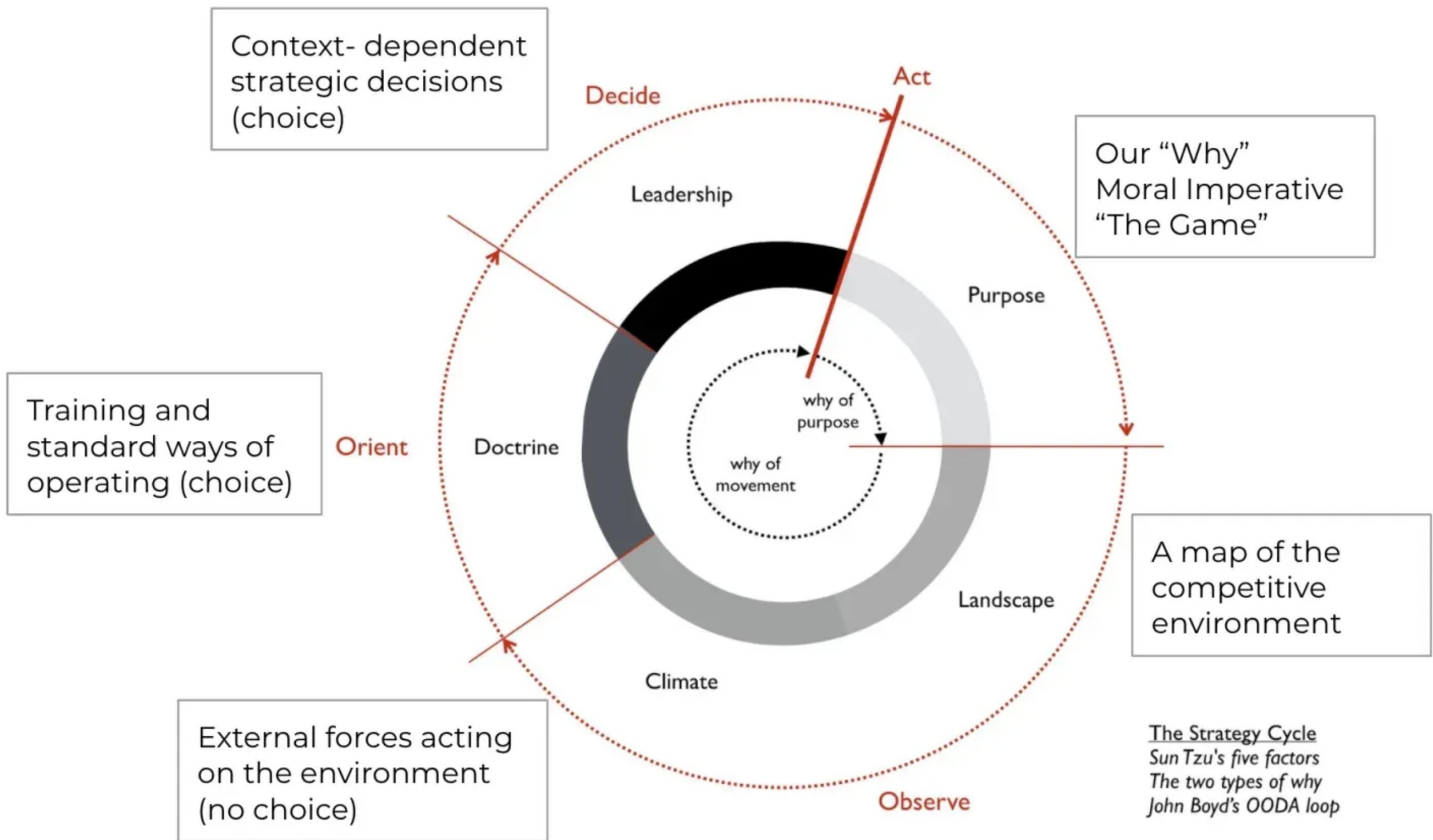
<https://strategy-madlibs.herokuapp.com/> h/t Simon Wardley

What is “strategy”?

- A list of tasks!
- OKRs
- Wishlist
- Imaginary thinking
- Set of goals based on understanding of the context that will change with situational awareness



