Jun 4, 2024

STPA for Data-Driven Safety: A Google Case Study

Ruben Barroso, *Site Reliability Engineering*

Google

Big Picture

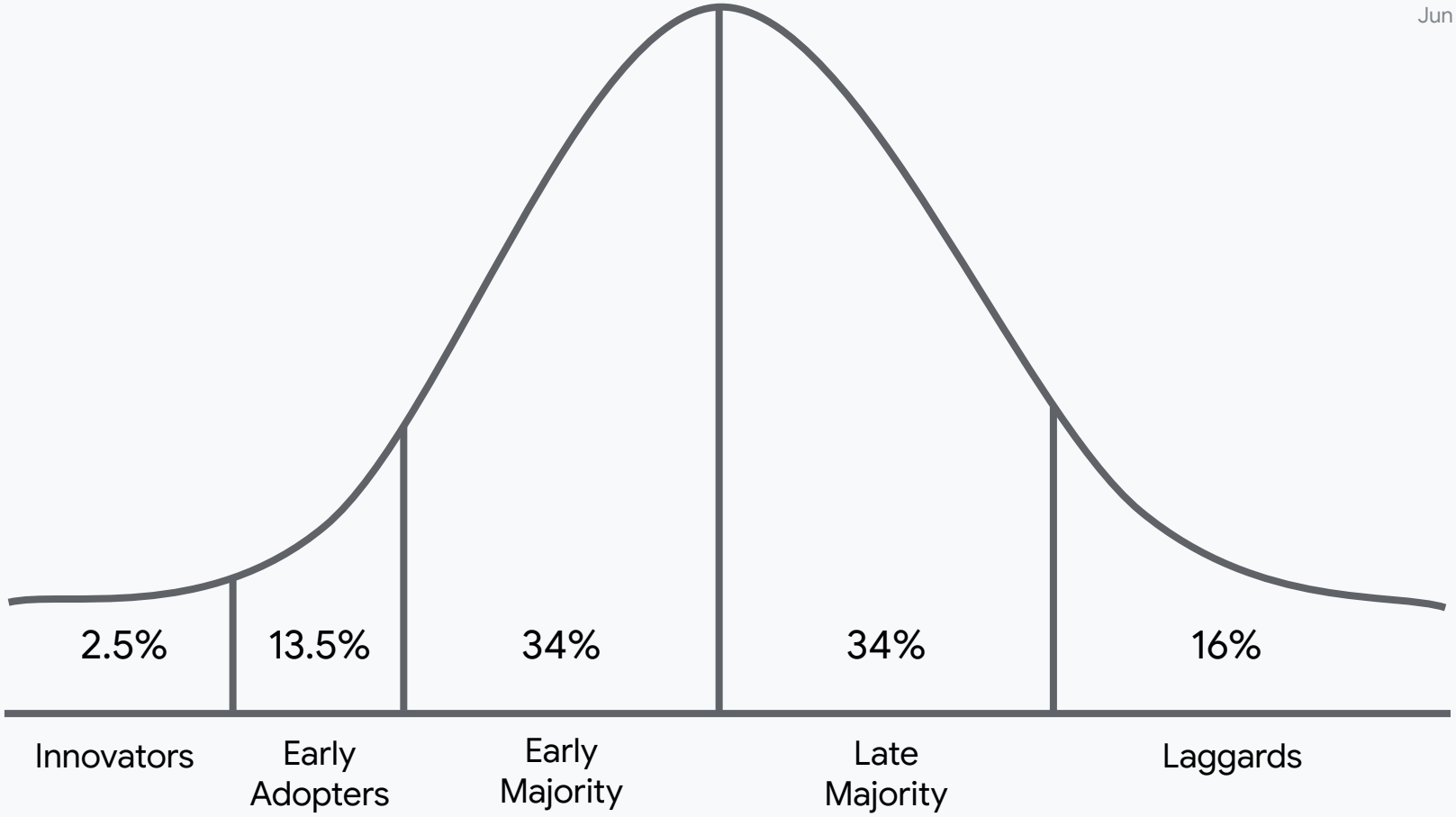
Three Challenges

Deep-Dive

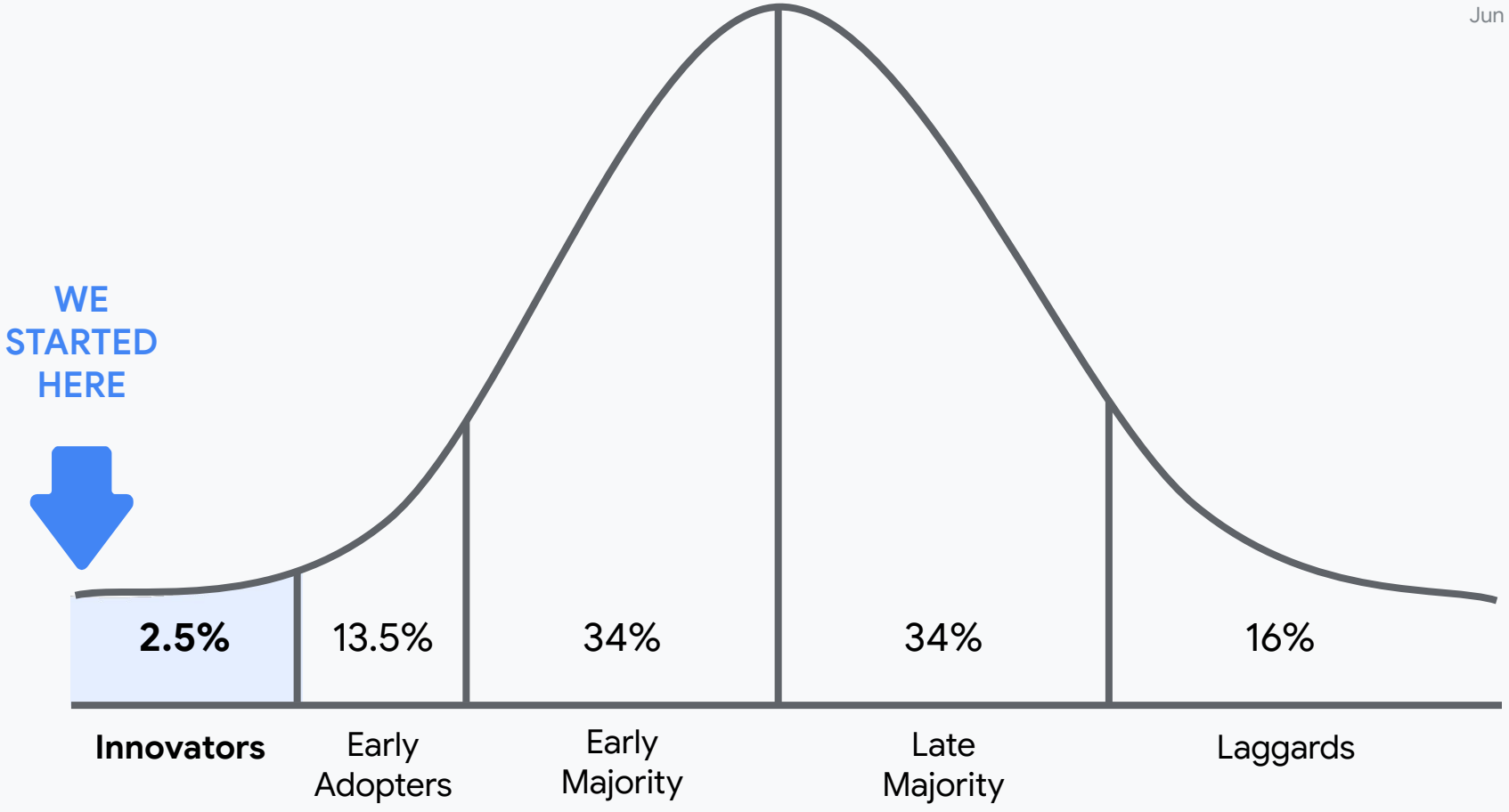


STPA ADOPTION

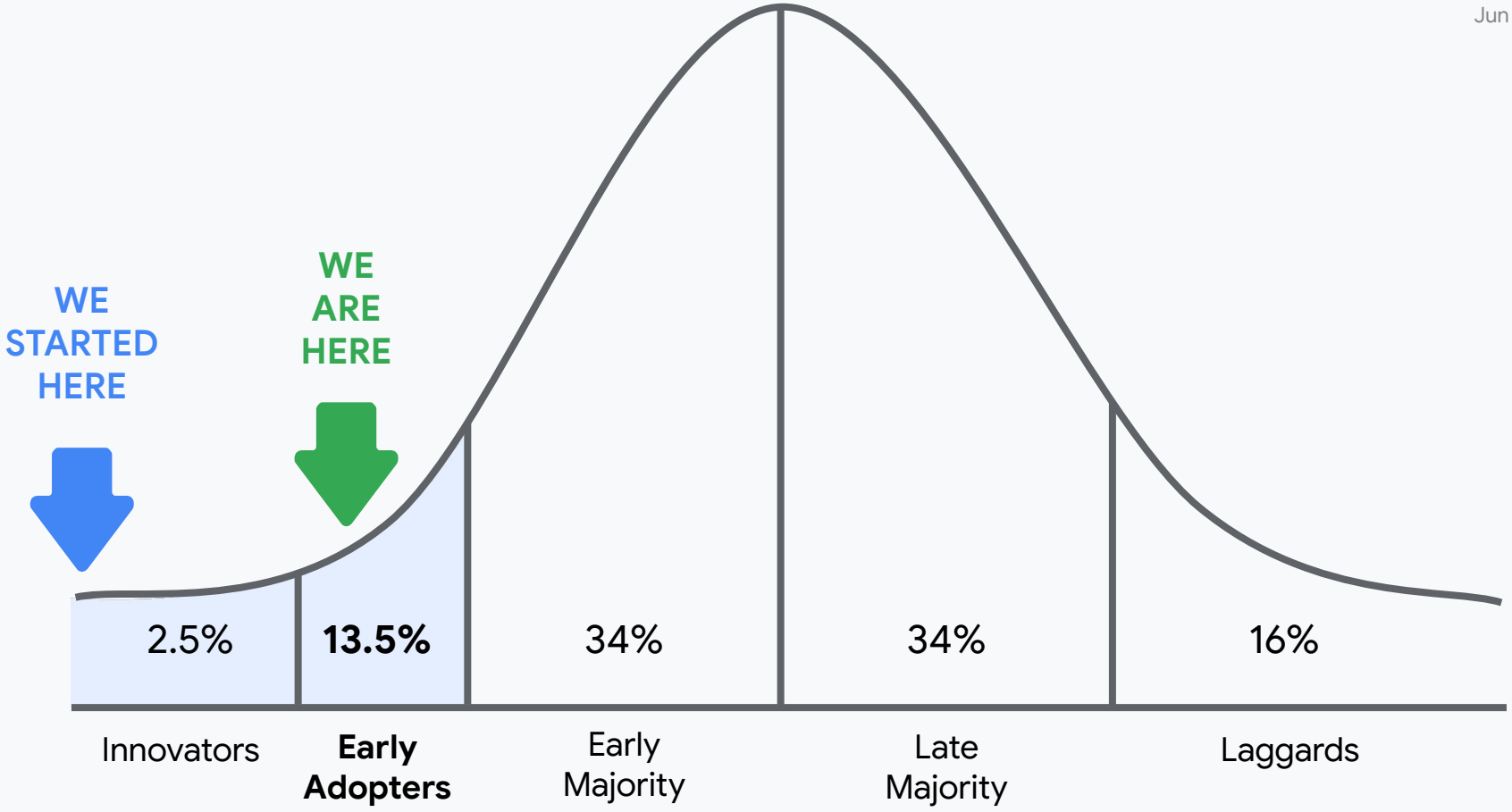
