

The Journey to Compliance



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



There is nothing in PCI DSS
that says “do this to
become compliant”

This is how I do it



The Compliance Journey

Prepare

Understand Scope

Scope Reduction

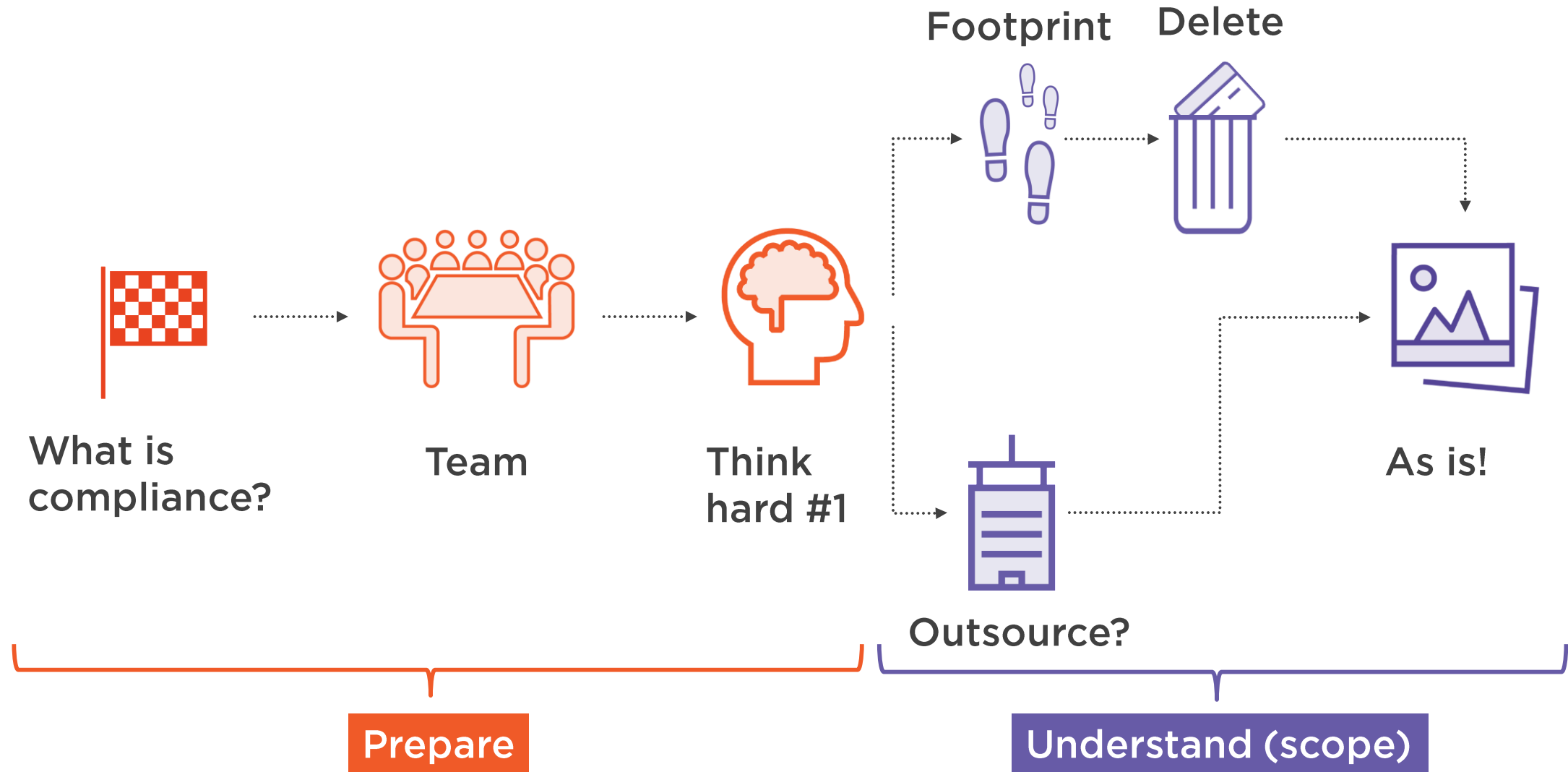
Remediate

Assessment

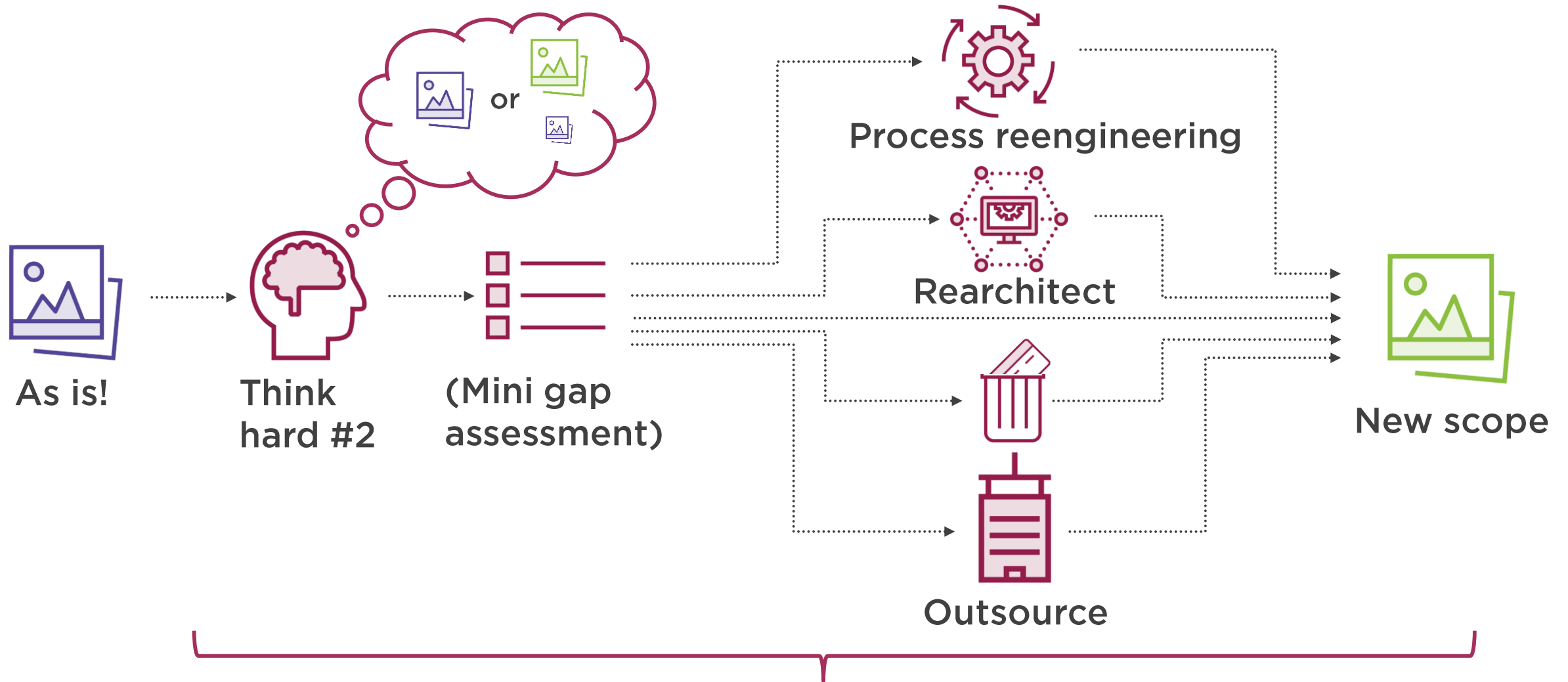
BAU Maintenance