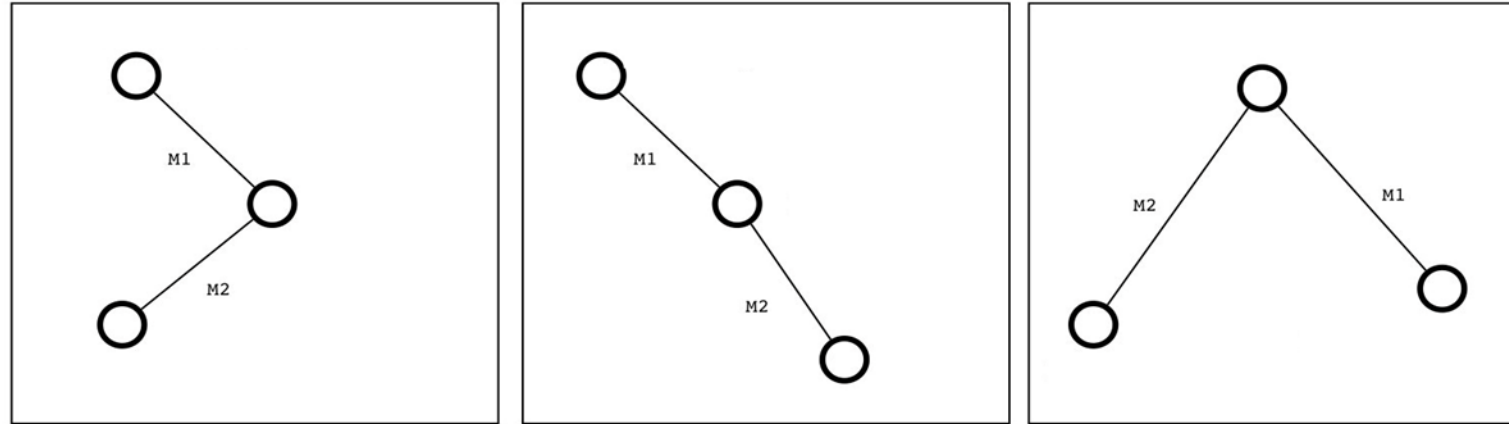




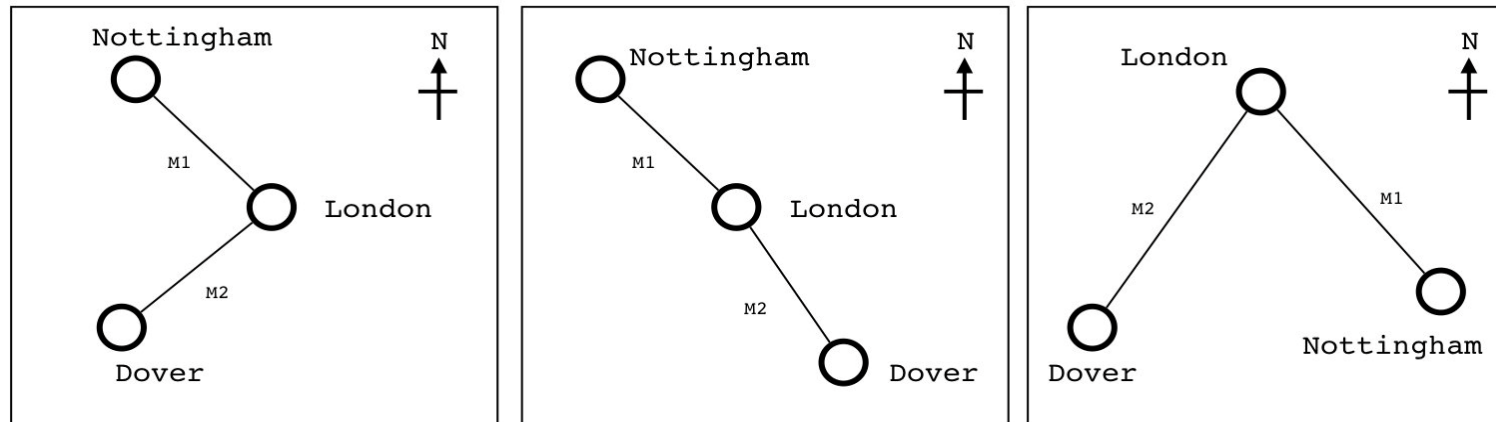
We need a map!

- Shows where things are in relation to other things
 - *Provides context*
 - *Location is important*
 - *Direction is important*
- Not static
 - *Maps can change*
 - *Movement is vital*
- Identify areas of possibilities

Graphs and Maps

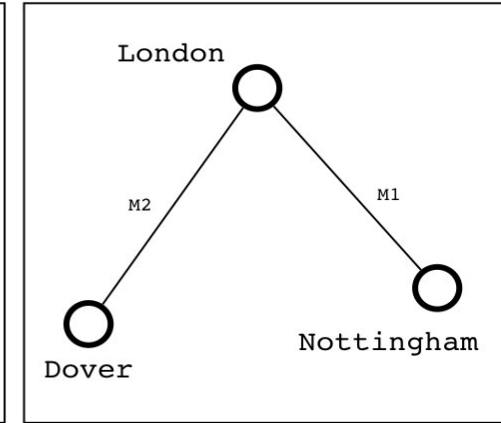
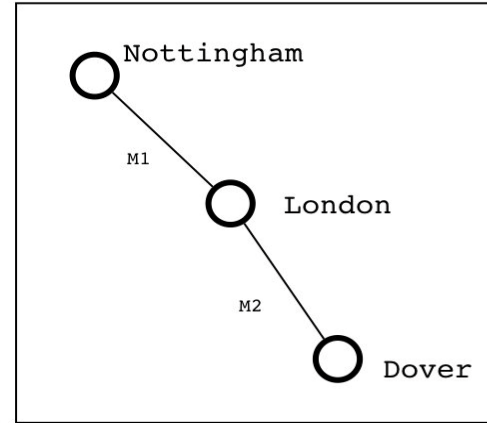
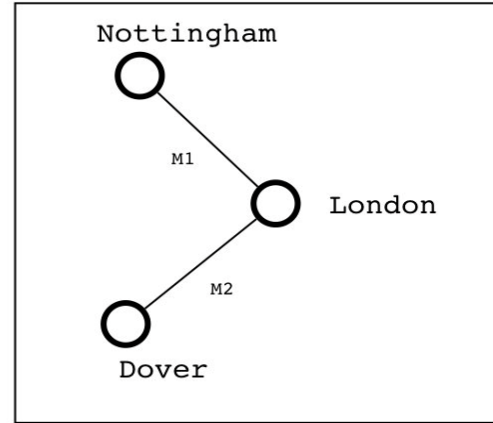