The Big Picture



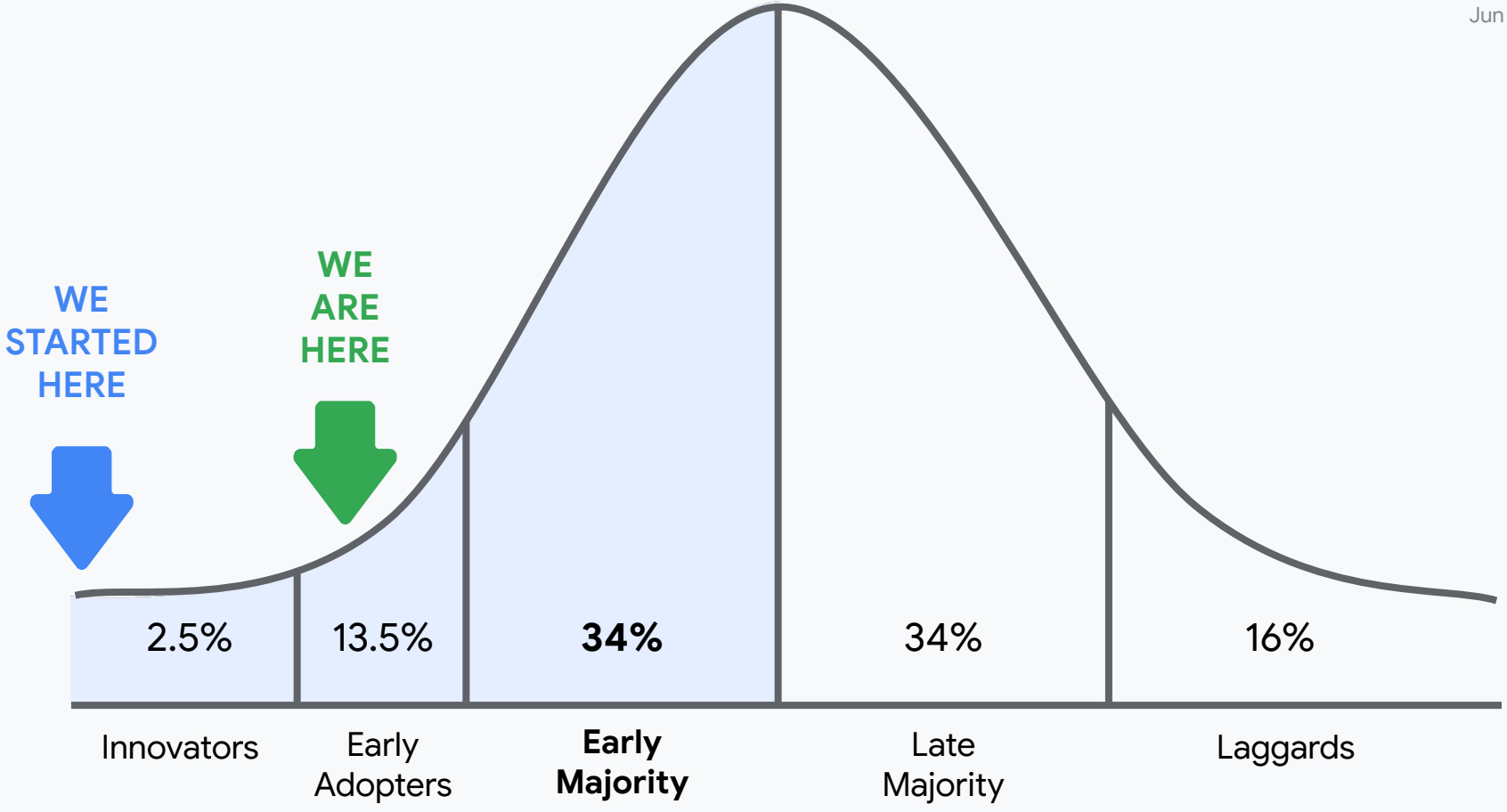
Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.



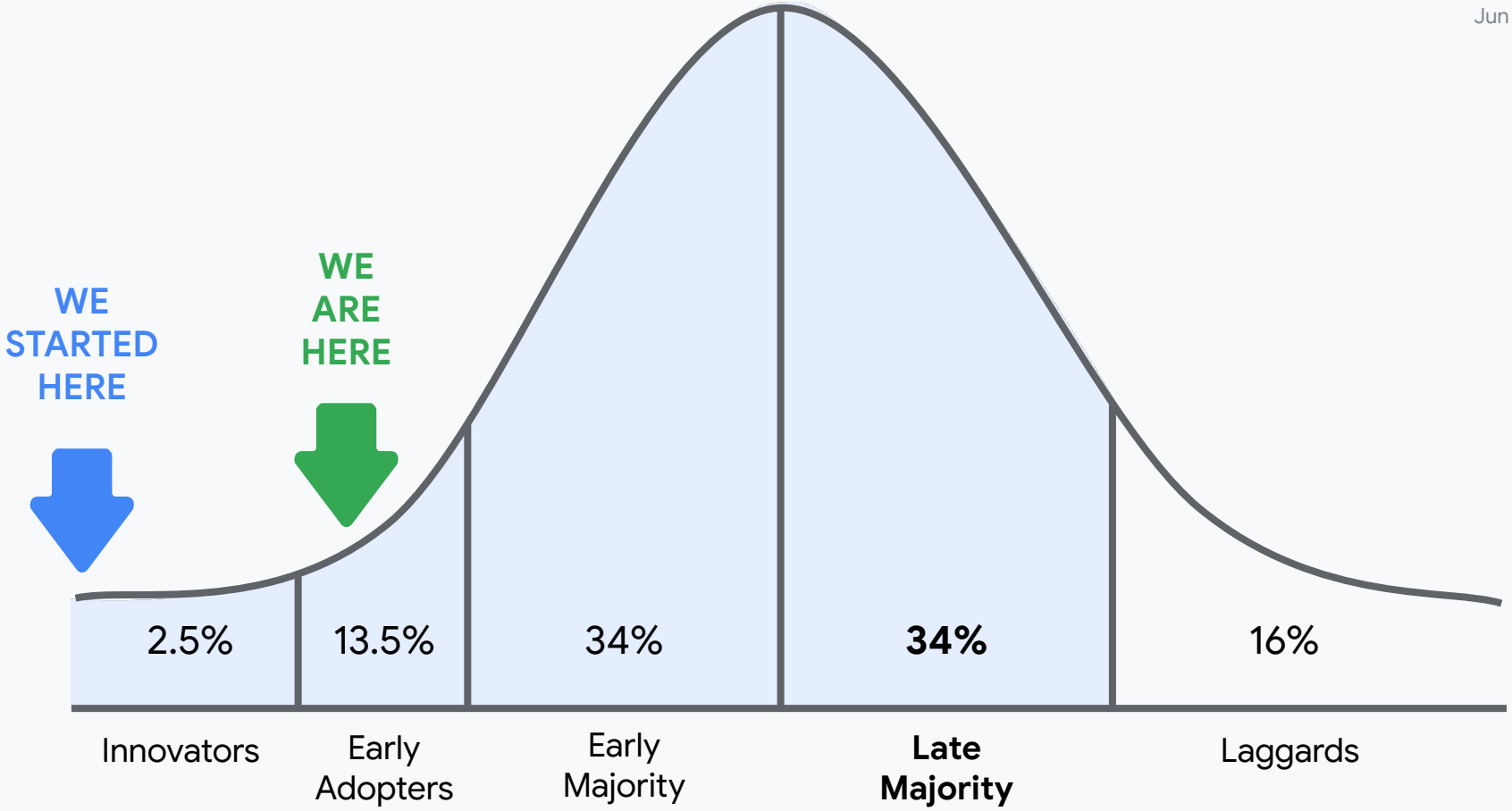
Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.



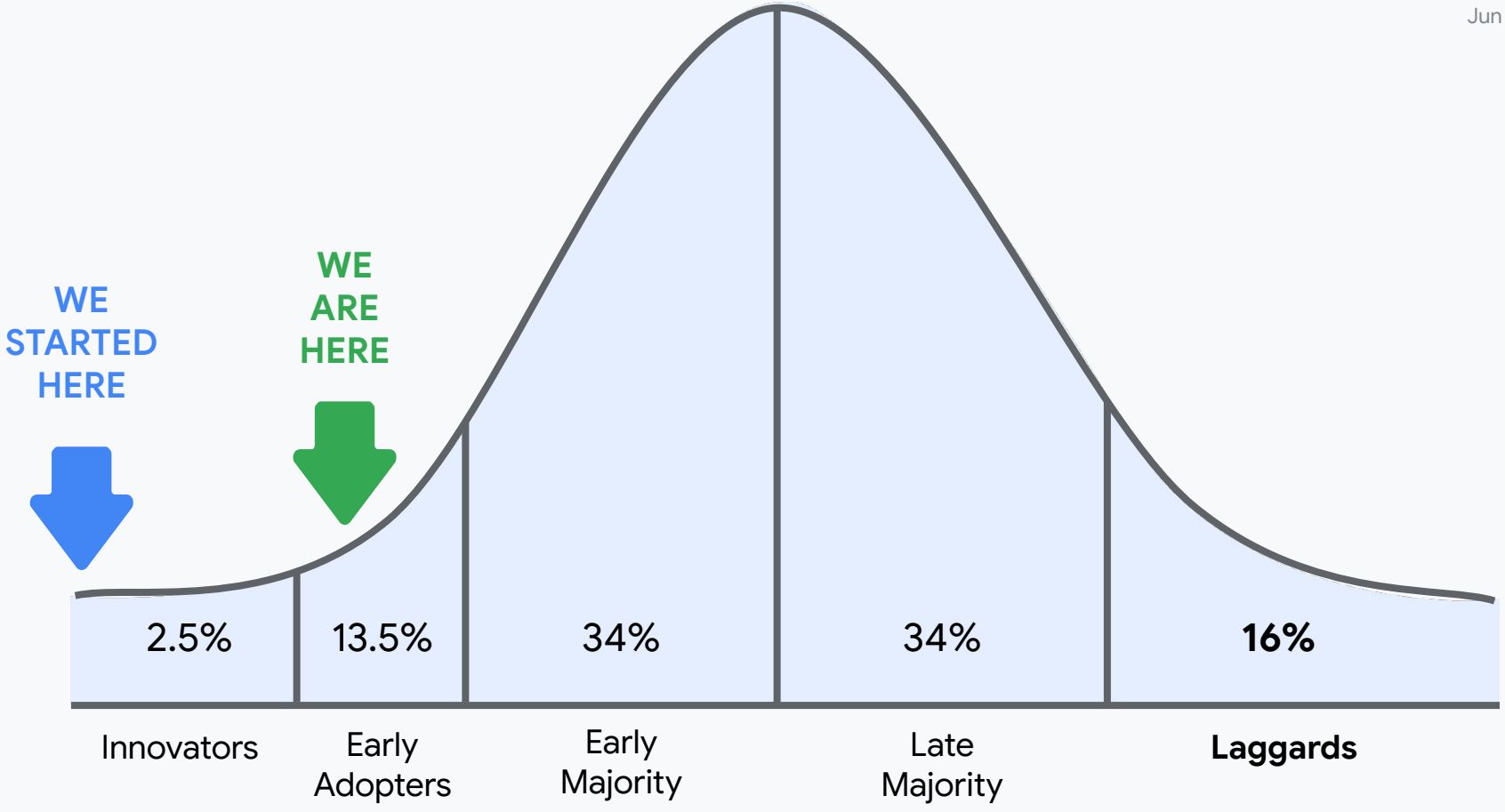
Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.



Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.



Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.



Rogers, E. M. & Shoemaker, F. F. (1971). Communication of Innovation. New York: The Free Press.

STPA ADOPTION

Three Challenges

Buy-in

*"Does STPA produce tangible **improvements** in our systems or processes?"*

Scalability

"Is STPA scalable to handle the complexity of our systems?"

Efficiency

*"Can STPA be **executed quickly** enough?"*

Jun 4, 2024

DEEP DIVE

Risk With Colored Pencils



Data Products



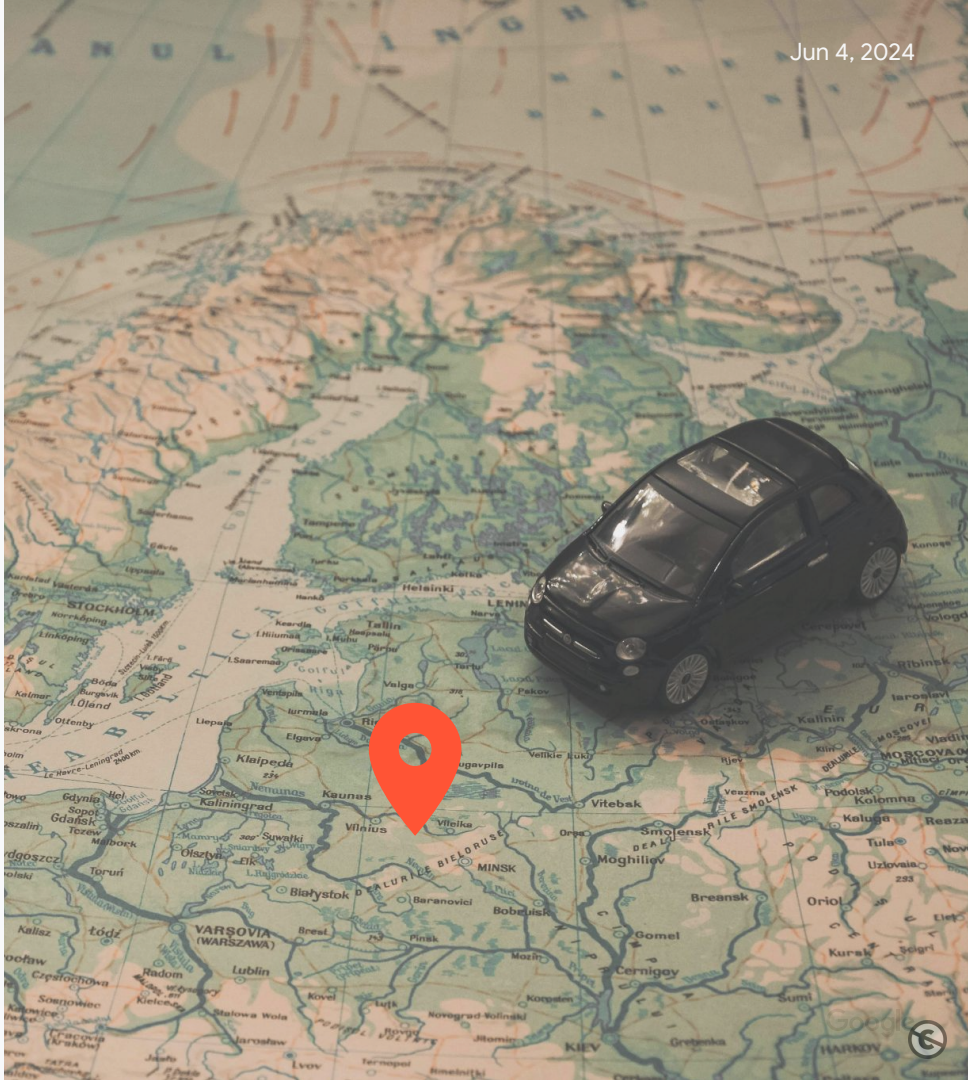






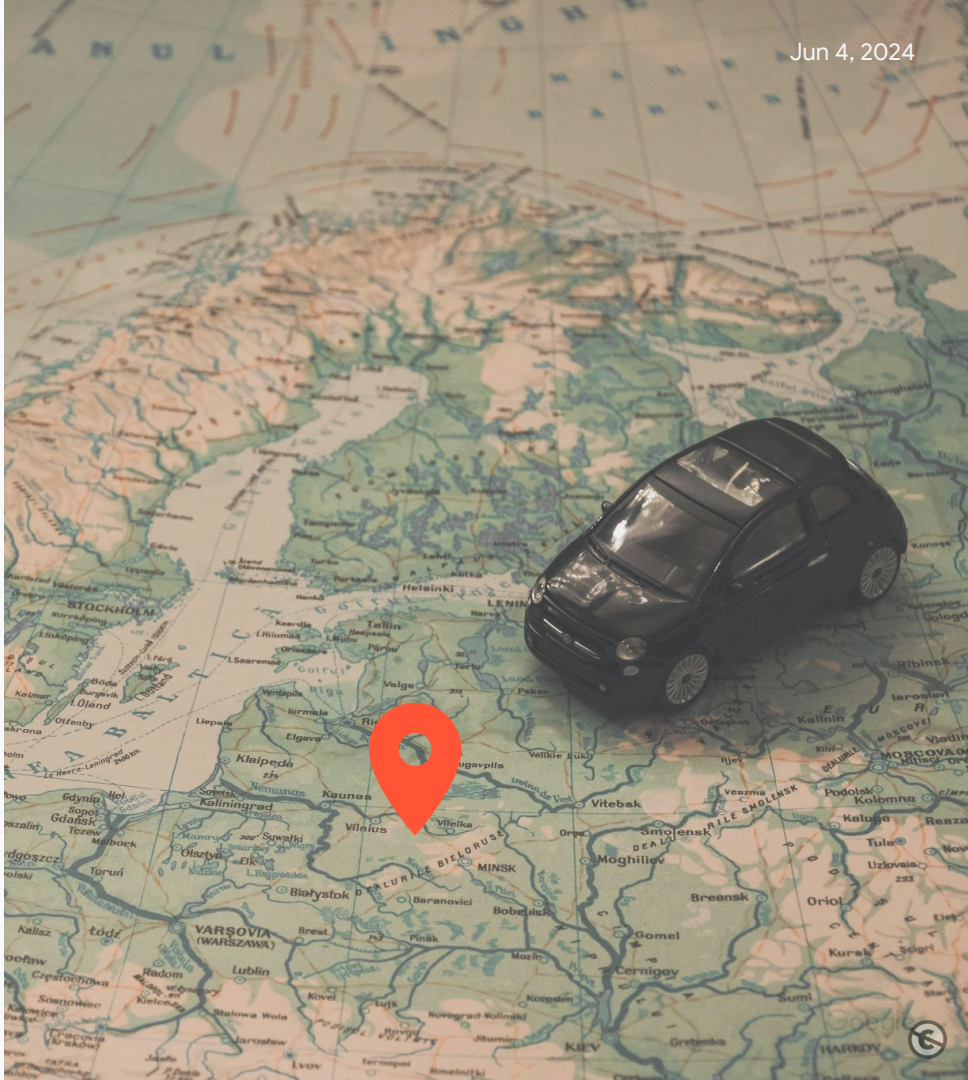




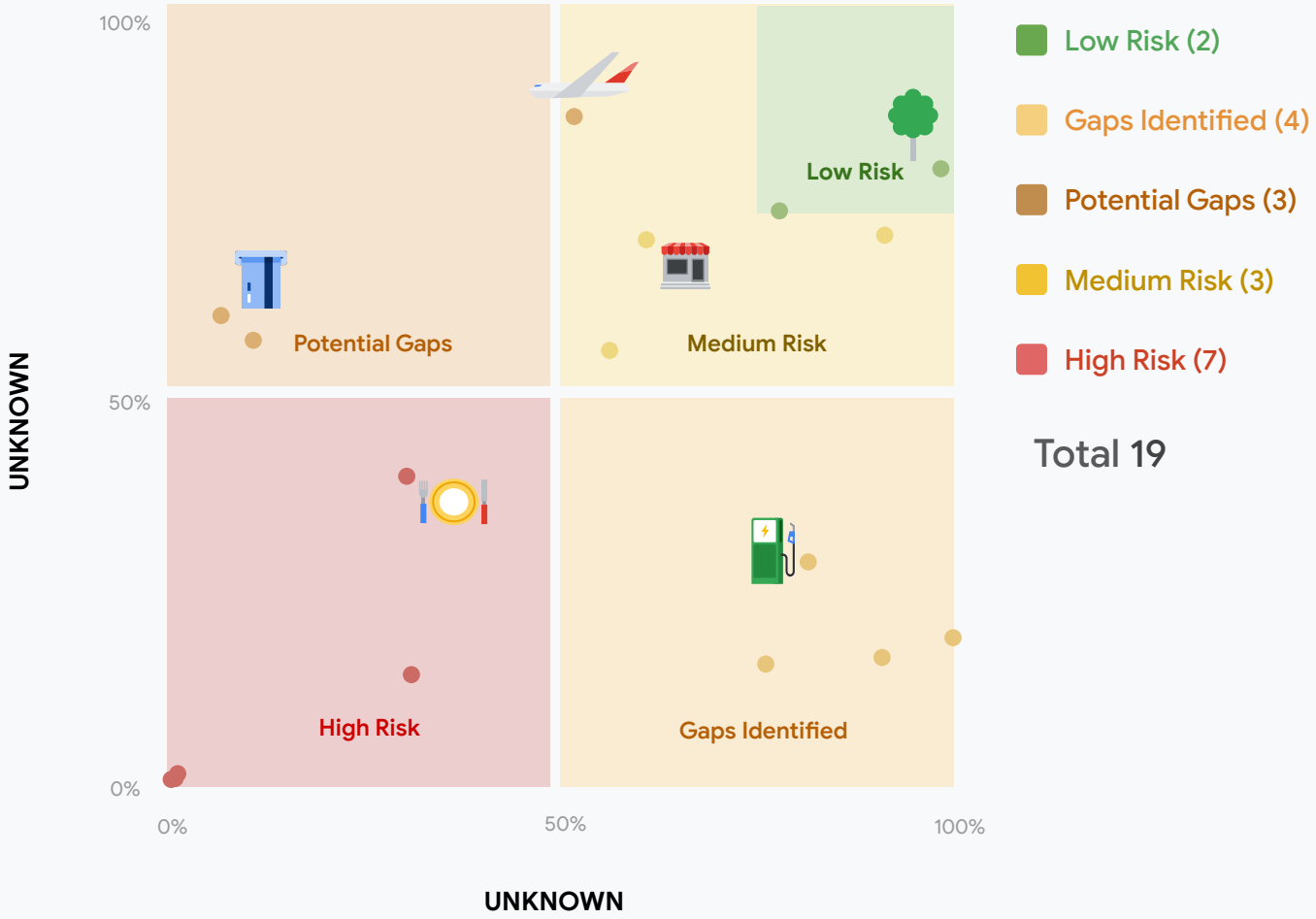


Data Products

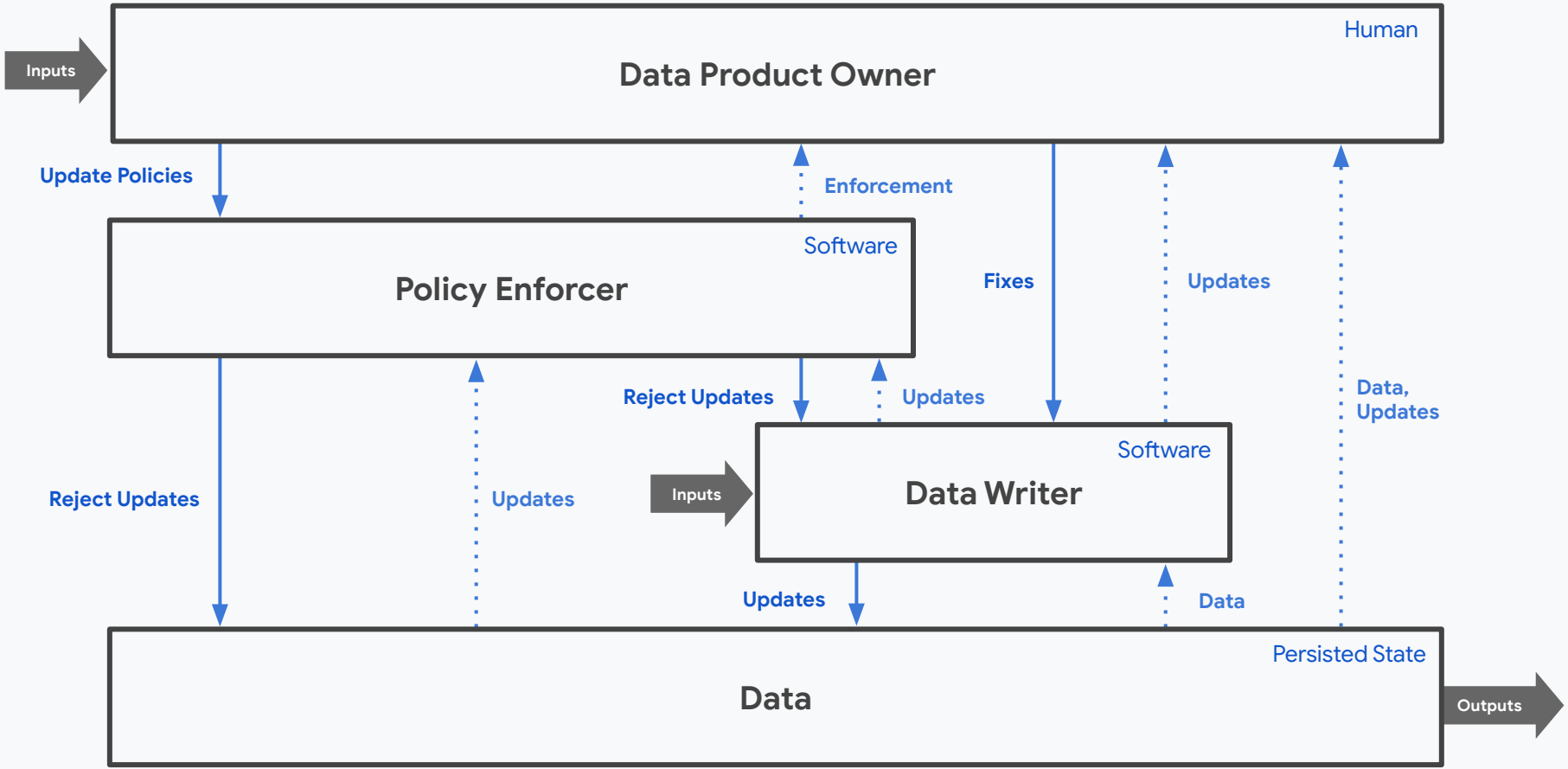
*"What is the **risk** associated to each one of those **data products**?"*