Achieving Compliance Is a Journey



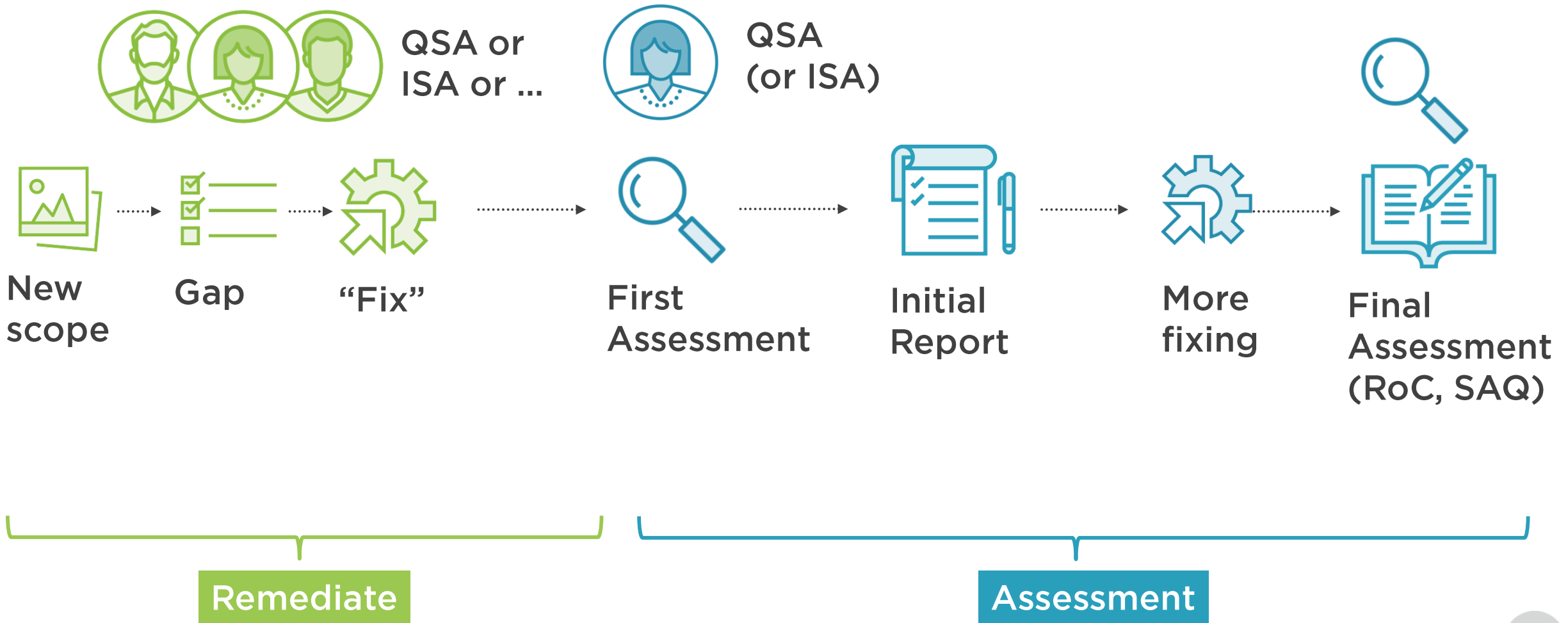
Achieving Compliance Is a Journey



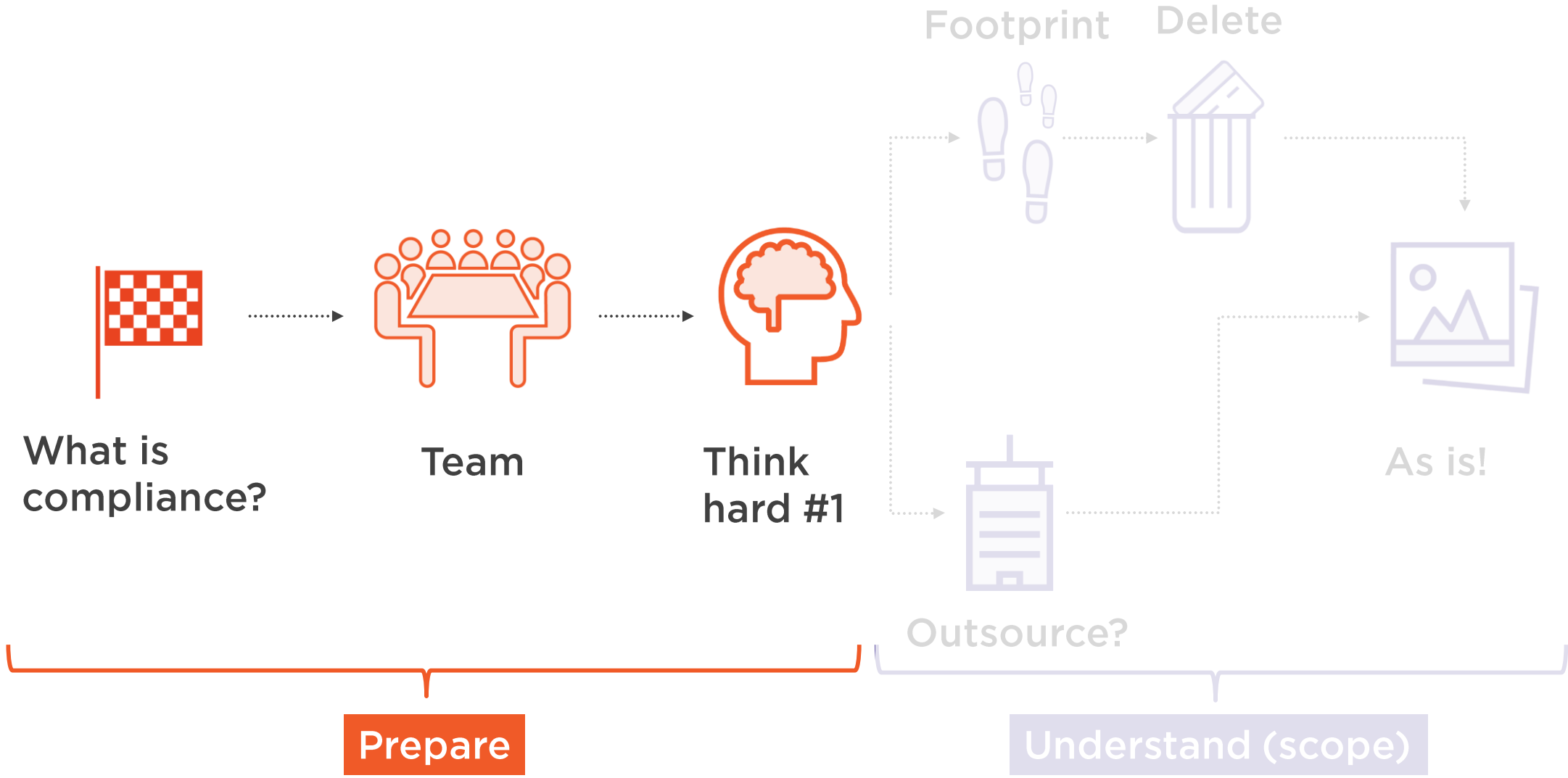
Scoping, segmentation & scope reduction



Achieving Compliance Is a Journey



Prepare



The Compliance Destination



What: RoC or SAQ

Who: Acquirer, brand or merchant

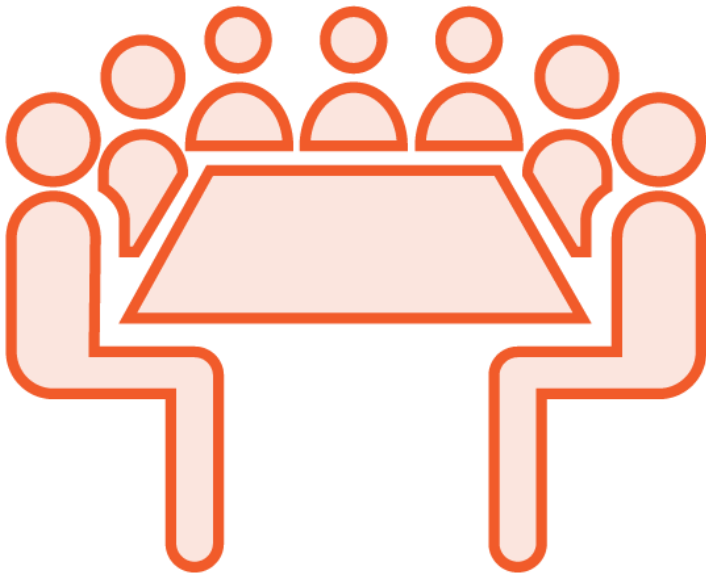
Why they want it

When:

What happens if we don't

How flexible they will be

Your PCI Team



Who owns the relationship with whoever is asking you to be compliant?

Who owns each channel?

Where is the budget coming from?

Who will deliver a PCI DSS Project / Program?

Who is your executive sponsor?

First Hard Think!



What is the chance of success?

