

Scoping, Segmentation, and Scope Reduction

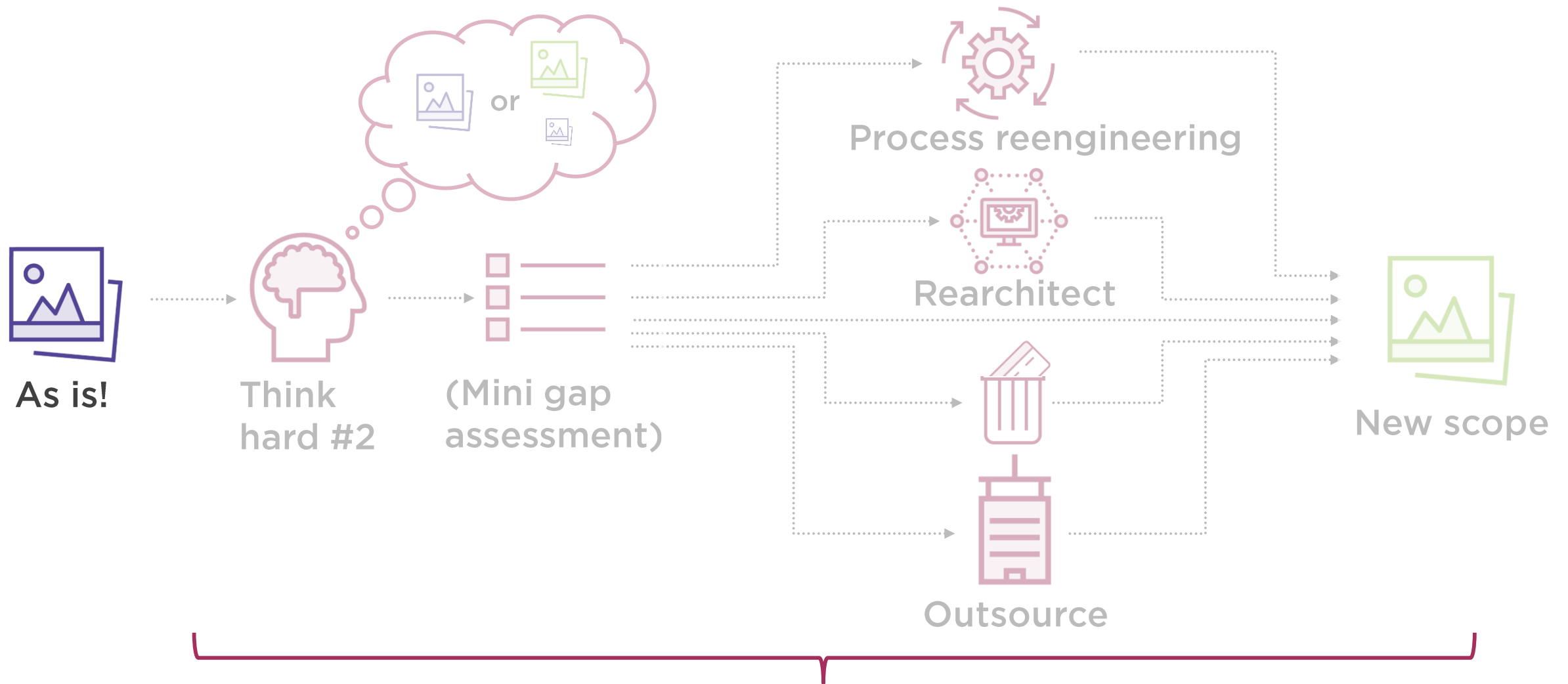


John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com





Scoping, segmentation & scope reduction





QSA or
ISA or ...



New
scope



Gap



“Fix”



Remediate



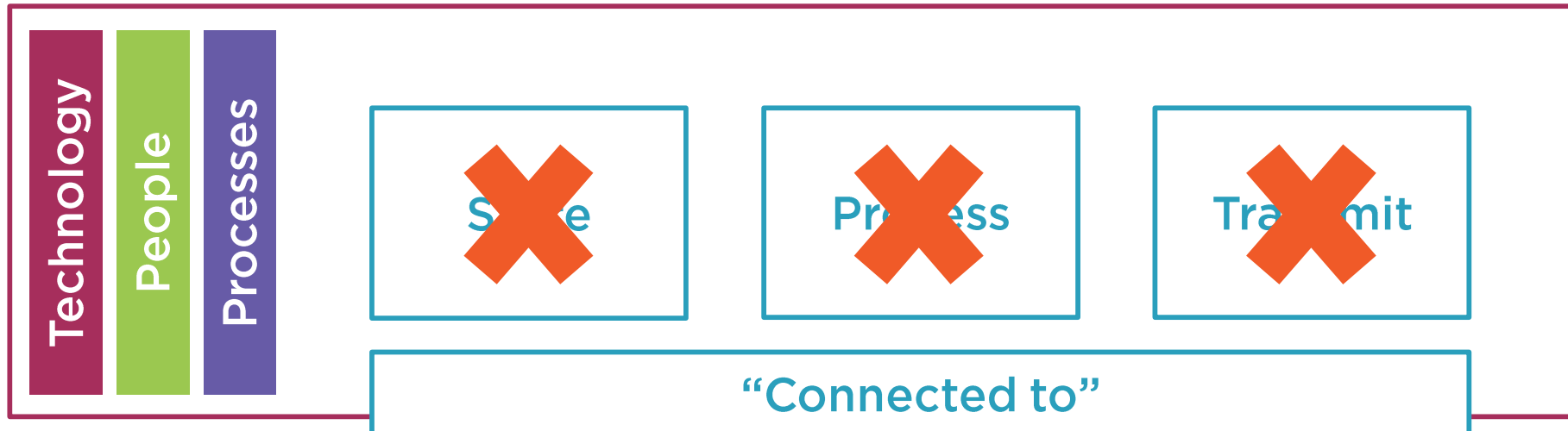
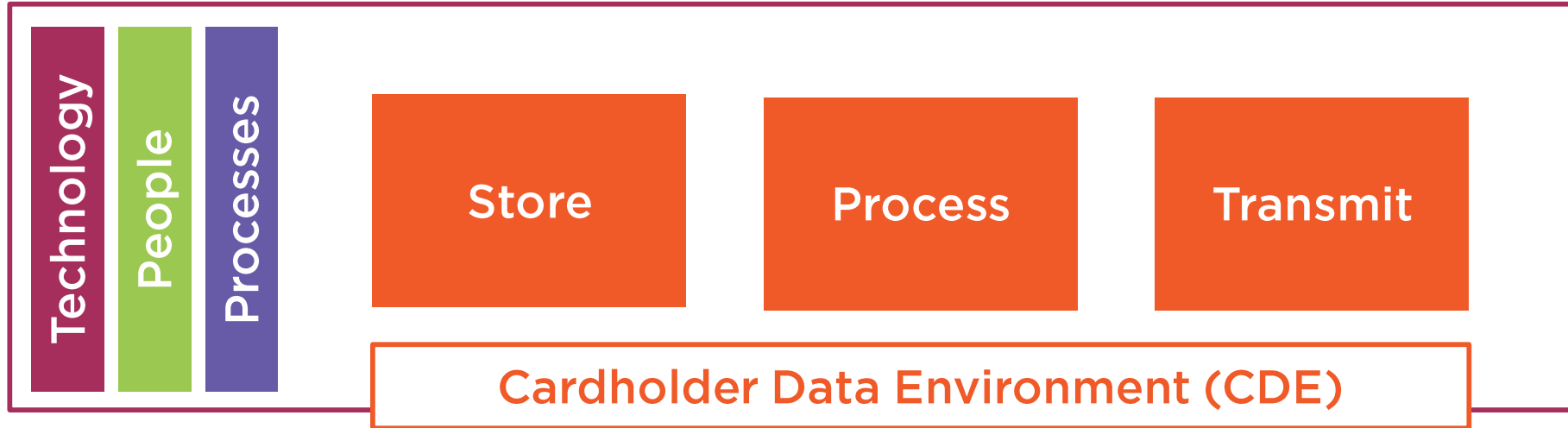
Scope: A Badly-used Word in PCI DSS