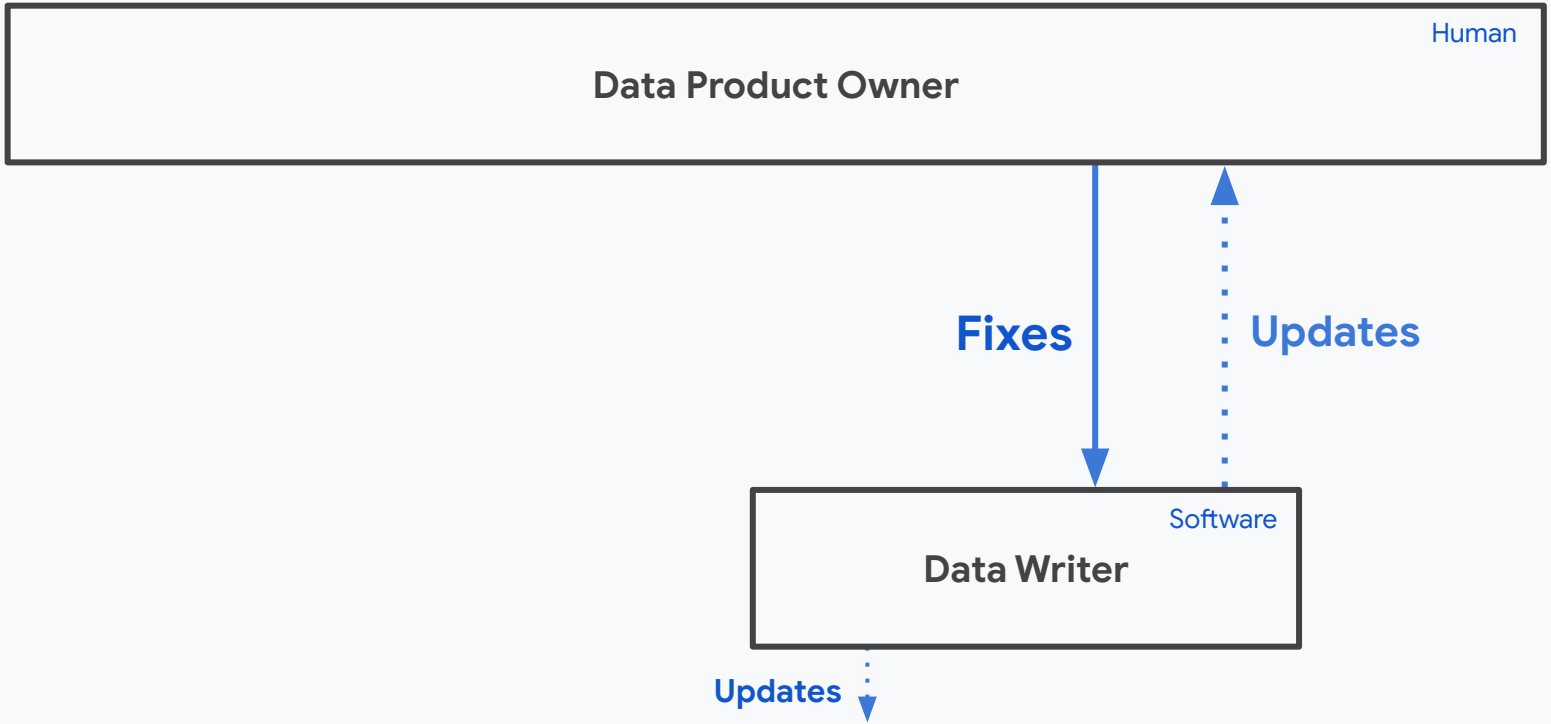


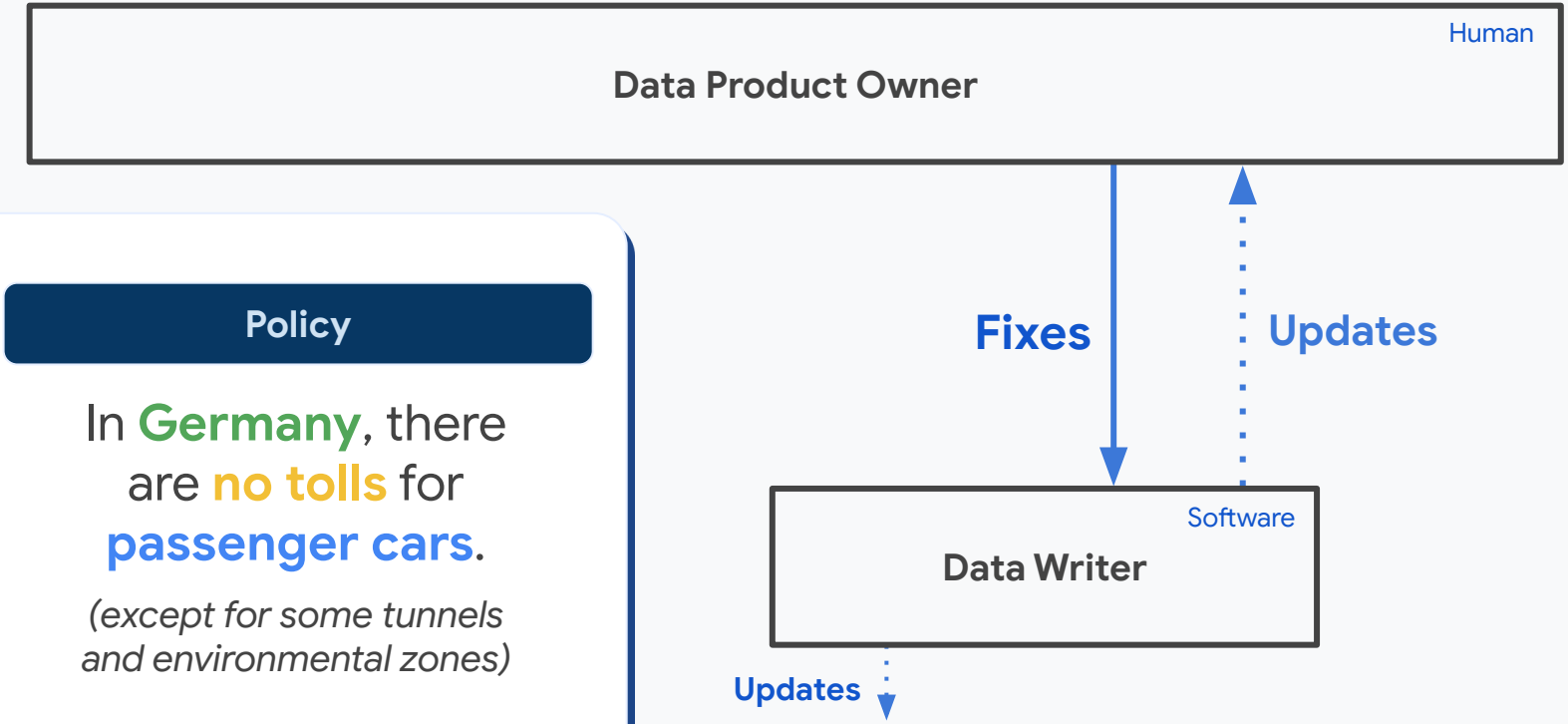
Jun 4, 2024



Google


Inputs
Human
Data Product Owner
Update Policies
Enforcement
Software
Policy Enforcer
Fixes
Updates
Data,
Updates
Reject Updates
Updates
Reject Updates
Updates
Inputs
Software
Data Writer
Updates
Data
Persisted State
Data
Outputs

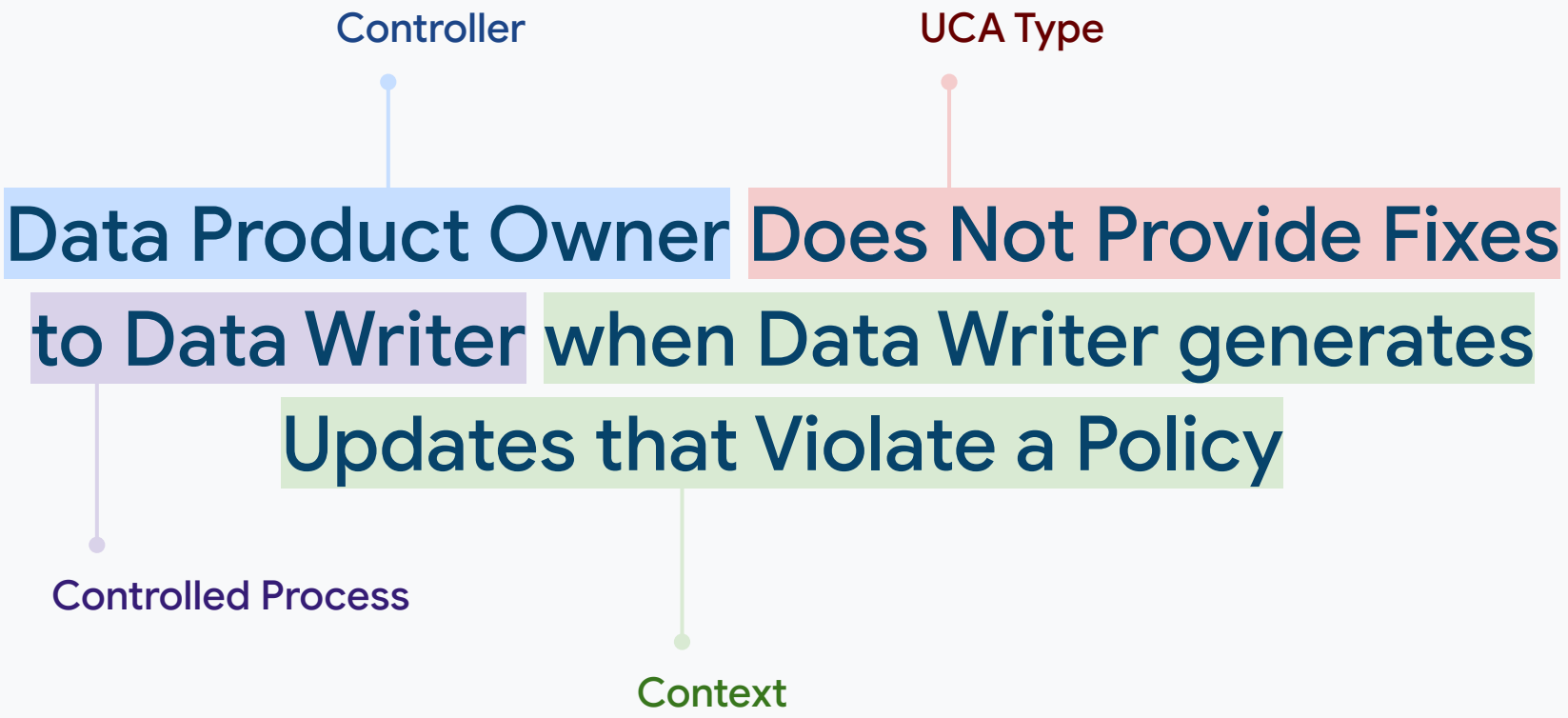

Human
Data Product Owner
Fixes
Updates
Software
Data Writer
Updates



Policy

In Germany, there are no tolls for passenger cars.

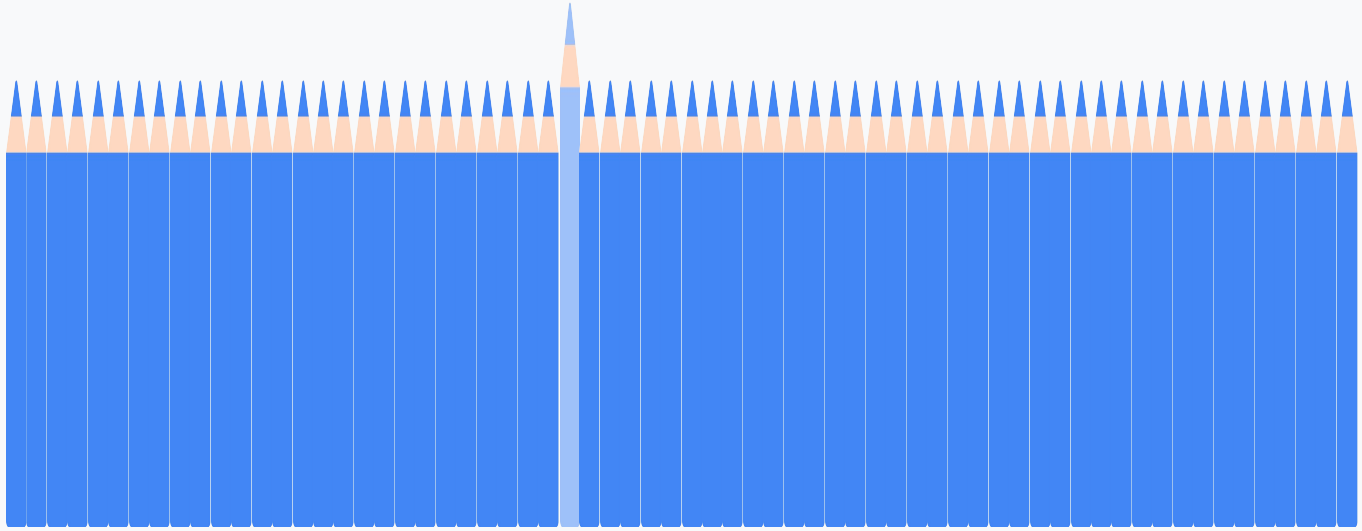