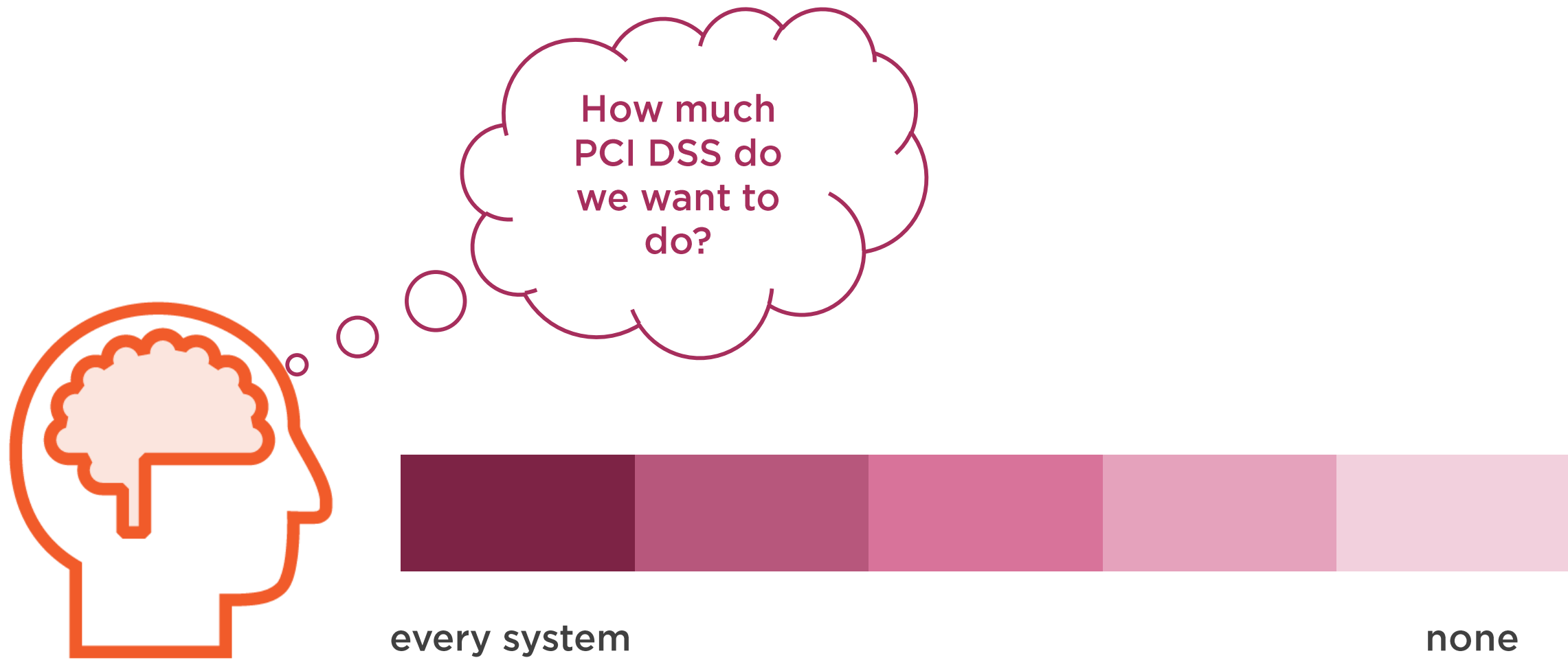
Is this a tick-box exercise?

Do we also want to get more secure

Do we need external help now?

- Cost of achieving compliance
- Cost of maintaining compliance





Alignment

Security



Compliance



How much
PCI?



Alignment

Security



Compliance



How much
PCI?



Some Mismatches Are Hard

Security



Compliance



How much
PCI?