In scope of
CONSIDERATION

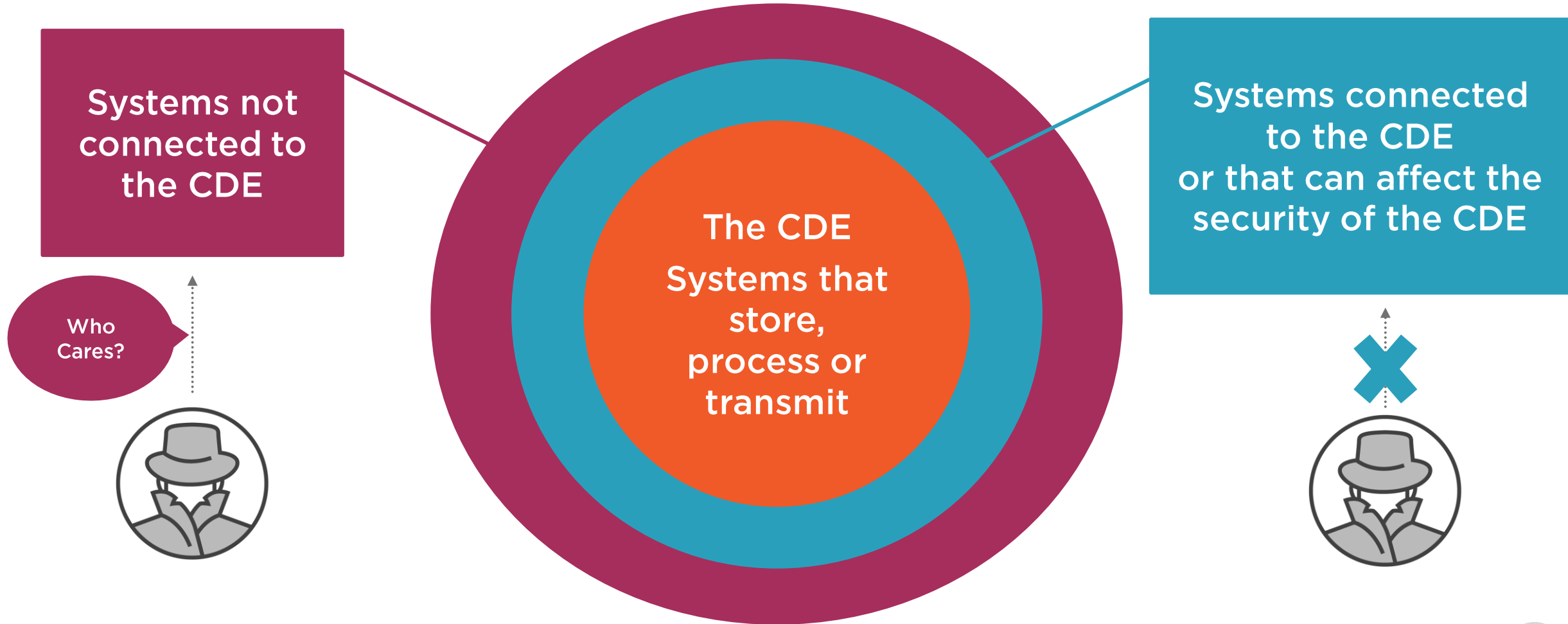
In scope of some
REQUIREMENTS



Scope of Requirements



Another Way of Thinking About Scope



Three Scopes

In scope:

Considered and decided
that no PCI DSS
requirements are applicable

In scope:

cardholder data environment

In scope:

“connected to”



We Have an 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

What's our CDE look like?

- What's 'connected to'



How much PCI DSS do you want to do?

How many new things do you want to do because of PCI DSS?

- Business change
- Security

What constraints?

- Time
- Cost

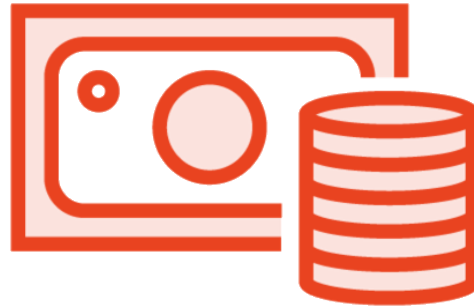
My personal strategy is to
do as little PCI DSS as I can



Why Do as Little PCI DSS as You Can?



Reduced attack
surface



Cost of ongoing
compliance



Organizational ability
to change



(De-)Scoping



What cardholder data can be deleted?



What can be outsourced?



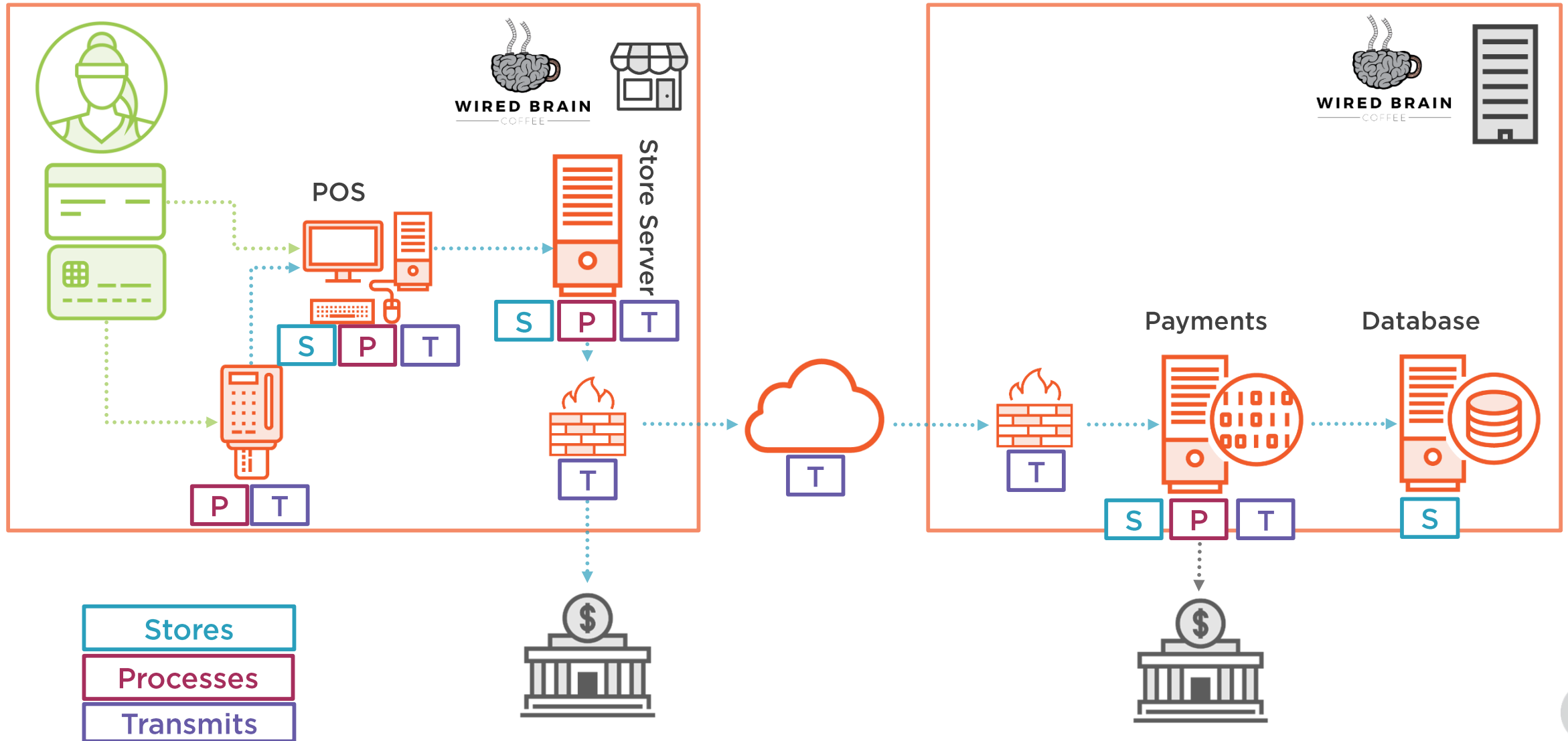
What processes can be changed?