(except for some tunnels and environmental zones)


Controller
UCA Type
Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy
Controlled Process
Context

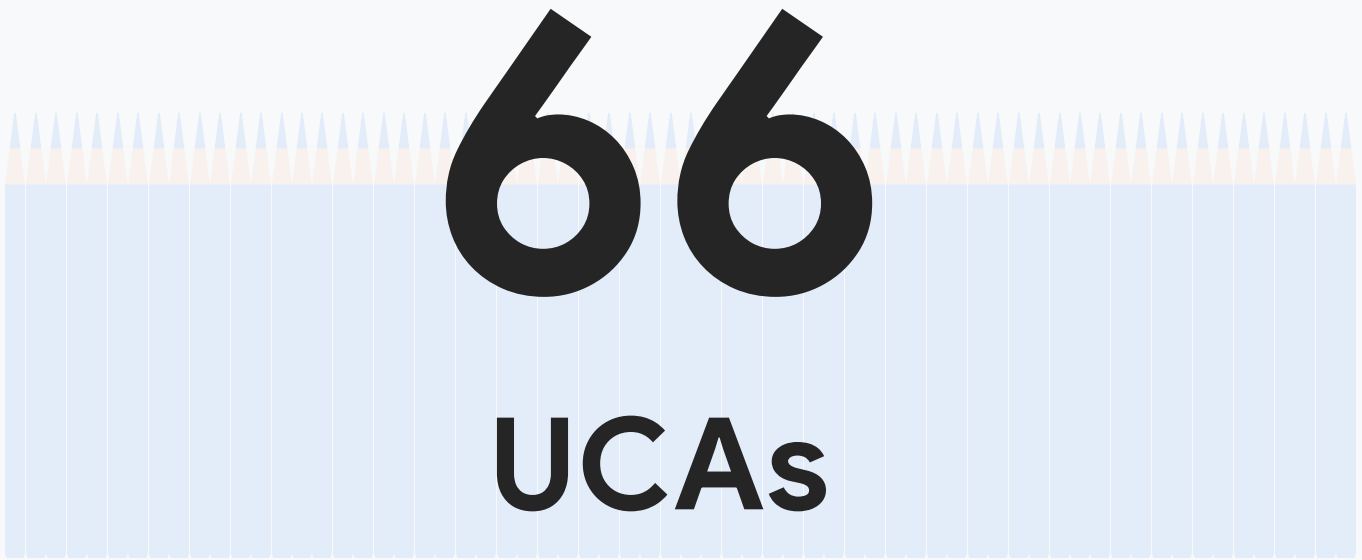
Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy



Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy



Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy



Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy

4 Questions

Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy

Are there ever situations where ...