Some Force Strategy

Security



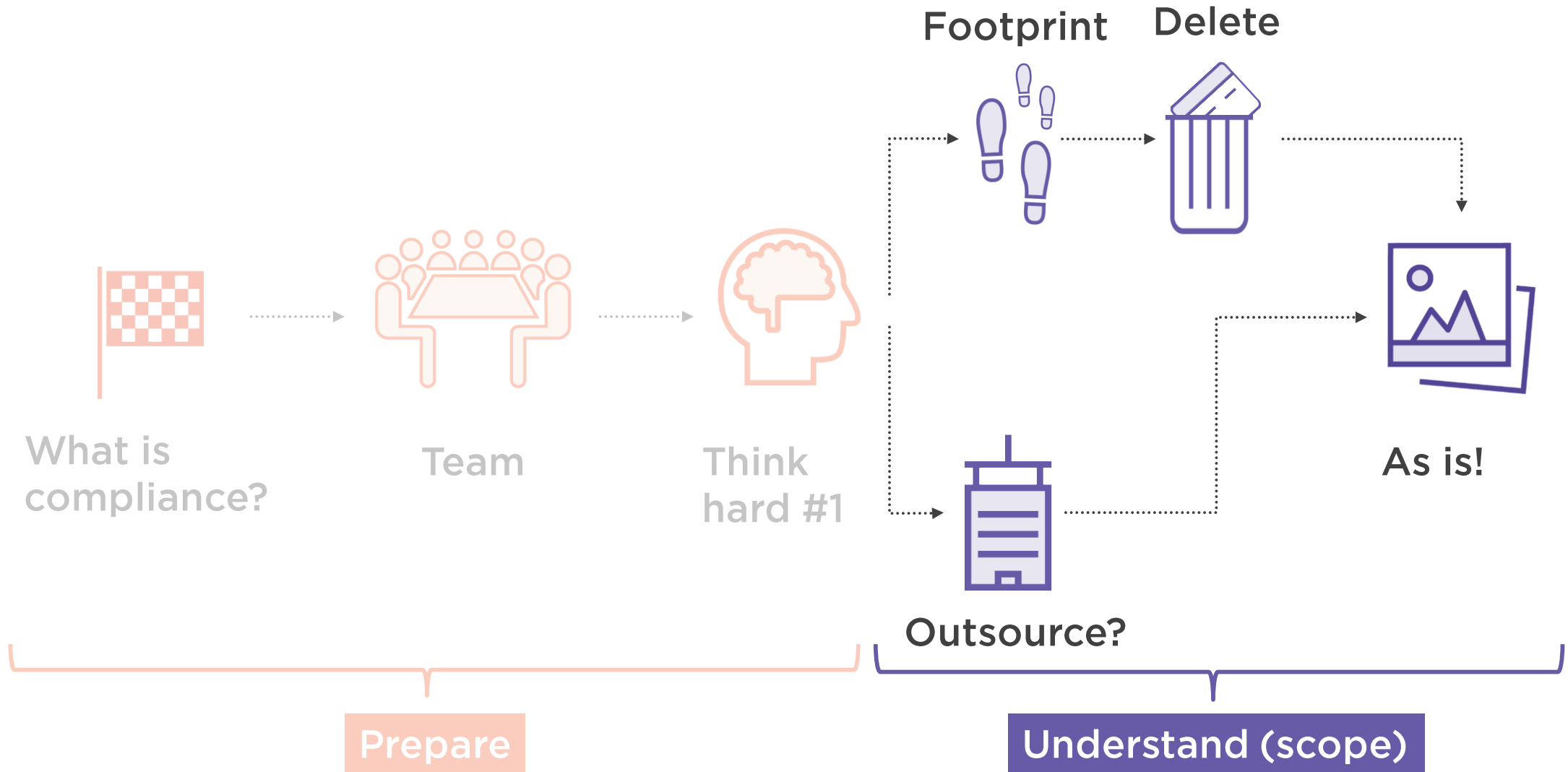
Compliance



How much
PCI?



Understand



The next destination
is to get this picture
as clear (accurate) as
we possibly can



What's the Cardholder Data Footprint?



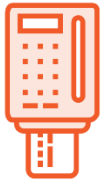
Where is cardholder data stored, processed or transmitted?

- Systems
- Networks
- Applications

Business process analysis

Discover cardholder data

How Are Cards Processed?



Face-to-face retail



e-Commerce



Mail Order / Telephone Order (MOTO)