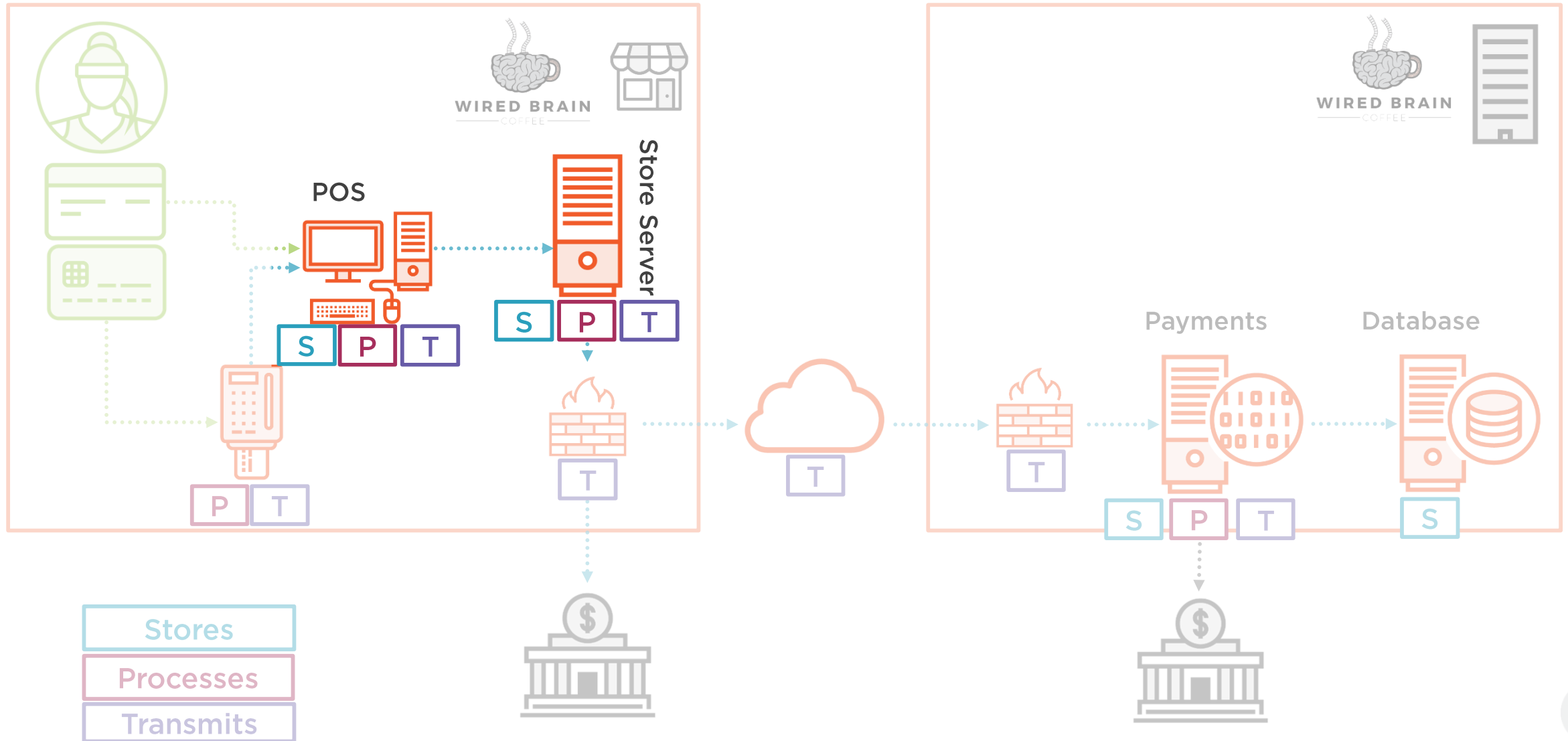
What networks and systems can be re-architected?



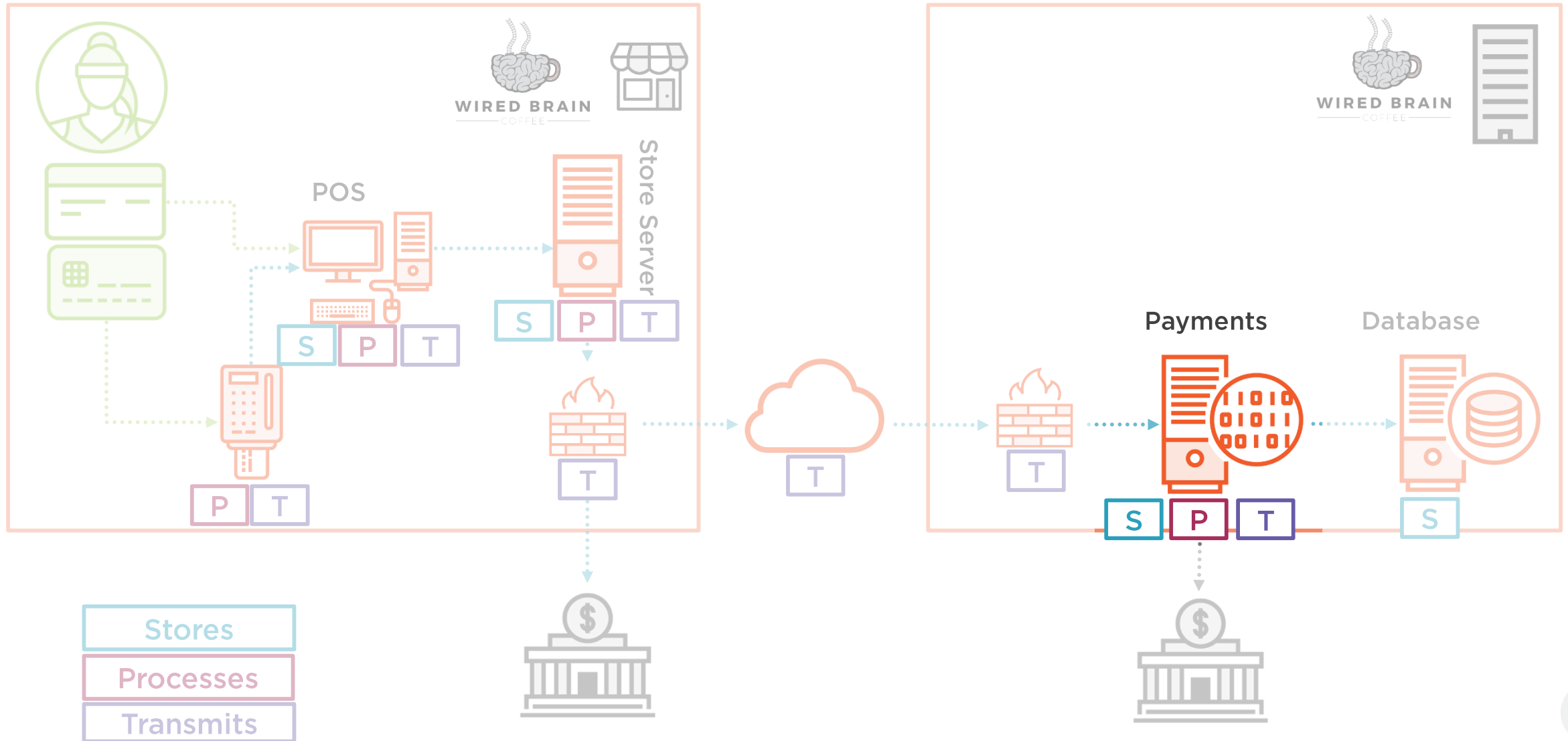
Can Data be Deleted?