Unsafe Controller Behavior

... **YOU KNOW** Data Writer generates invalid data, but **YOU DON'T FIX** Data Writer?

Cabosky, R. (2020). Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation. MIT.

Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Cabosky, R. (2020). Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation. MIT.

Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Cabosky, R. (2020). Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation. MIT.

Data Product Owner Does Not Provide Fixes to Data Writer when Data Writer generates Updates that Violate a Policy

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?

Cabosky, R. (2020). Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation. MIT.

QUESTIONS

STRENGTH OF CONTROLS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?

QUESTIONS

STRENGTH OF CONTROLS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?



UNKNOWN
UNKNOWN

QUESTIONS

STRENGTH OF CONTROLS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

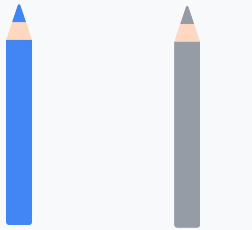
... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?



UNKNOWN UNKNOWN

KNOWN UNKNOWN

QUESTIONS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

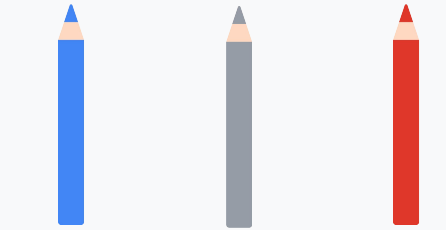
Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?

STRENGTH OF CONTROLS



QUESTIONS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

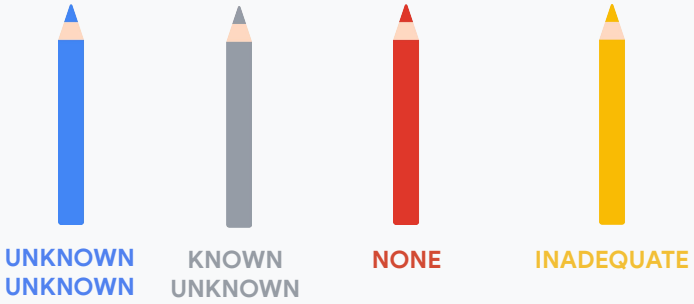
Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

Unsafe Controlled Process Behavior

... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?

STRENGTH OF CONTROLS



QUESTIONS

Are there ever situations where ...

Unsafe Controller Behavior

... YOU KNOW Data Writer generates invalid data, but YOU DON'T FIX Data Writer?

Unsafe Feedback Path

... you MIGHT NOT KNOW when Data Writer generates invalid data, thus YOU DON'T FIX Data Writer?

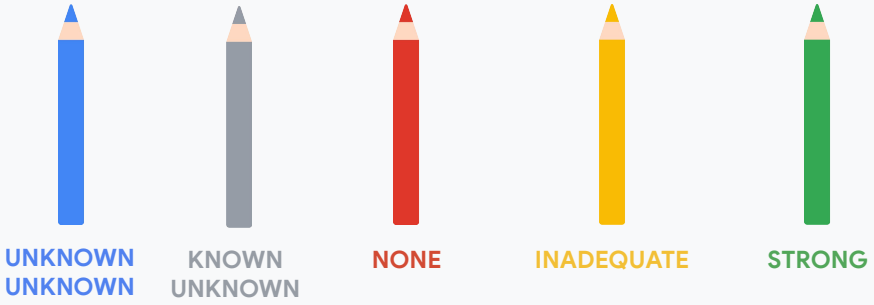
Unsafe Control Path

... YOU FIX Data Writer, but the FIX MIGHT NOT BE APPLIED?

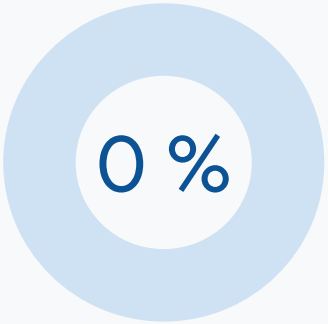
Unsafe Controlled Process Behavior

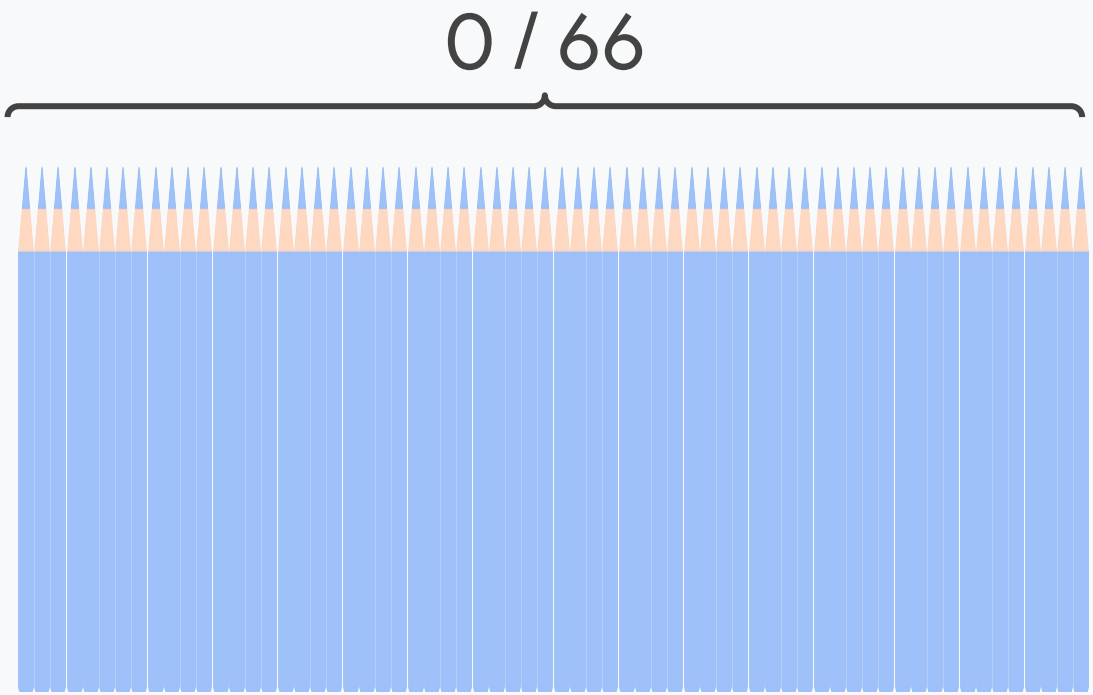
... you fix Data Writer, the FIX IS APPLIED, but FIX DOESN'T WORK as intended?

STRENGTH OF CONTROLS



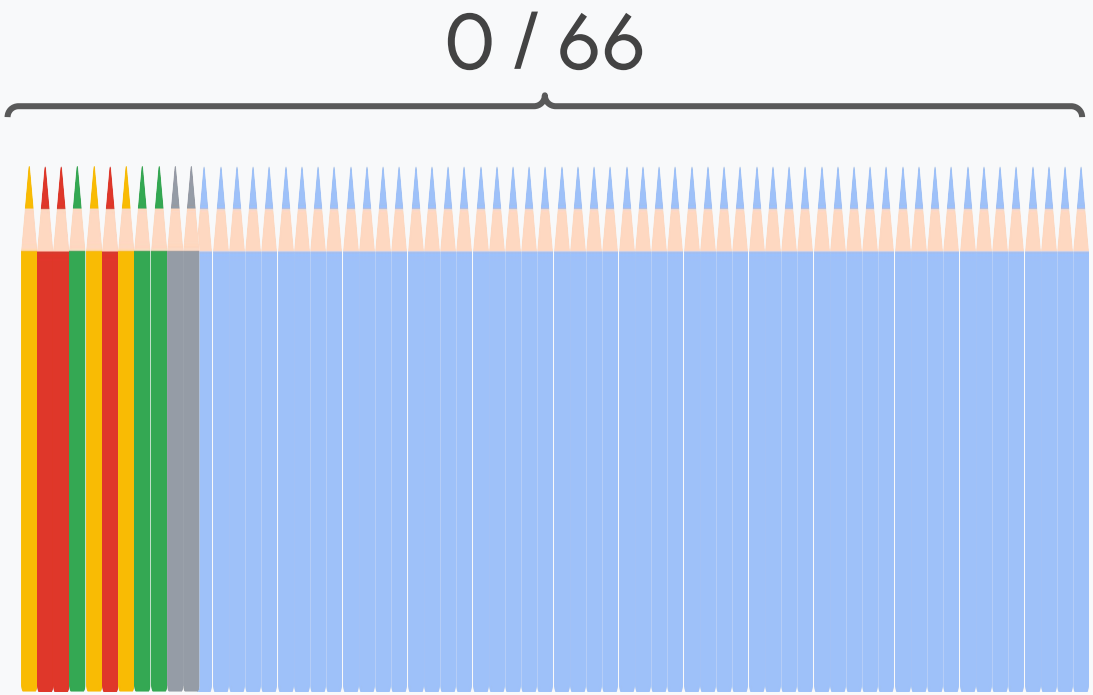
How Much Do We **Know**?



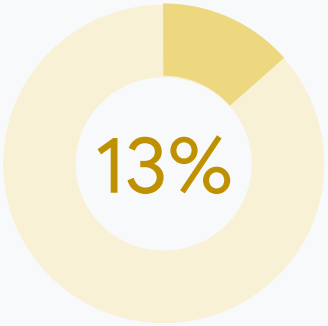


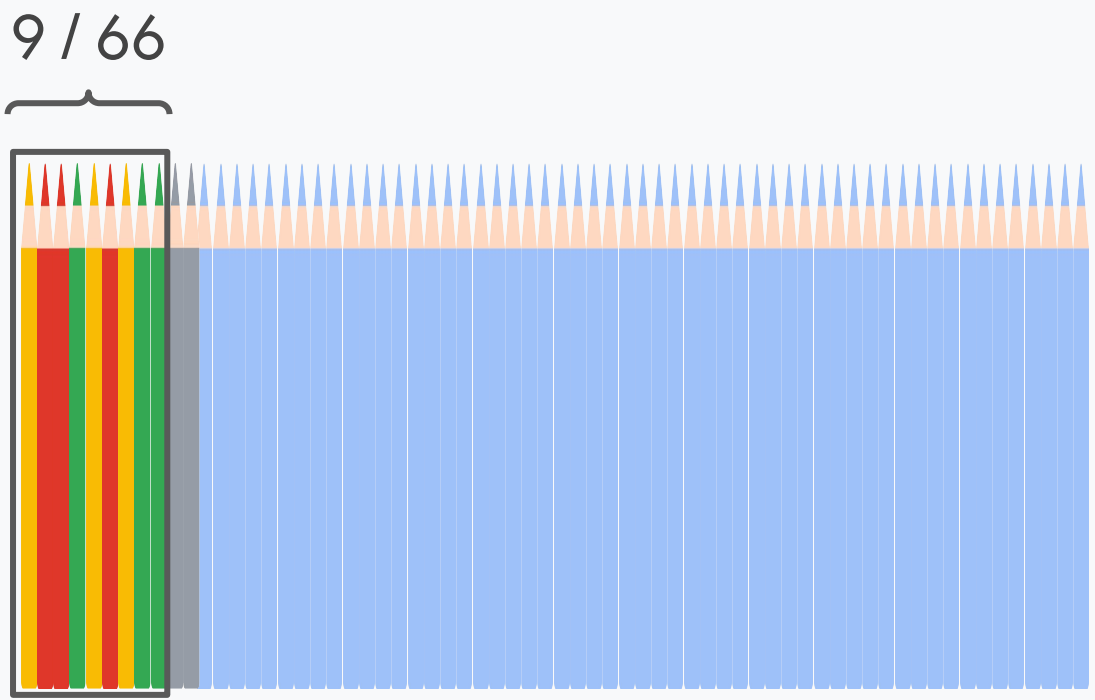
How Much Do We Know?