For Each Channel – Process Analysis

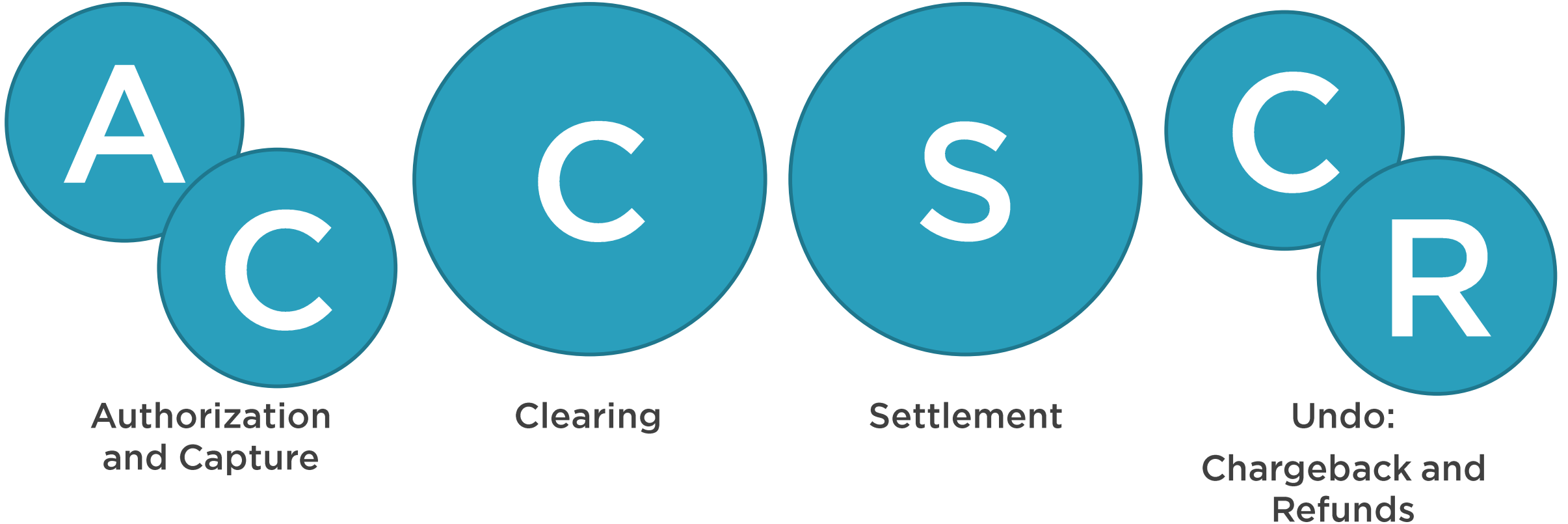
**Where does the
data go?**

**How much data is
there?**

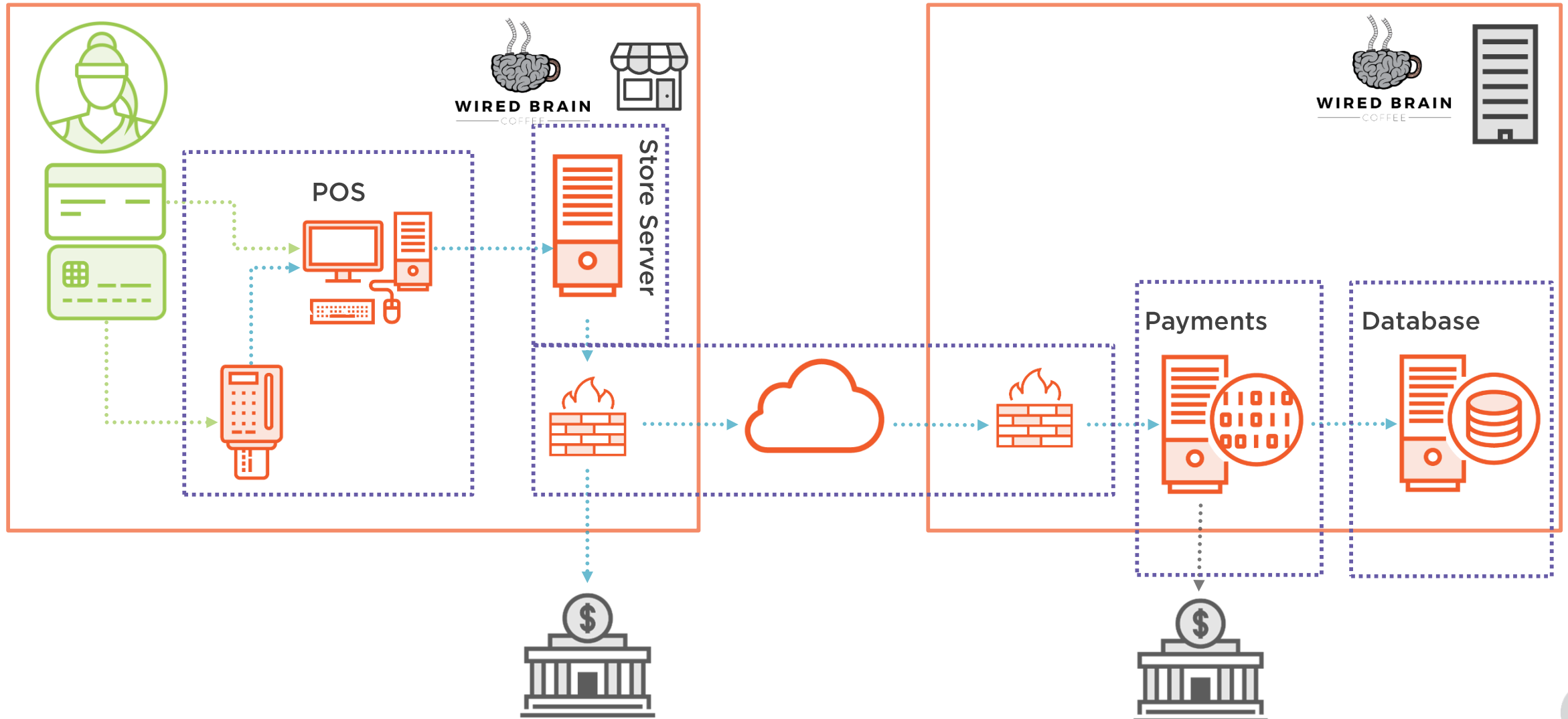
**Who owns this
business process?**



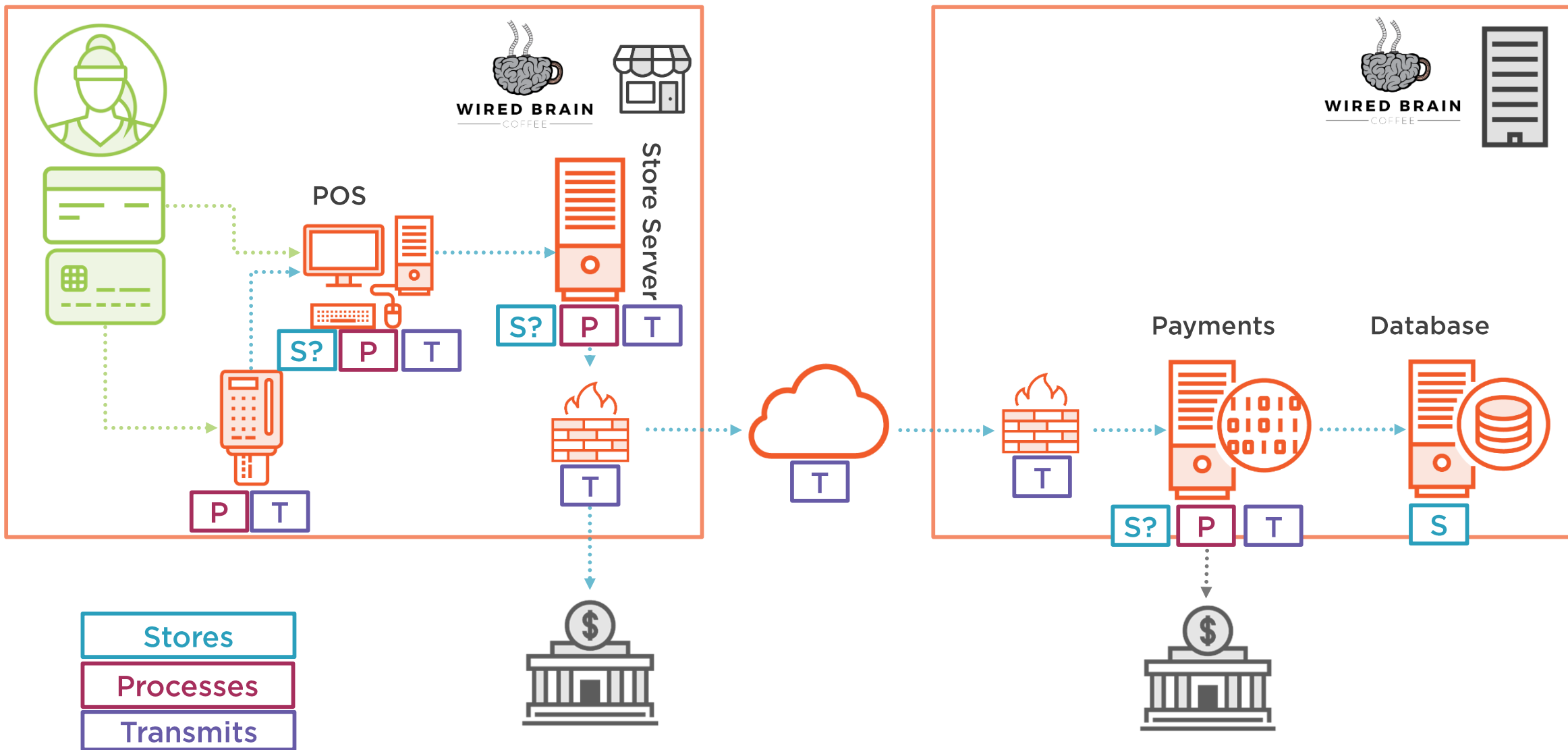
Where Is the Data?