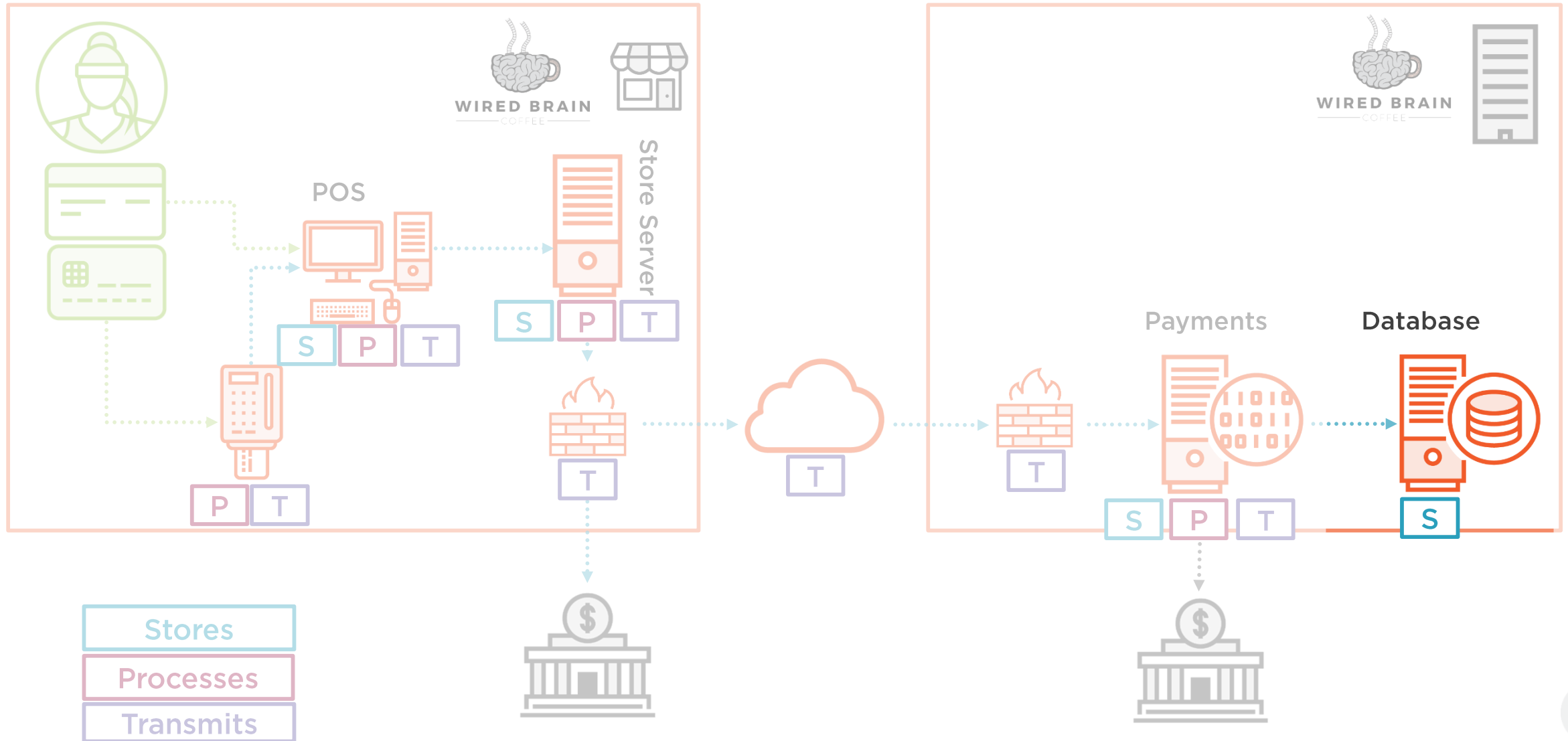
Can Data be Deleted?



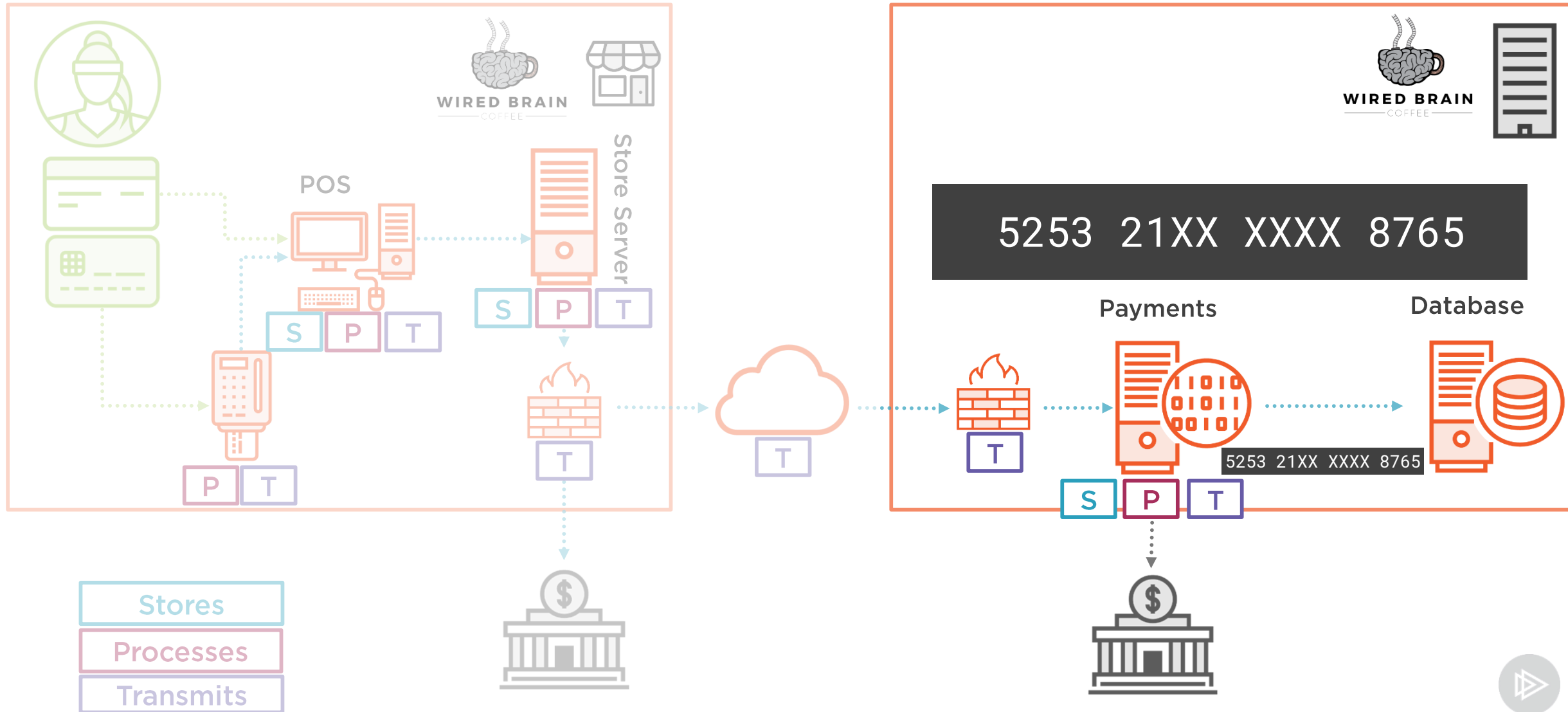
Can Data be Deleted?