Graphs and Maps

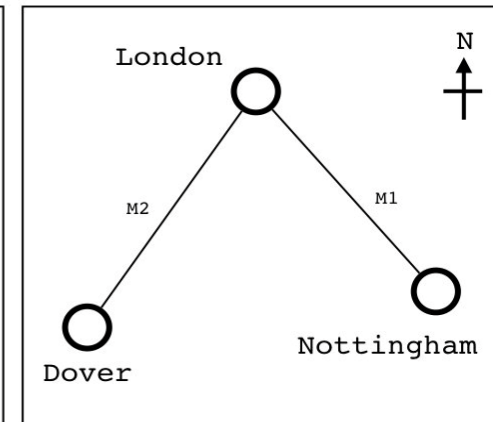
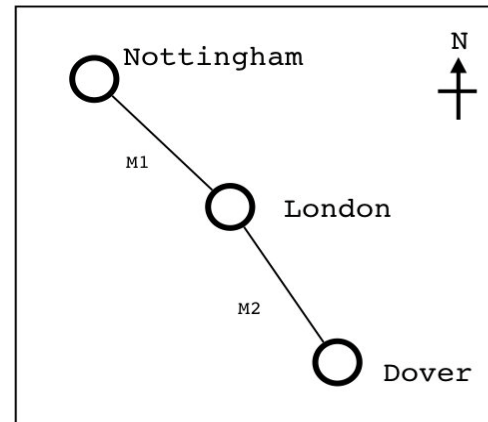
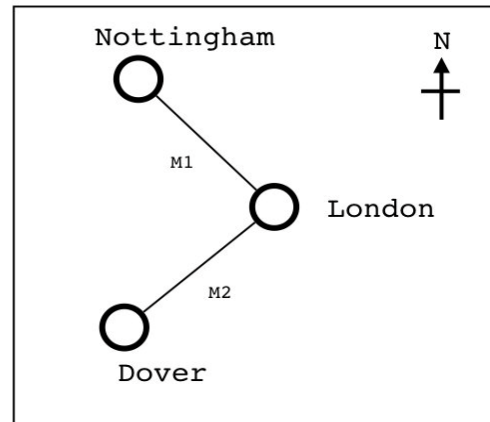