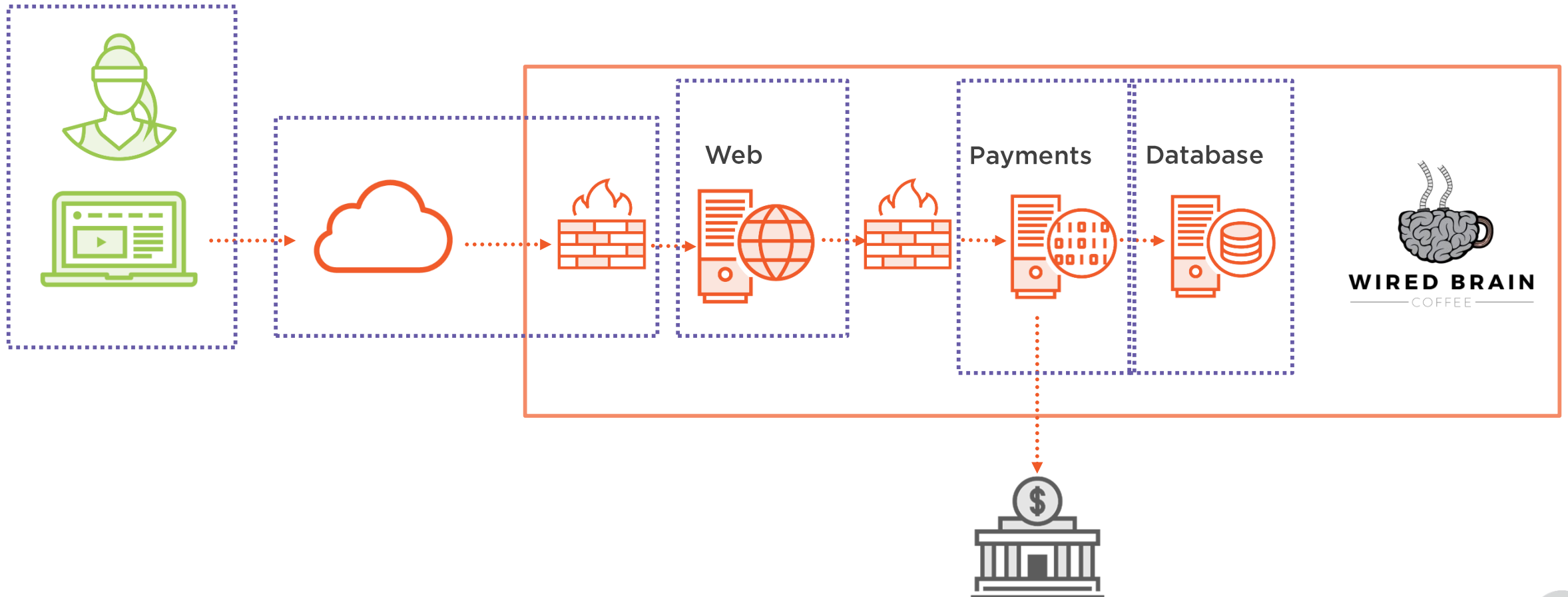
Face-to-face



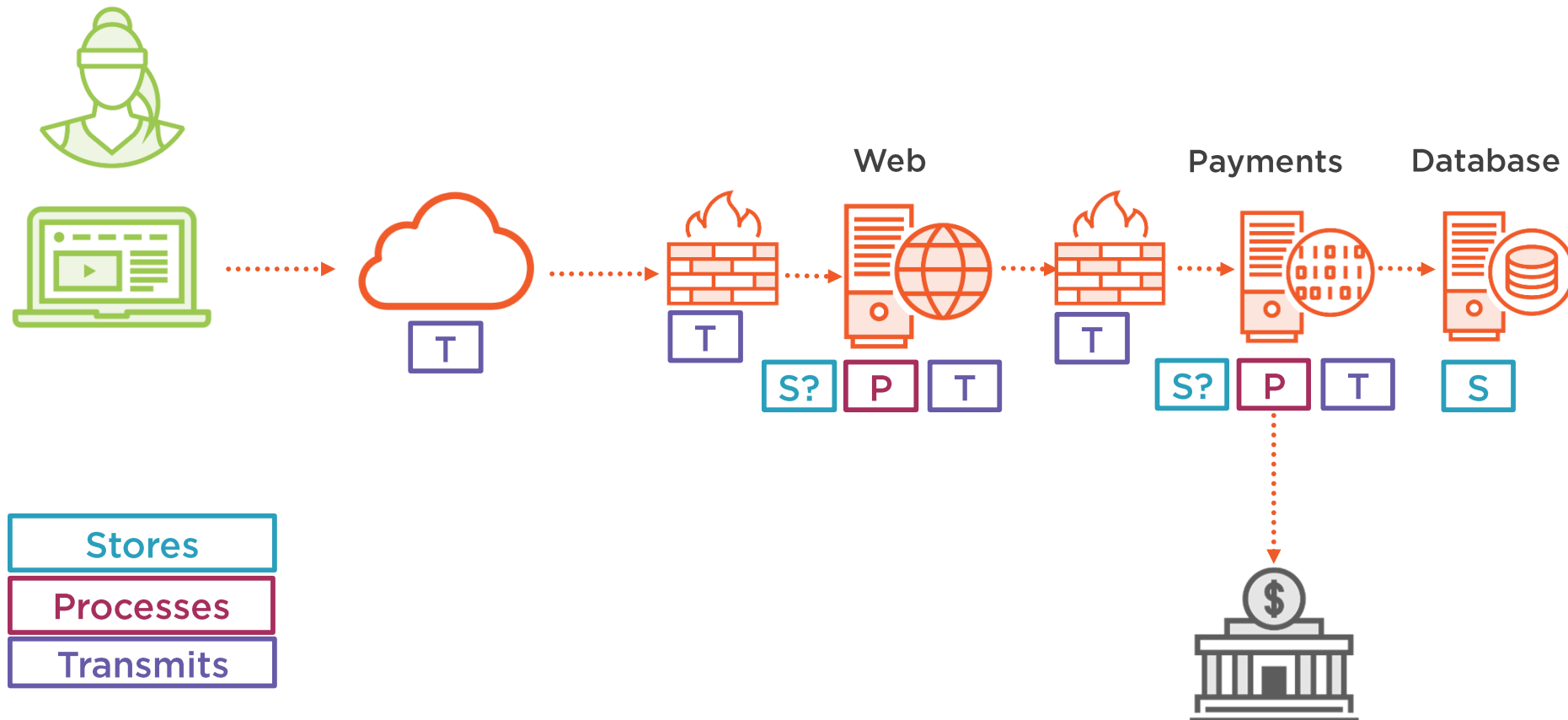
Face-to-face - Data Flow



E-commerce



E-commerce Data Flow



Data Discovery



Databases



Flat files



Every system

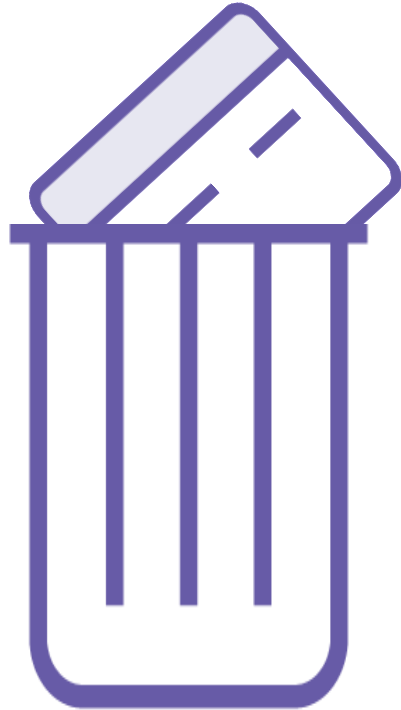


Every website



Don't forget log files





You will find unexpected cardholder data

Delete data you don't need as you find it

- Instantly reduce risk



Who Else has Your Cardholder Data?