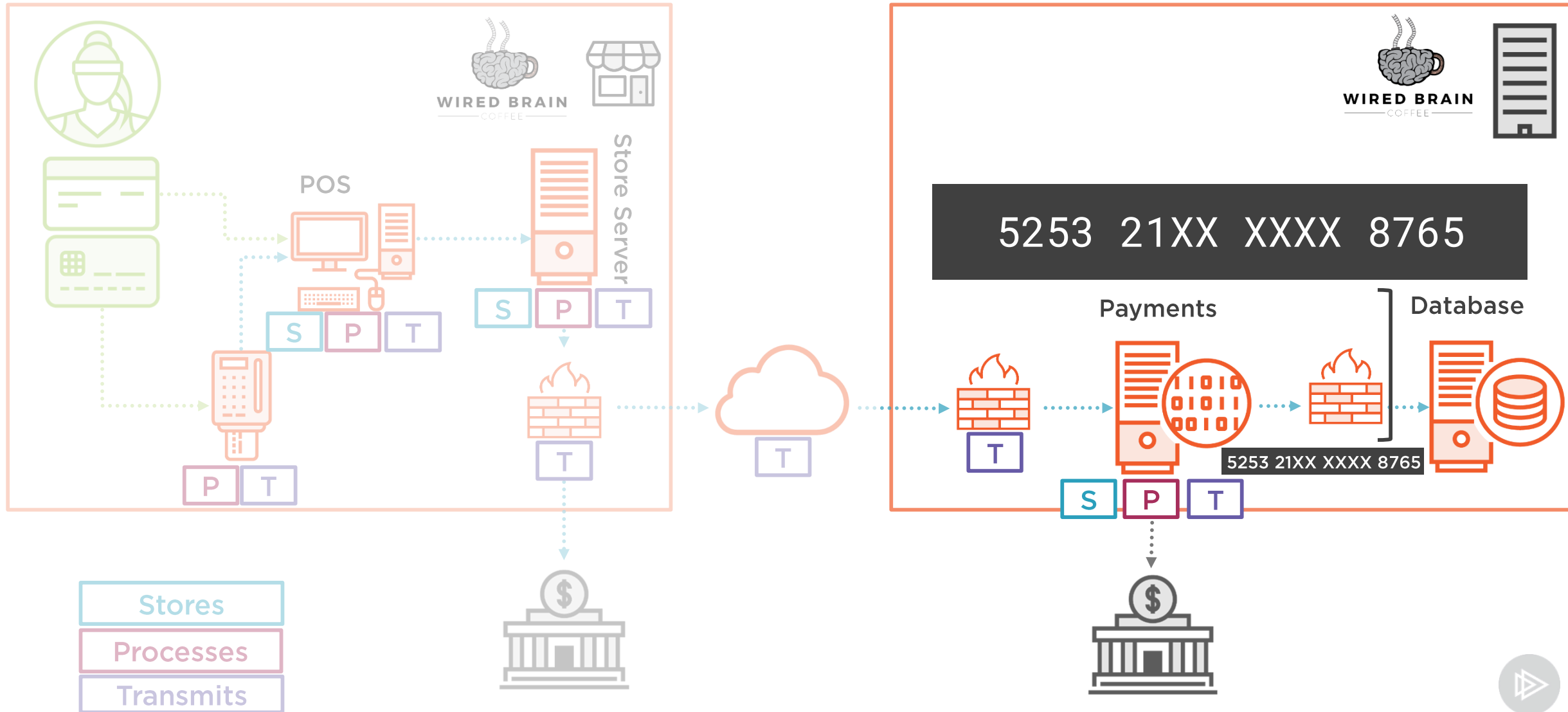
Can Data be Deleted?



Can Data be Deleted?



Can Data be Deleted?