Graphs and Maps

**THESE THREE
GRAPHS
ARE THE
SAME**



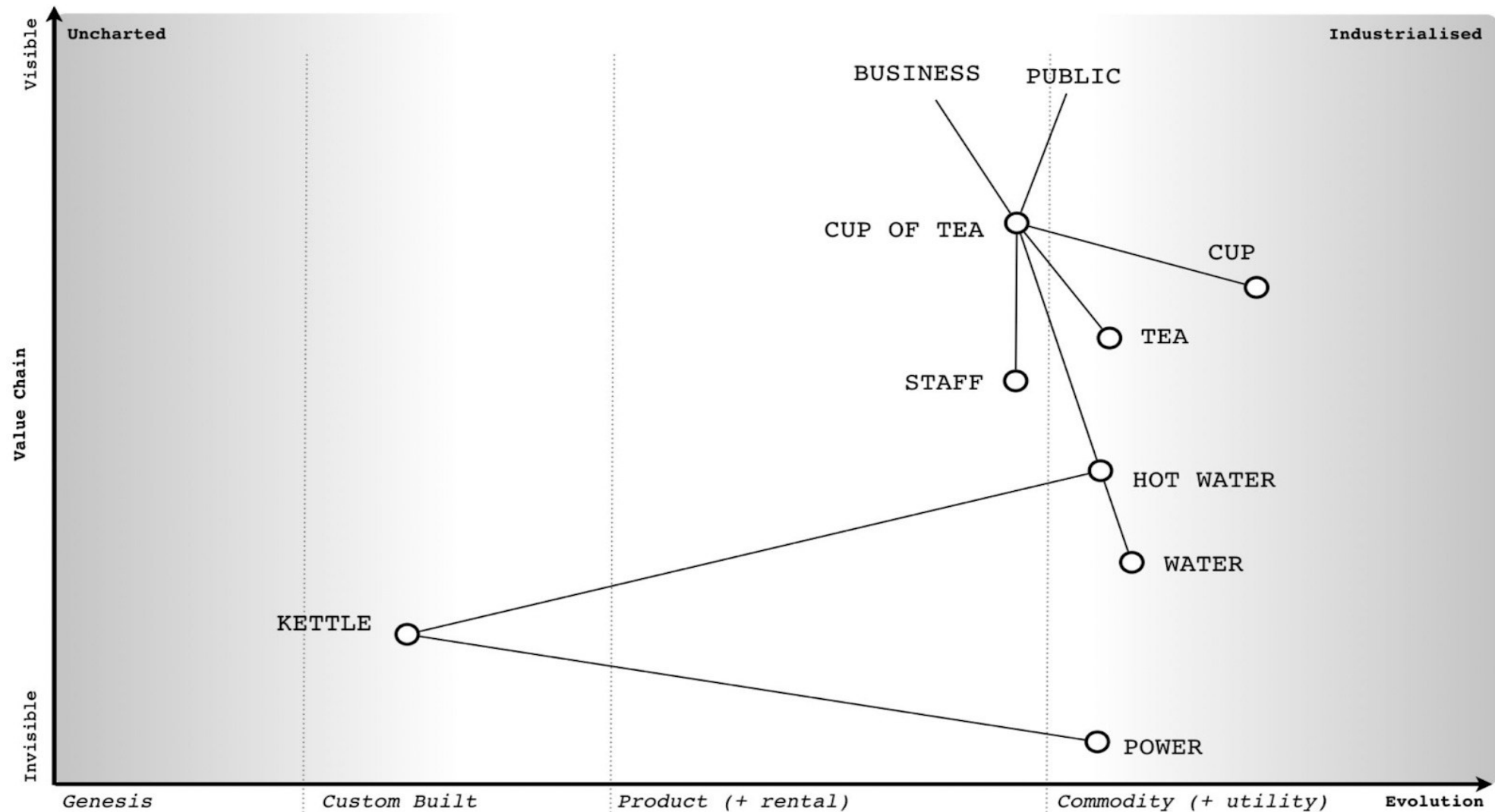
**THESE THREE
MAPS
ARE
DIFFERENT**

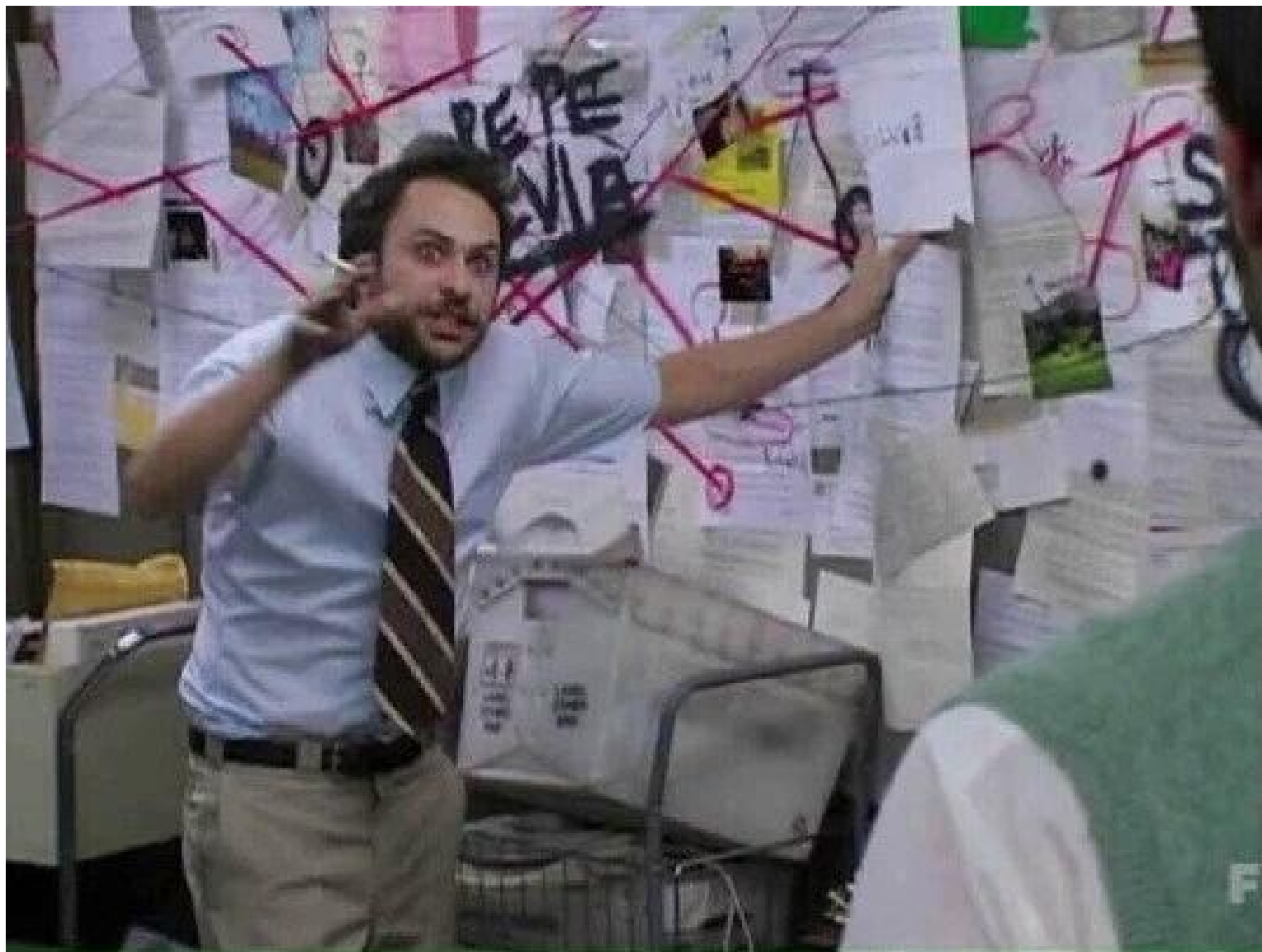


Characteristics of a “map”

- Anchor (*users and their needs*)
- Relative position (*value flow*)
- Movement over time (*evolution – x-axis*)
- Context (*value chains + evolution*)
- Components (*nodes*)
- Visibility & value (*y-axis*)