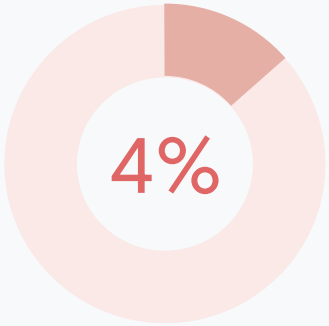


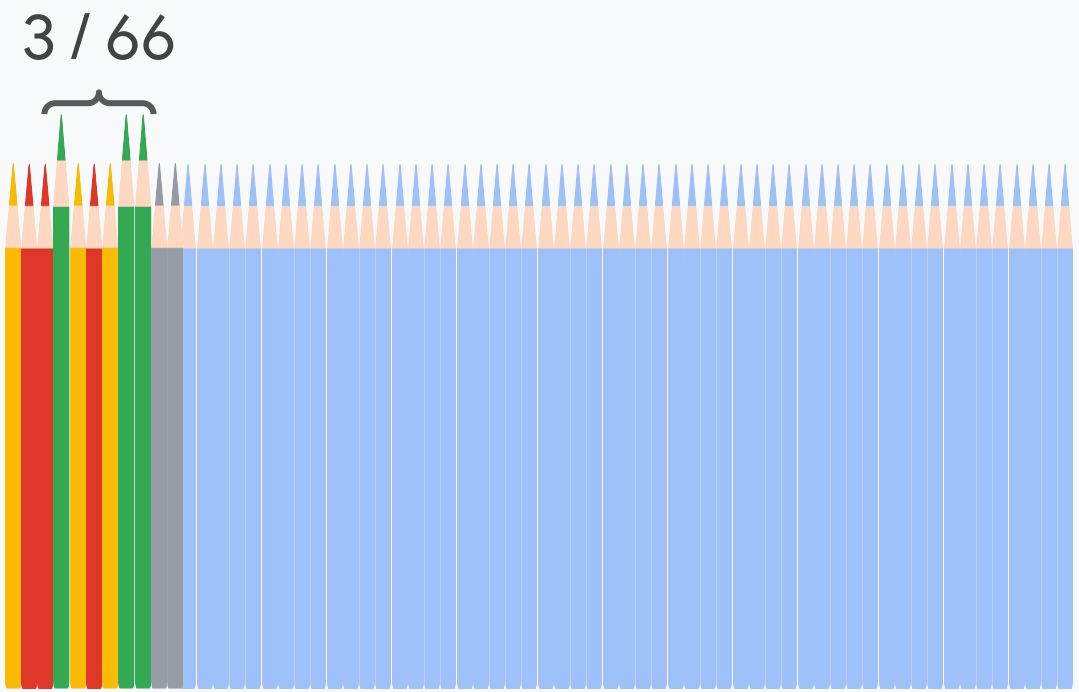
How Much Do We Know?



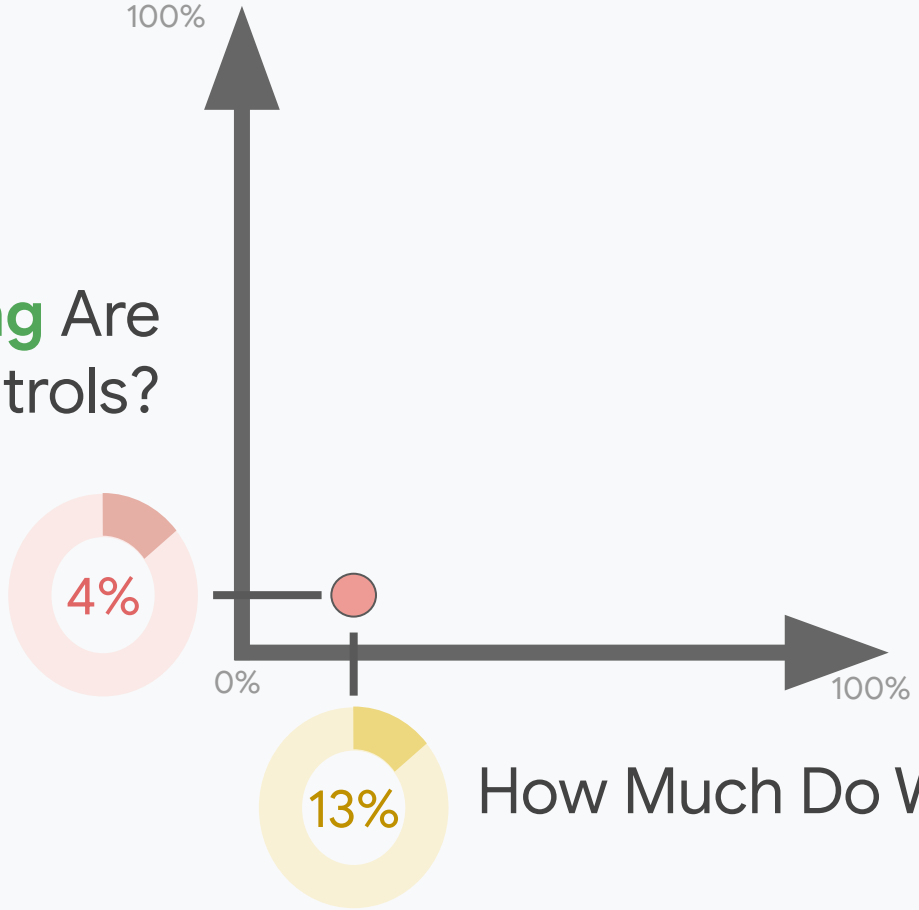


How **Strong** Are The Controls?



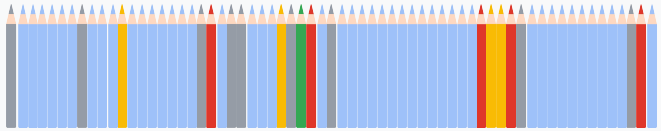
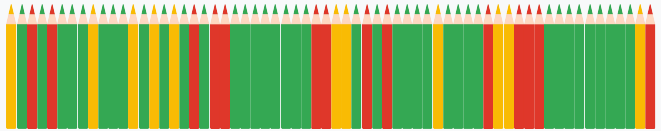


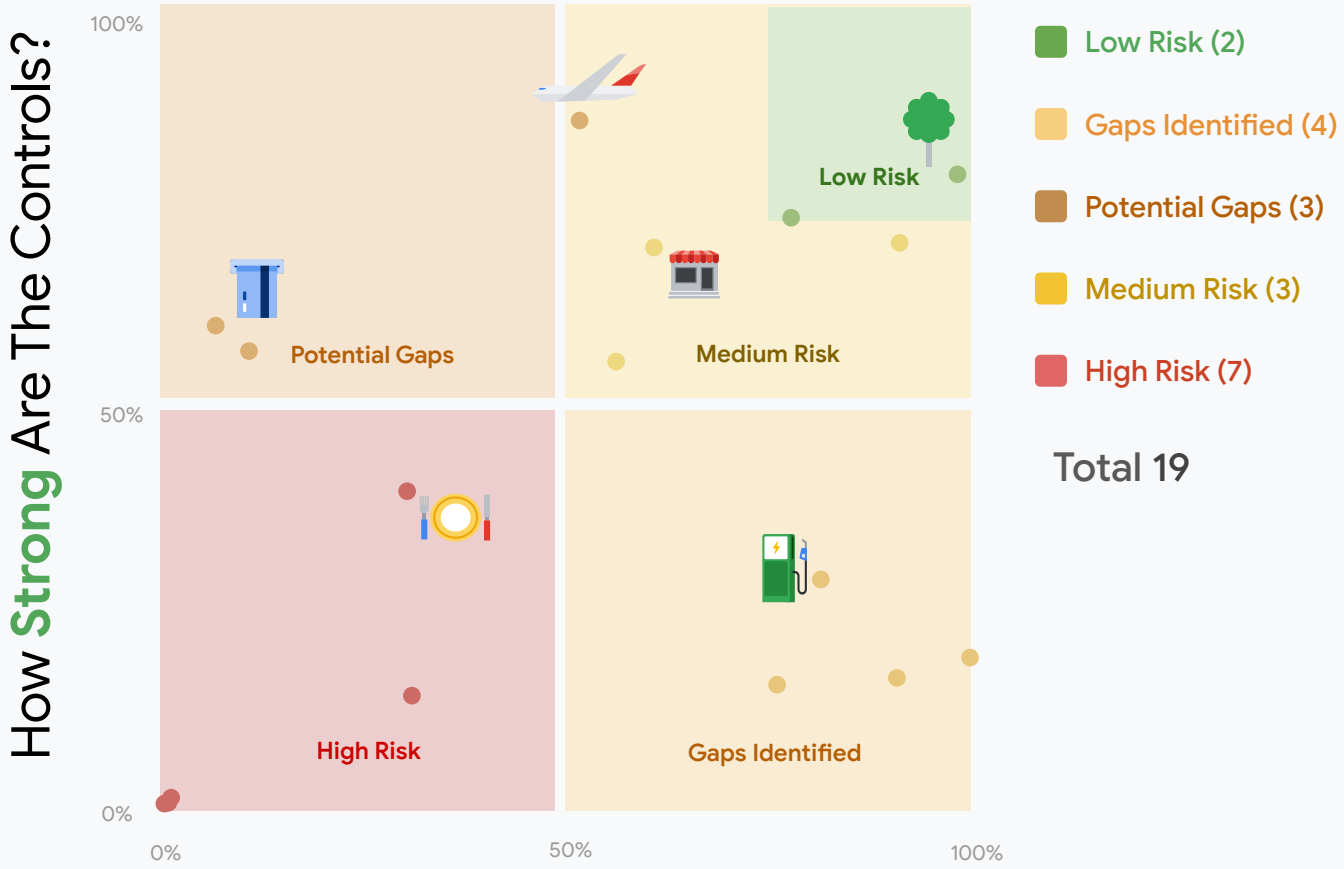
How **Strong** Are The Controls?