Ways to Remove Cardholder Data

5252 87**
**** 1234

Truncation

<6:%Z6*69ypK
OF.8}P@RAQz
CDQ"Kgcb6jZ
m/I|'DiVxijroFc
Zwq+k.B'5K9g
Op

Hashing

5252 87AB
DEFQ 1234

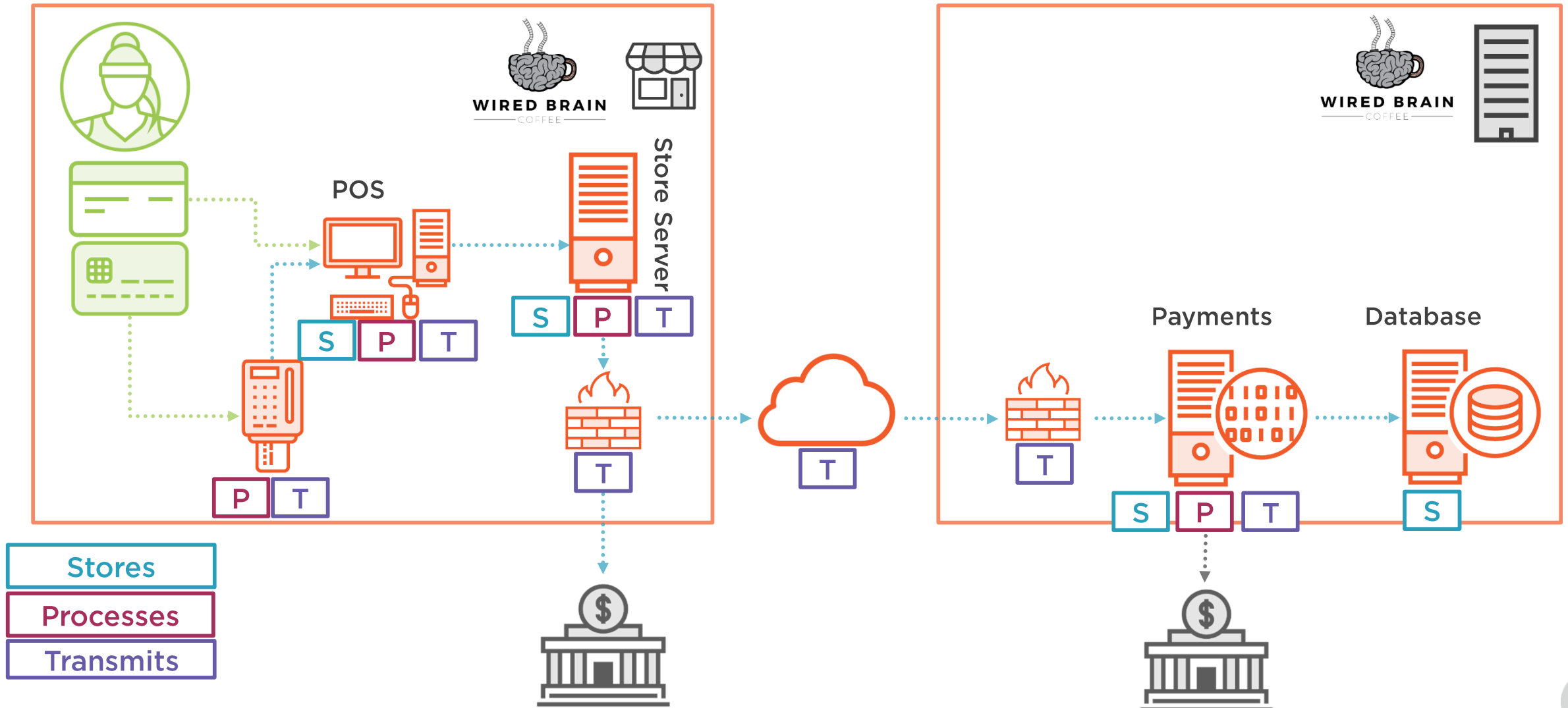
Tokenization



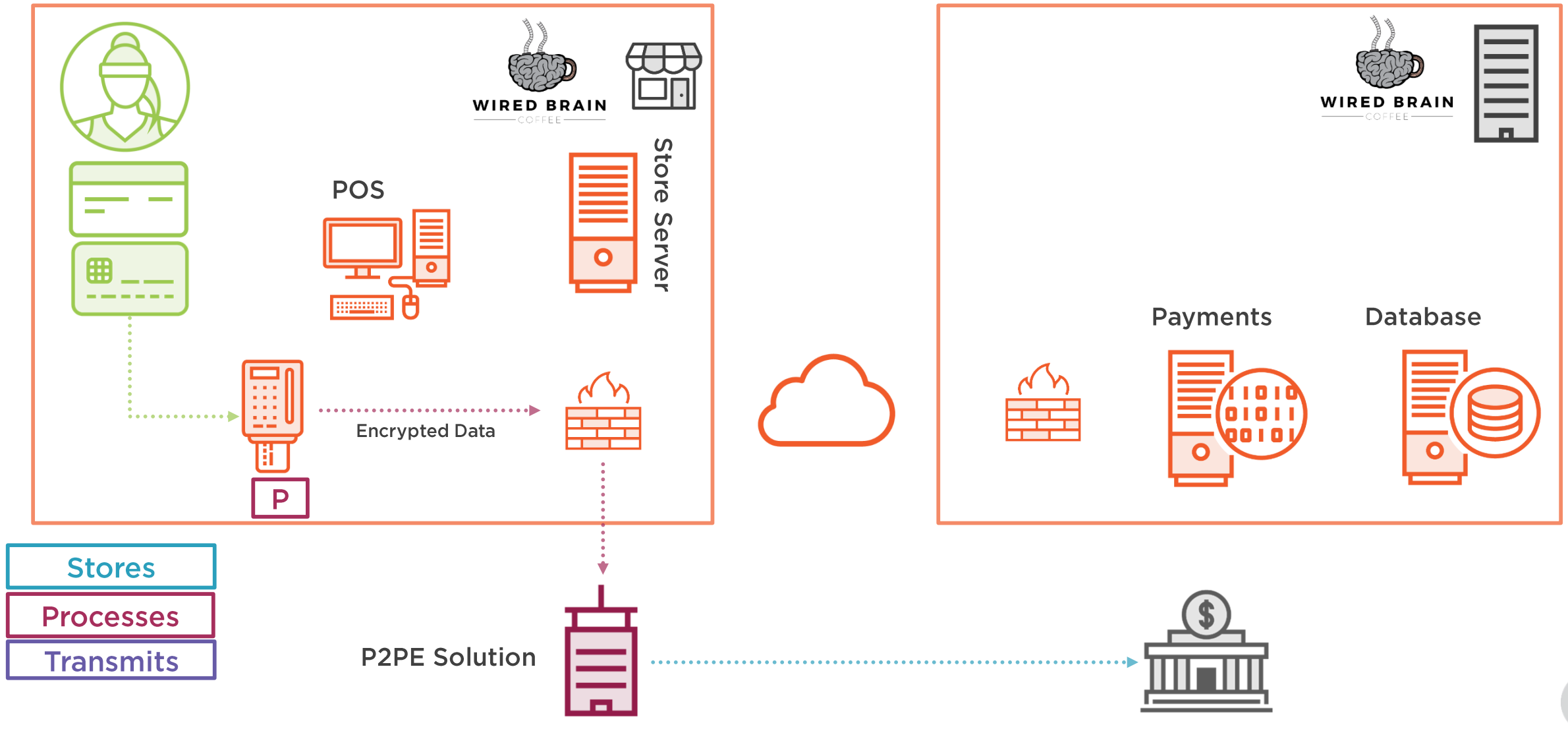
Encrypted cardholder data
is still cardholder data



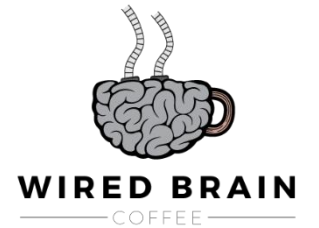
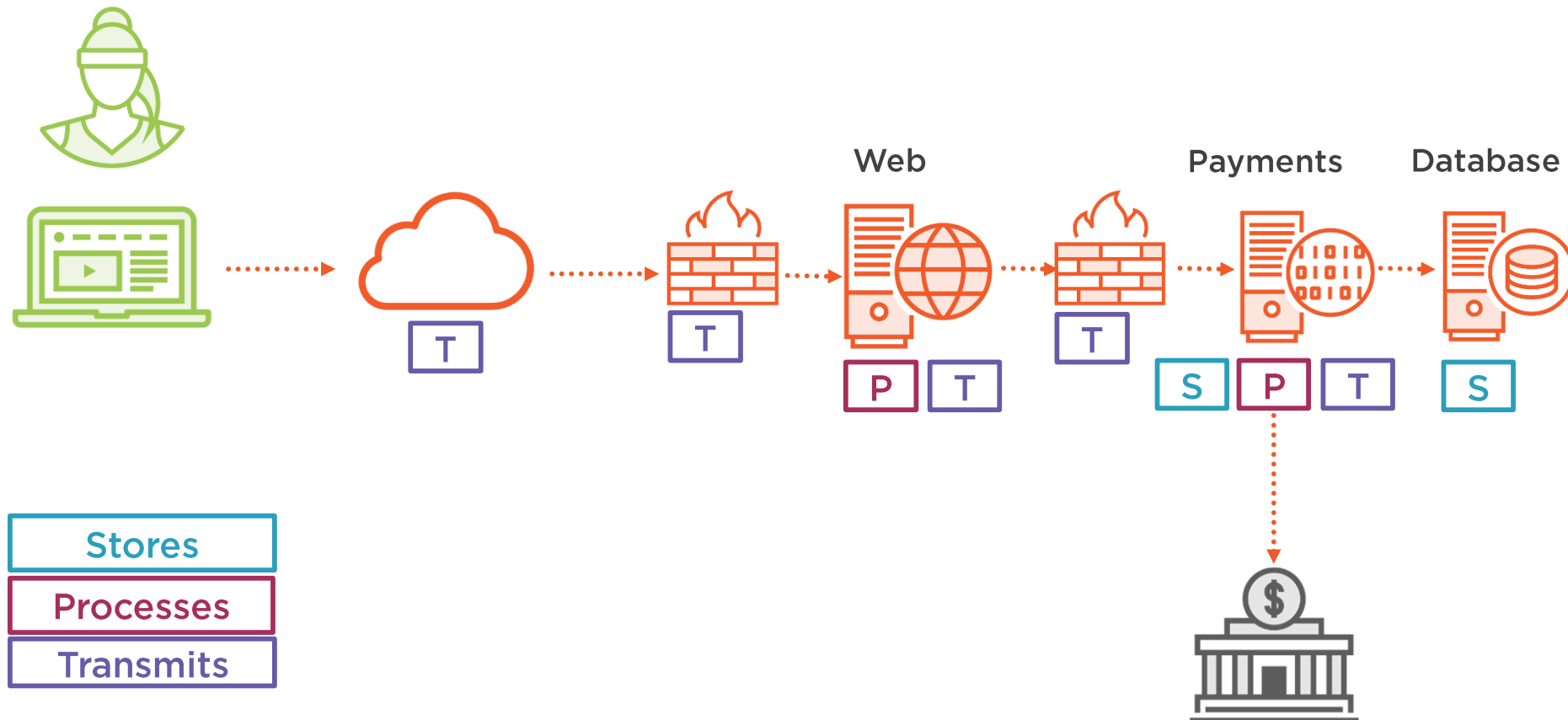
What Can be Outsourced?



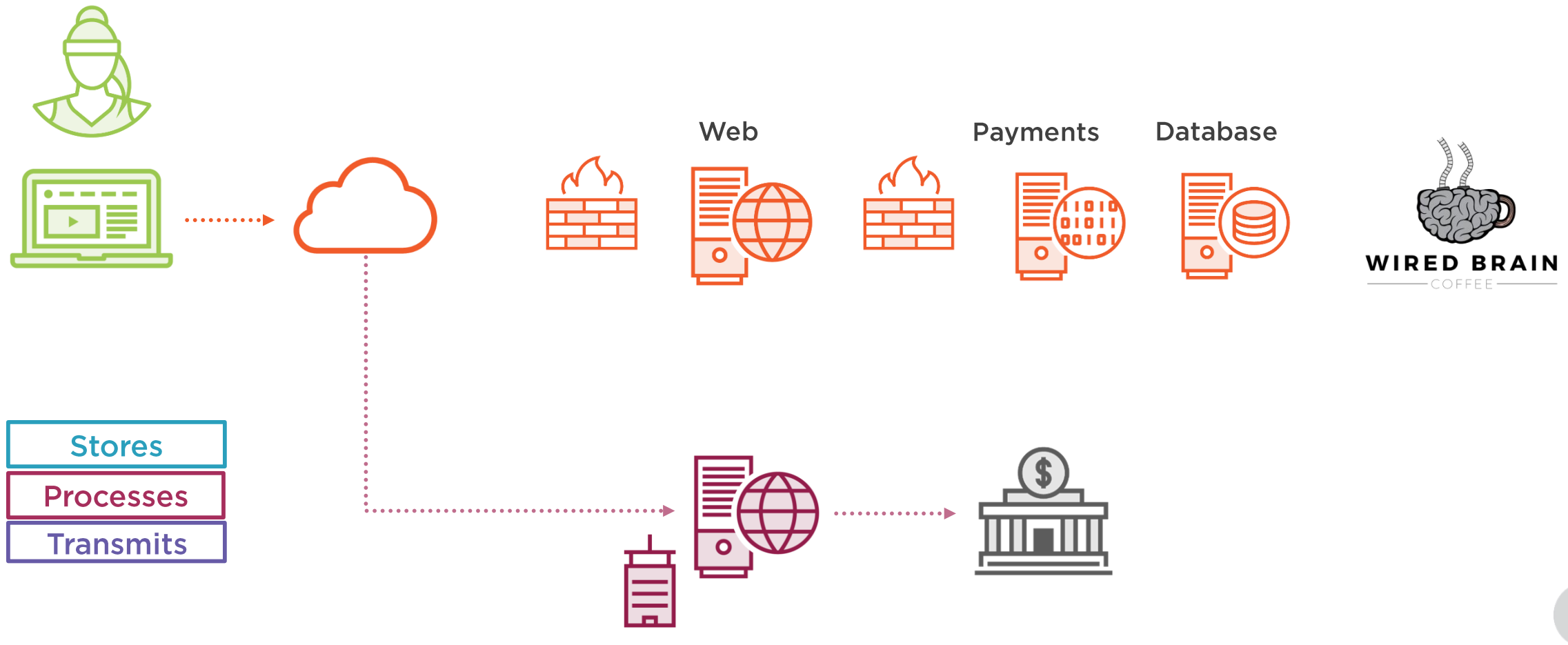
What Can be Outsourced?