Wardley Map





Value Driven Roadmapping

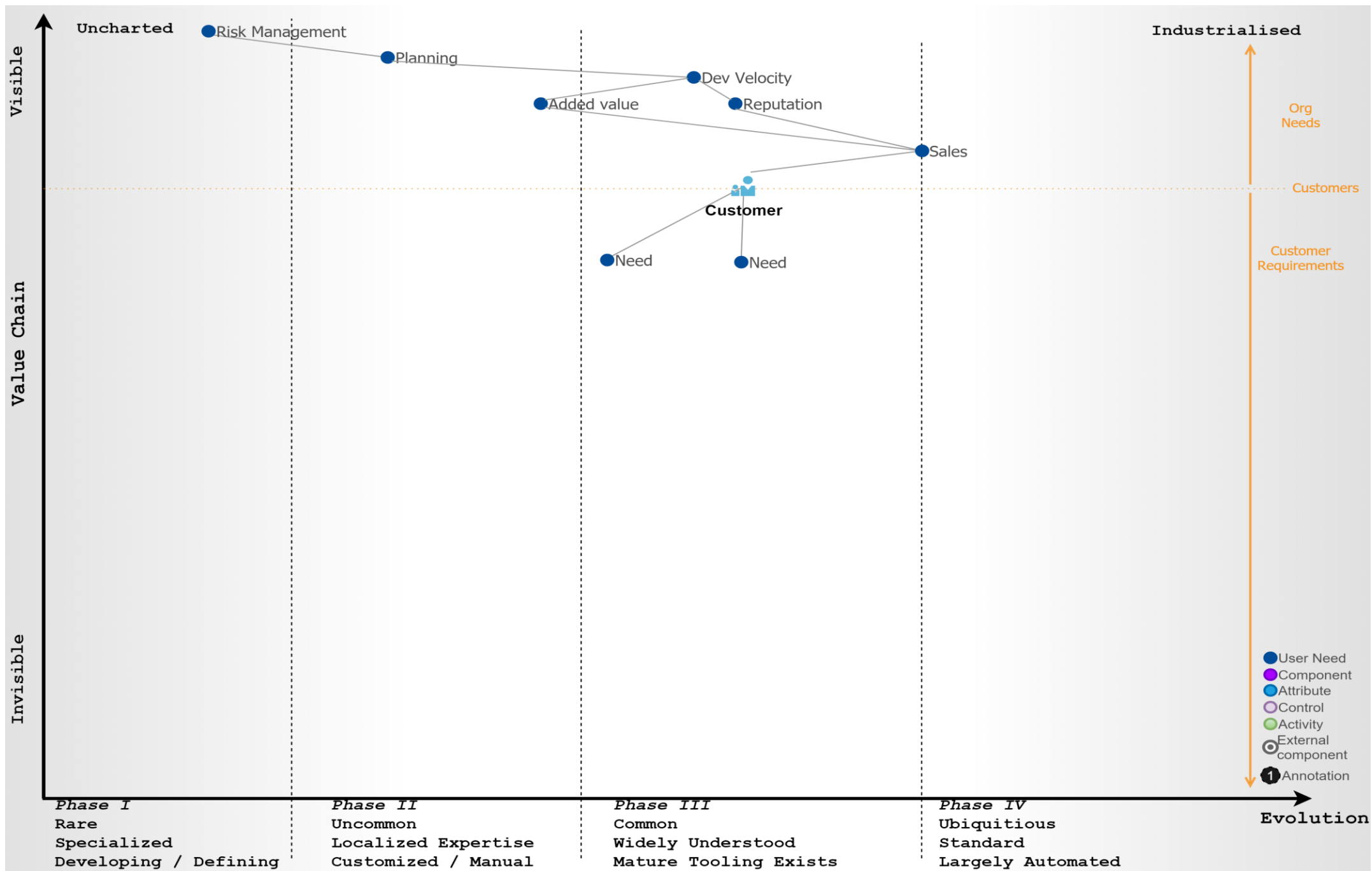
Mapping a security programme

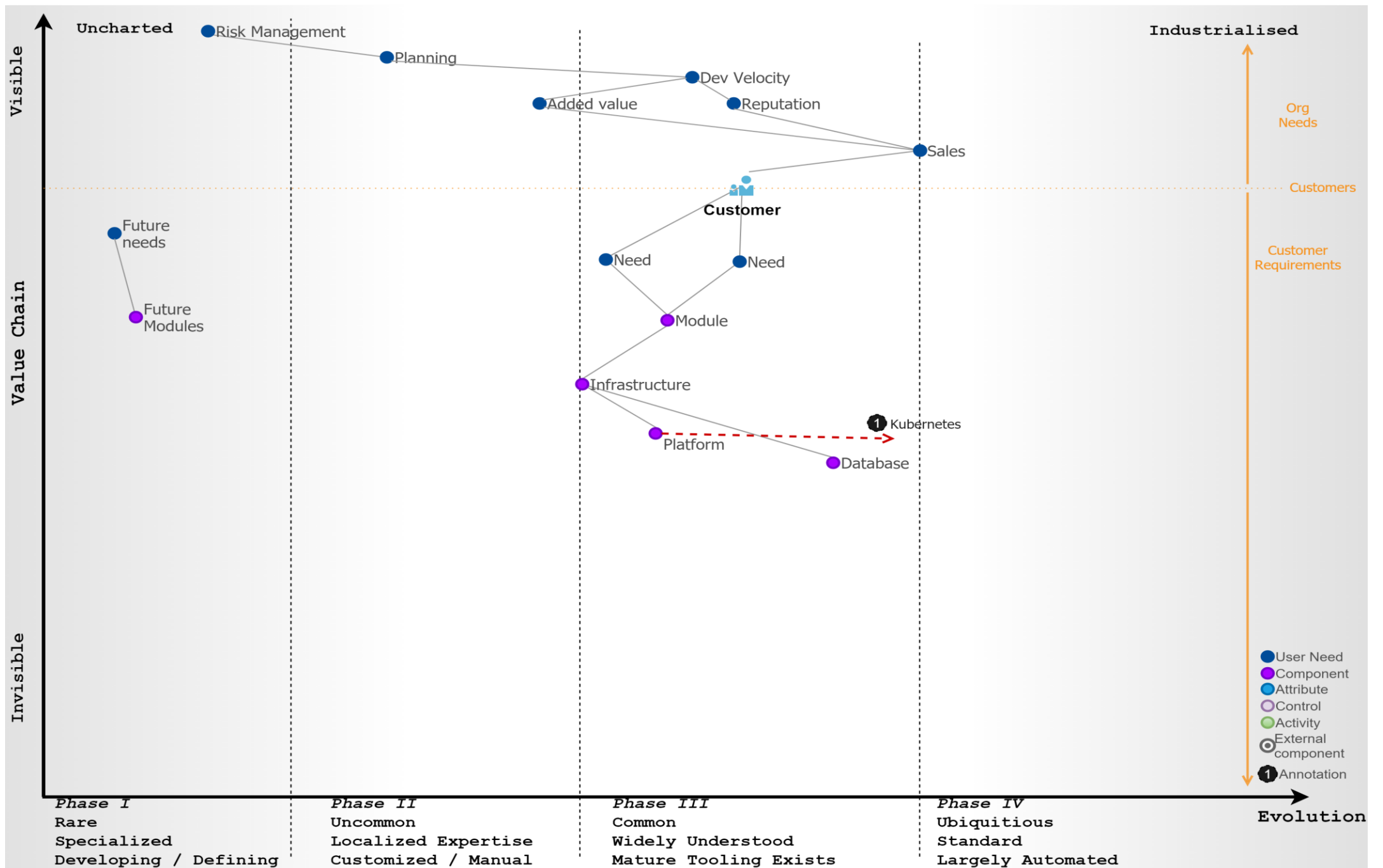
- Types of customers
- What are their primary needs? Secondary needs?
 - *Why do they come to you?*
- What do we need from them?
- System components to meet the needs
 - *Functionality + Infrastructure*
 - *Are there any other components?*