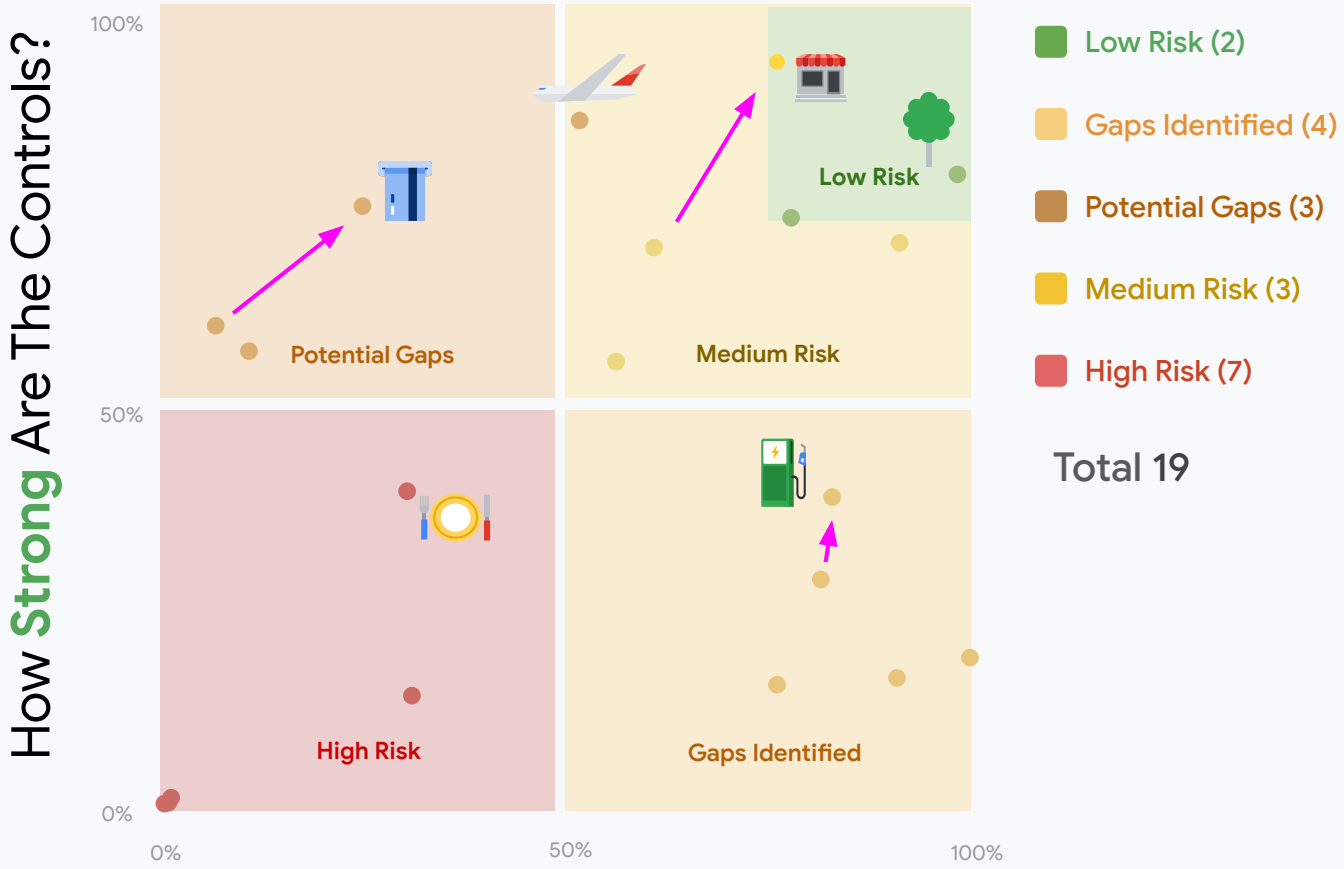


How Much Do We **Know**?

Jun 4, 2024

	How Much Do We Know?	How Strong Are The Controls?
	86%	4%
	47%	0%
	75%	9%
	15%	1%
	100%	59%


How Strong Are The Controls?
100%
50%
0%
0%
50%
100%
Low Risk
Potential Gaps
Medium Risk
High Risk
Gaps Identified
Low Risk (2)
Gaps Identified (4)
Potential Gaps (3)
Medium Risk (3)
High Risk (7)
Total 19
How Much Do We Know?


How Strong Are The Controls?
100%
50%
0%
0%
50%
100%
Potential Gaps
Medium Risk
Low Risk
High Risk
Gaps Identified
Low Risk (2)
Gaps Identified (4)
Potential Gaps (3)
Medium Risk (3)
High Risk (7)
Total 19
How Much Do We Know?

Buy-in



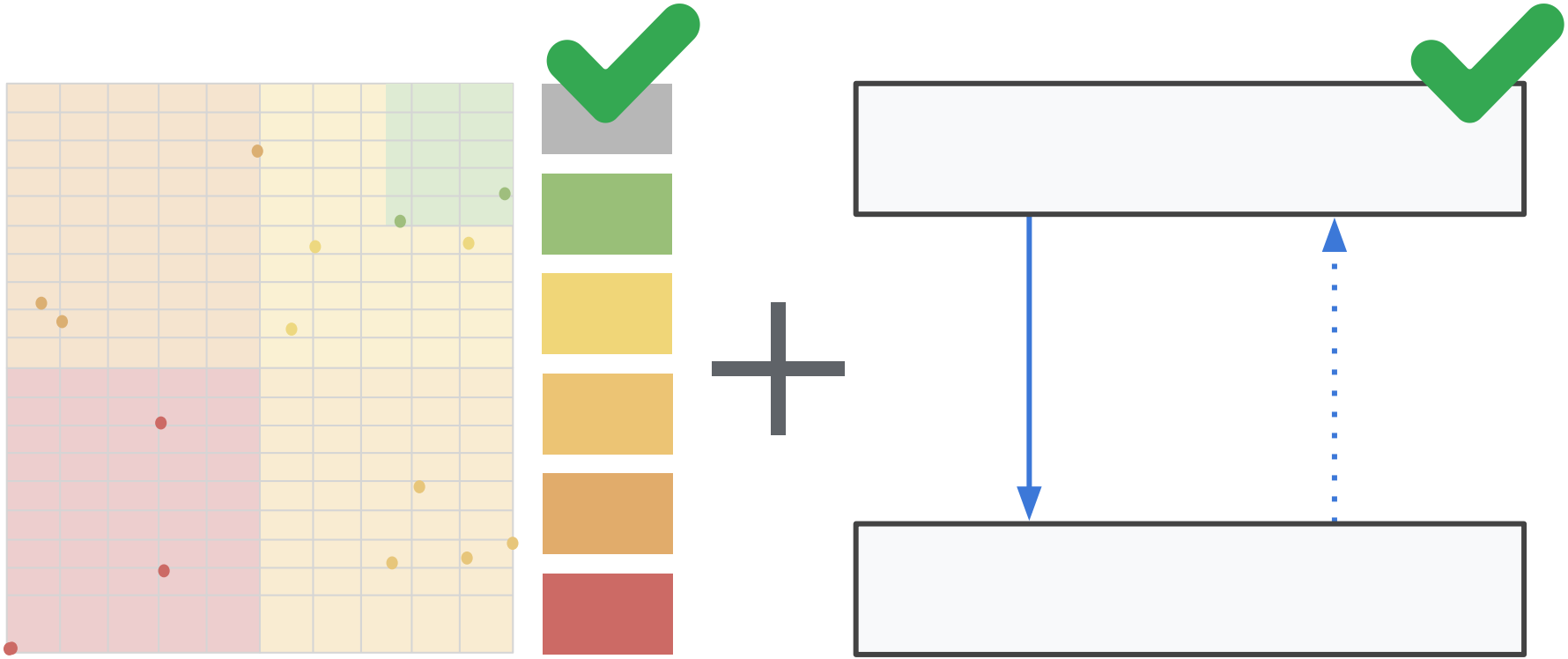
Buy-in 

Scalability 

Buy-in 

Scalability 

Efficiency 

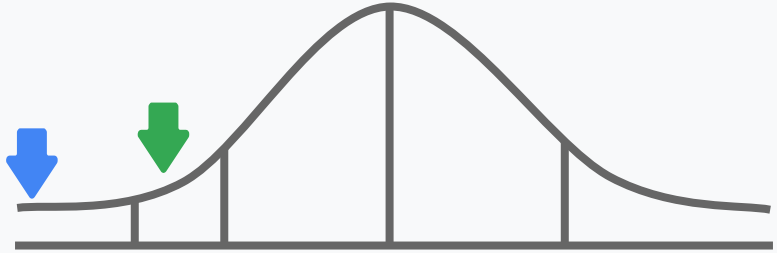


Jun 4, 2024

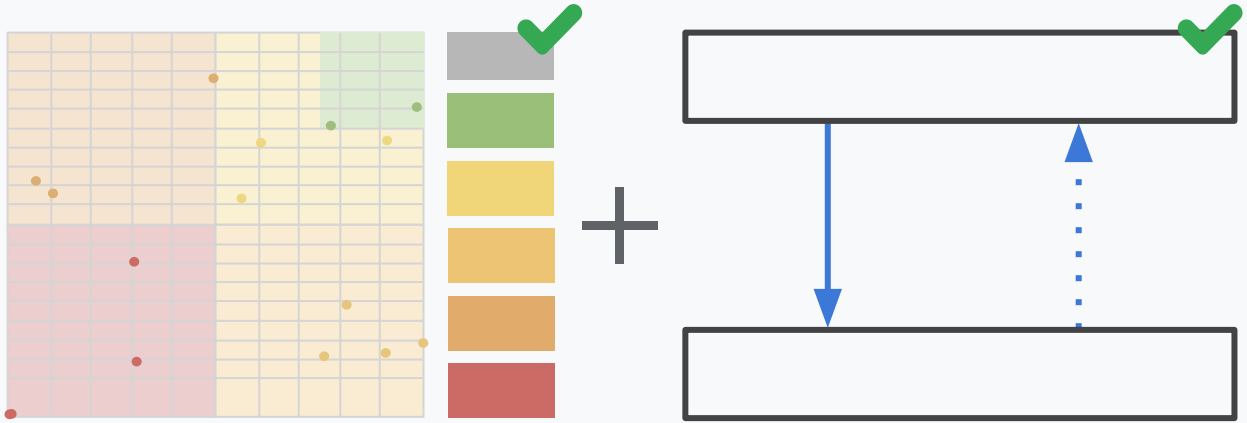
STPA ADOPTION

Recap

Google



Buy-in ✔ Scalability ✔ Efficiency ✔



Questions?