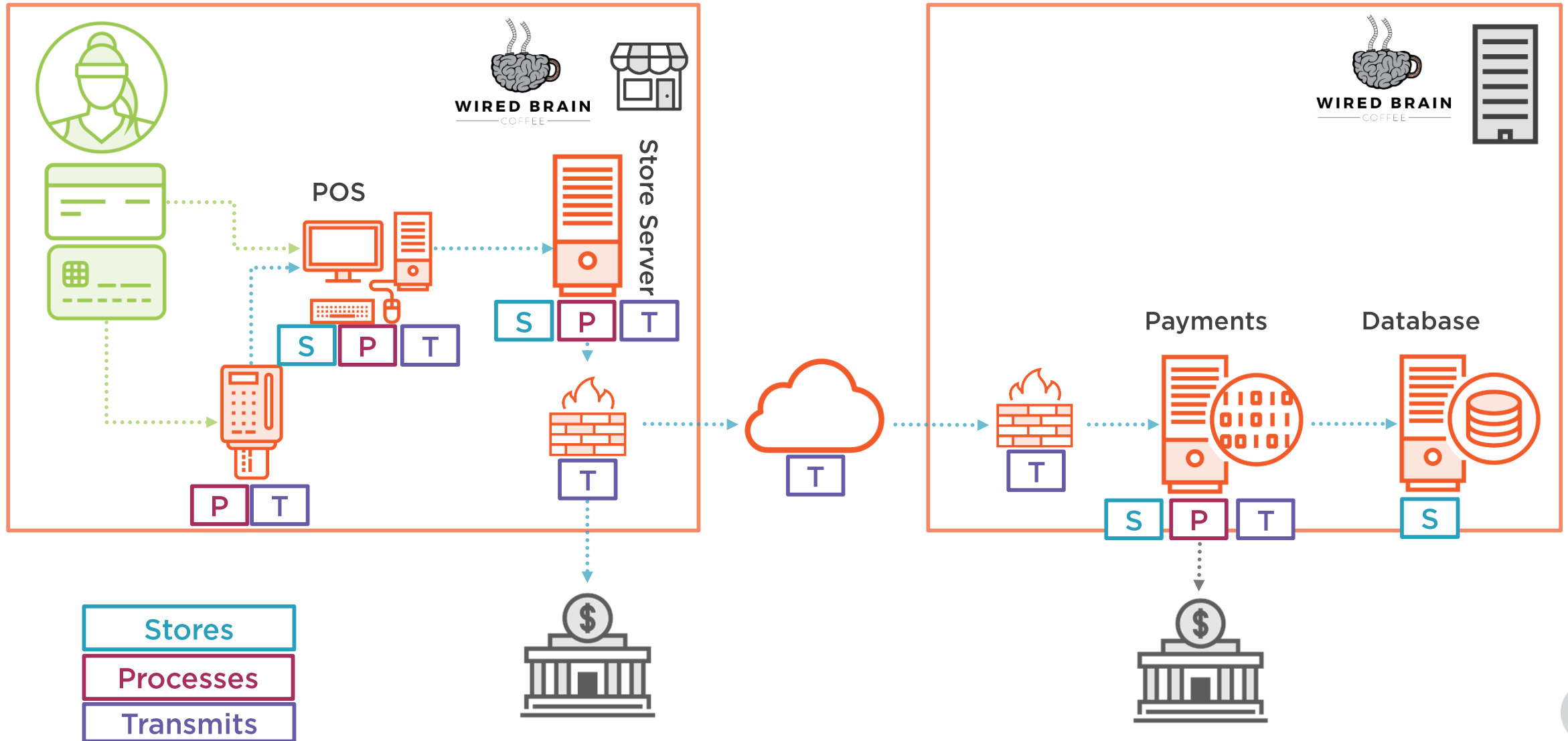
What Can be Outsourced?



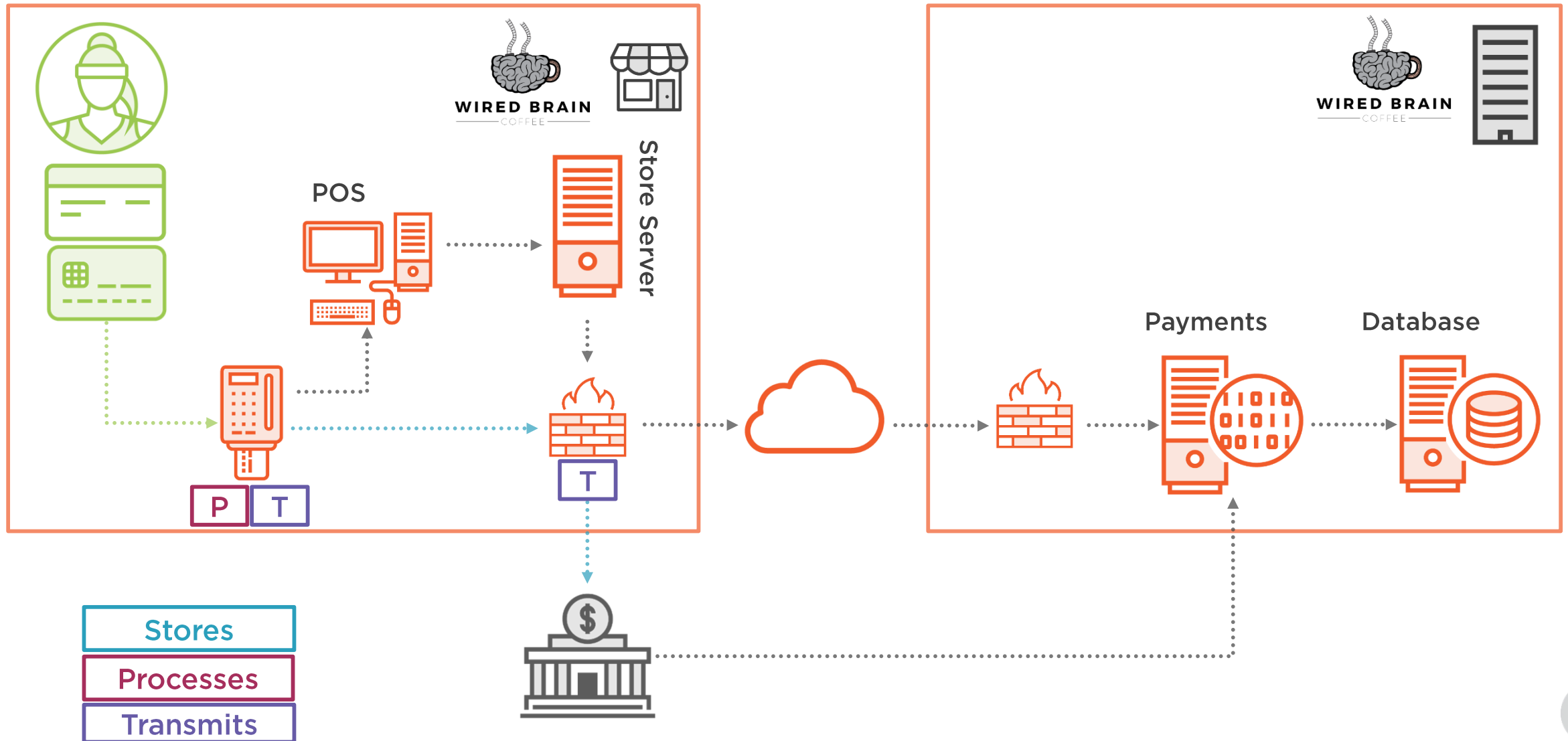
What Can be Outsourced?