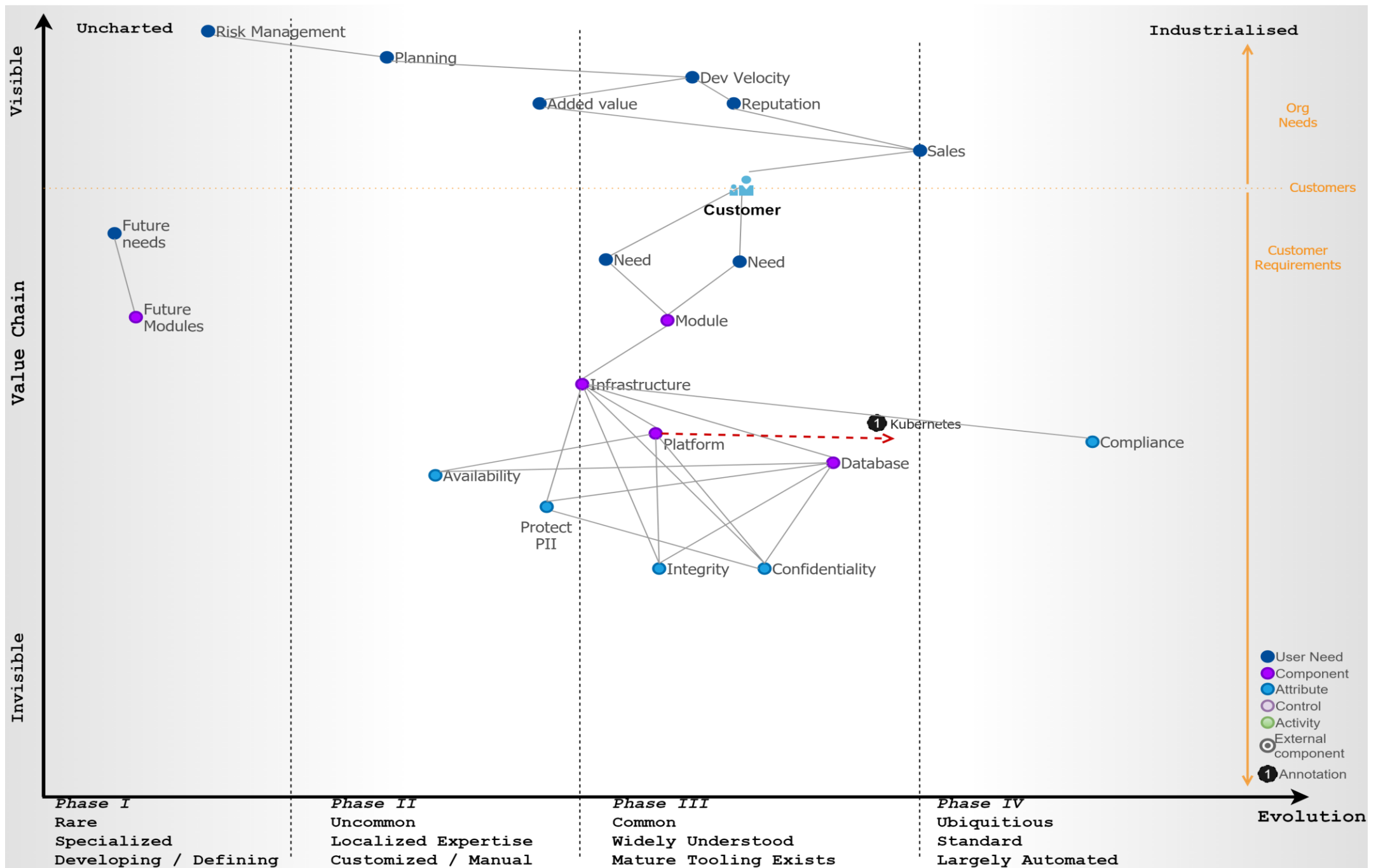
Mapping a security programme

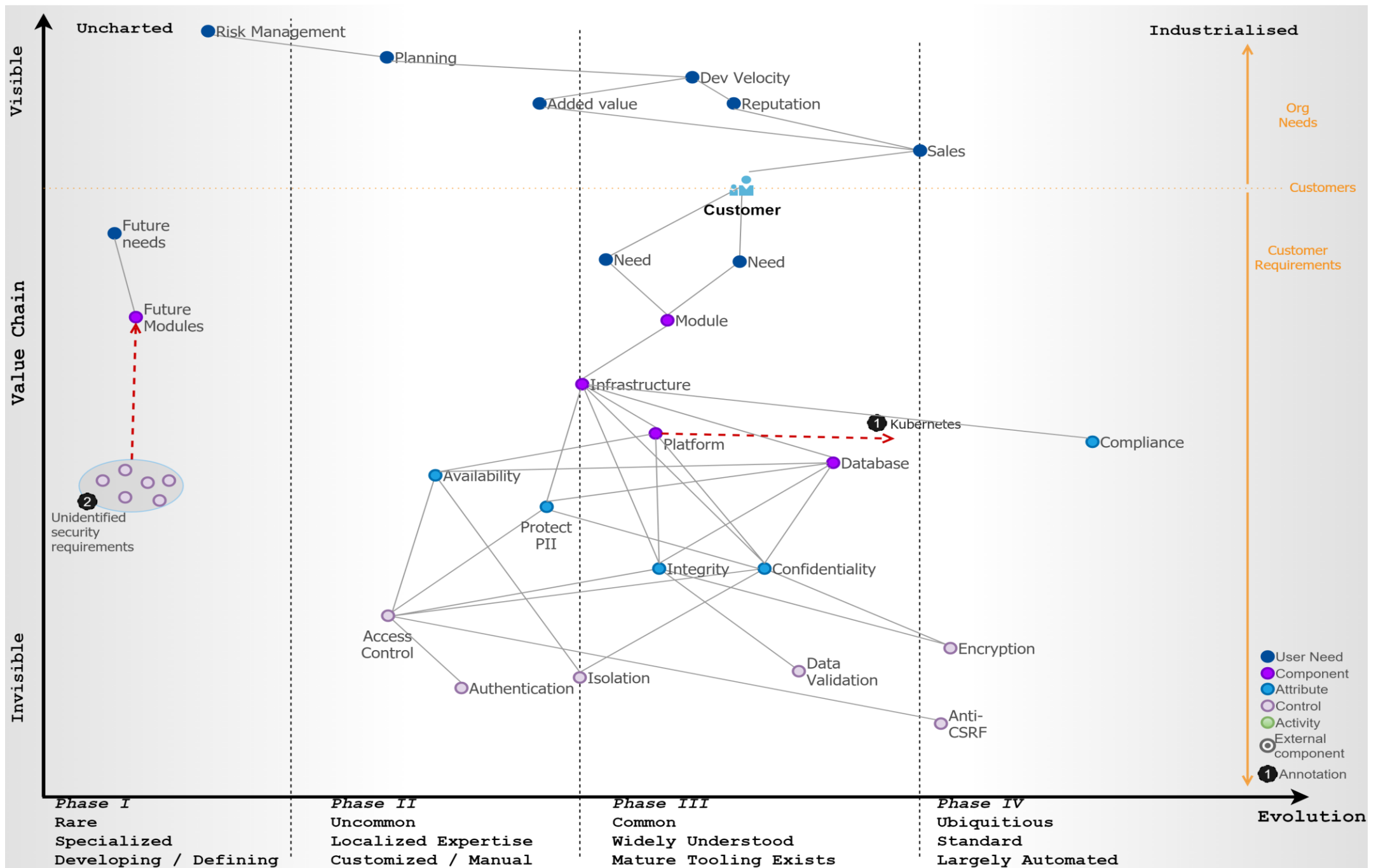
- Security attributes for each component
 - *E.g. CIA...*
- Security controls to provide those attributes
- What security-related activities are done currently?
 - *Which are not done at all, but would provide an unmet need?*
- What are the key focal points?