Third parties who store, process or transmit cardholder data on your behalf

Or who can affect the security of cardholder data

If you speak to them ask “what PCI help or services can you also offer?”



Our Accurate Picture



What systems store, process or transmit cardholder data?

- PAN or SAD?

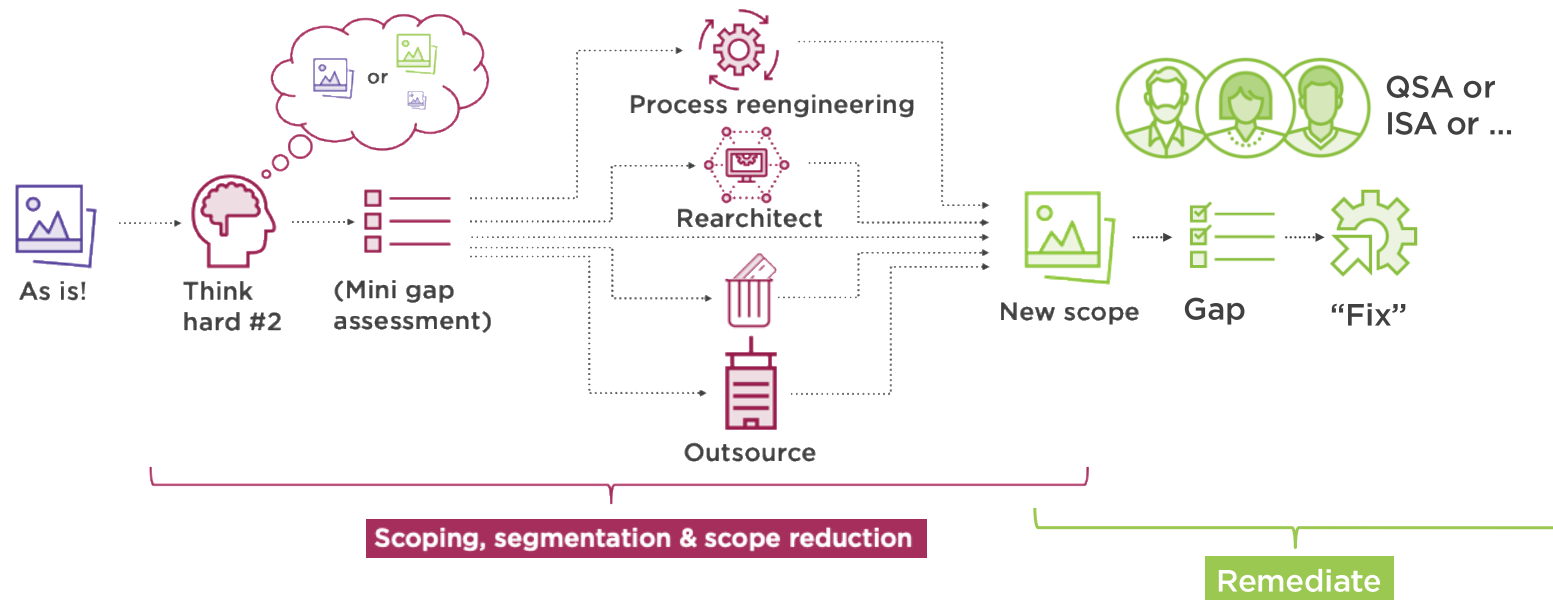
What business processes generate that?

Who owns those?

Third party service providers



Next: Scoping, Reduction, and Remediation



But in The Real World ...