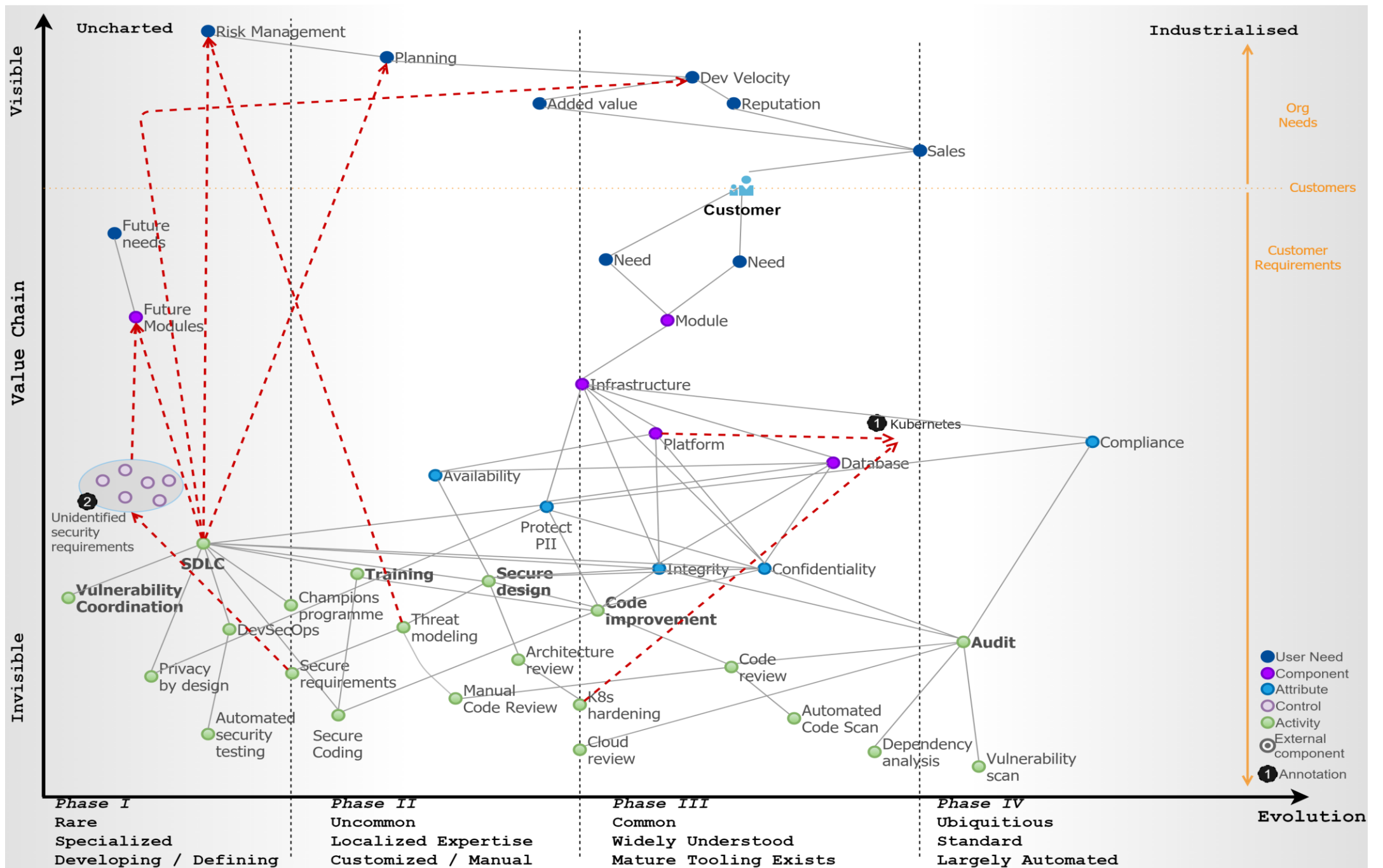












Maturity phases for security

■ Phase I

*Rare
Specialized
Developing / Defining*

■ Phase II

*Uncommon
Localized Expertise
Customized / Manual*

■ Phase III

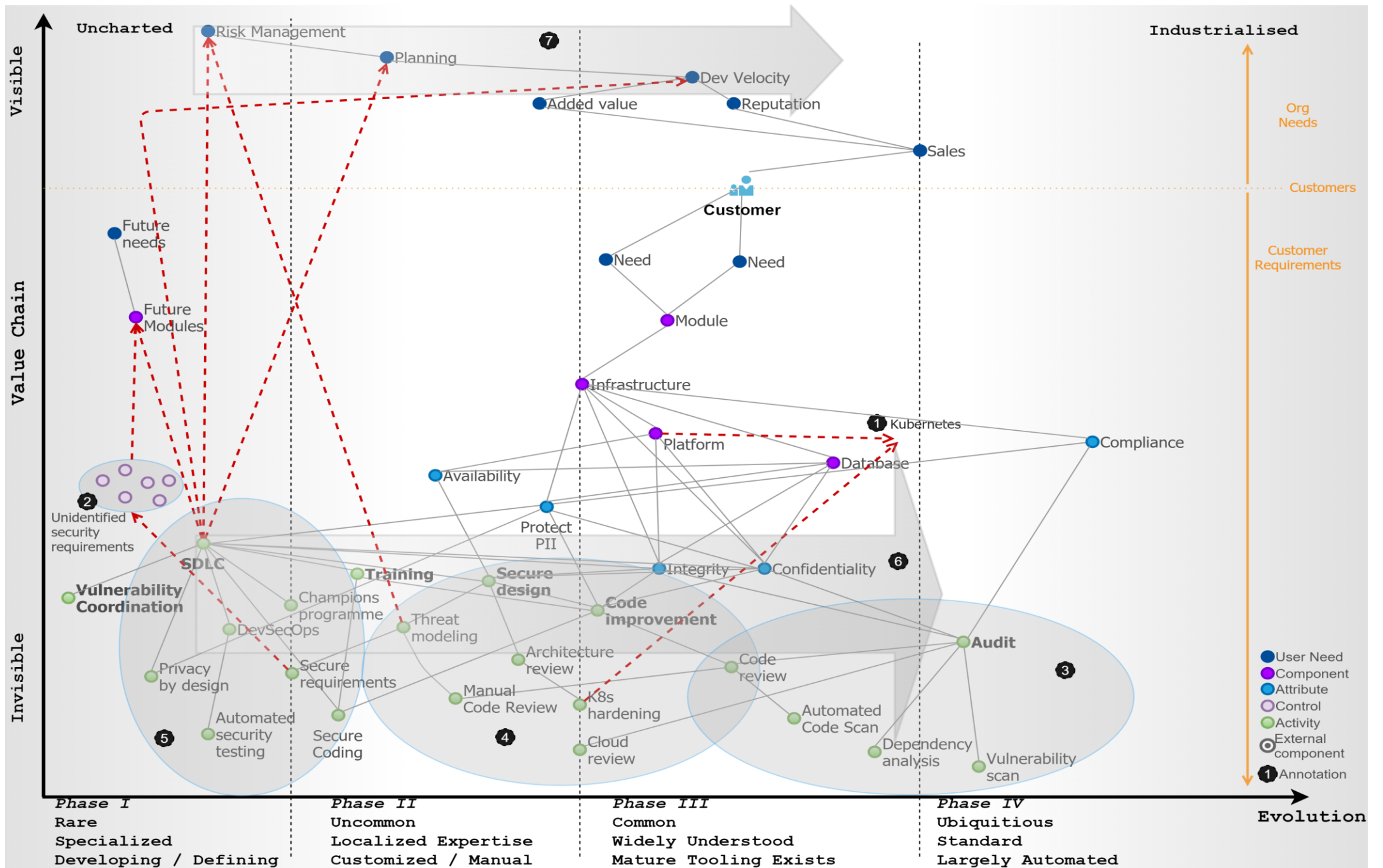
*Common
Widely Understood
Mature Tooling Exists*

■ Phase IV

*Ubiquitous
Standard
Largely Automated*

Planning improvements

- State of the Art vs State of Practice
- What should be done? What perhaps shouldn't be done, and what should be postponed? What could be done with a limited focus?
- Identify clumped regions



Takeaways

- Think about the value chain – focus on user needs
- Understand your landscape
- Work on movement (evolution) to create value
- Look for patterns and opportunities
- Create situational awareness
- Don't be generic, drive for specific business value

THANKS FOR LISTENING!



Avi Douglen
Bounce Security
 @sec_tigger