Rearchitect Processes and Networks



Rearchitect Processes and Networks





Changes in scope require changes in business processes and commercial relationships. These are not IT problems.

It is strongly recommended that you get professional, independent advice (i.e. not a supplier) to validate your scoping decisions.

It's QSA time!





Standard: PCI Data Security Standard (PCI DSS)

Date: May 2017

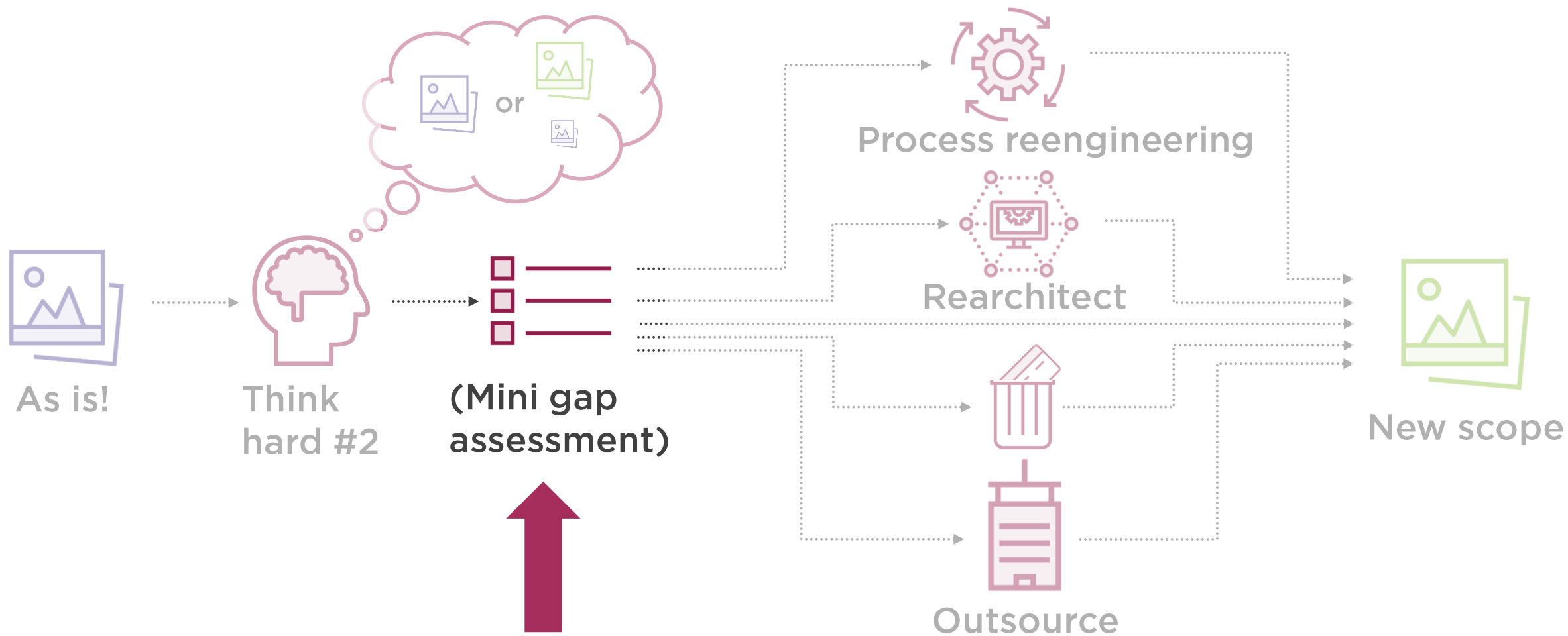
Author: PCI Security Standards Council

**Information Supplement:
Guidance for PCI DSS Scoping
and Network Segmentation**

Scoping guidance and worked examples

[https://www.pcisecuritystandards.org/documents/
Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf](https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf)





Mini-gap Assessment

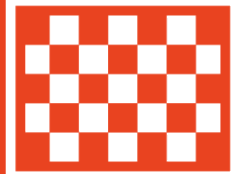


=



Final scope

+



Compliance target

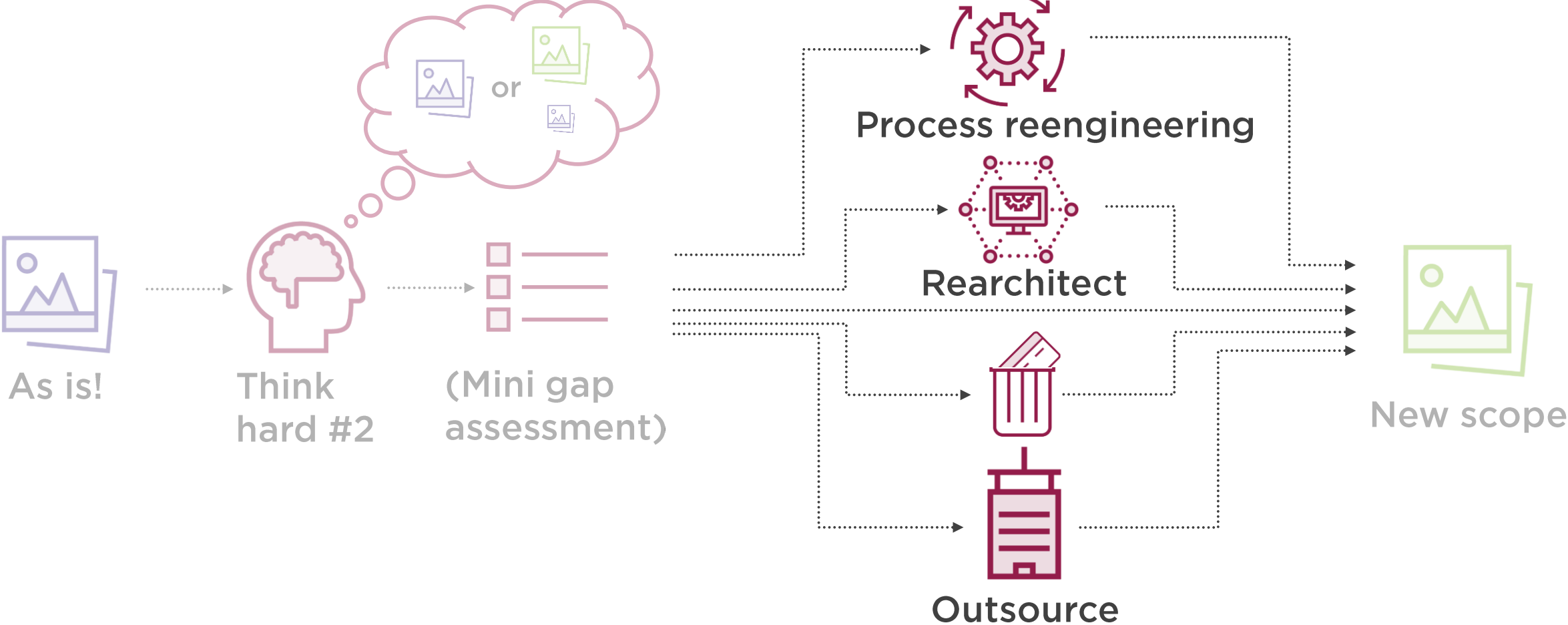
What requirements are in place?

What do we need to buy?

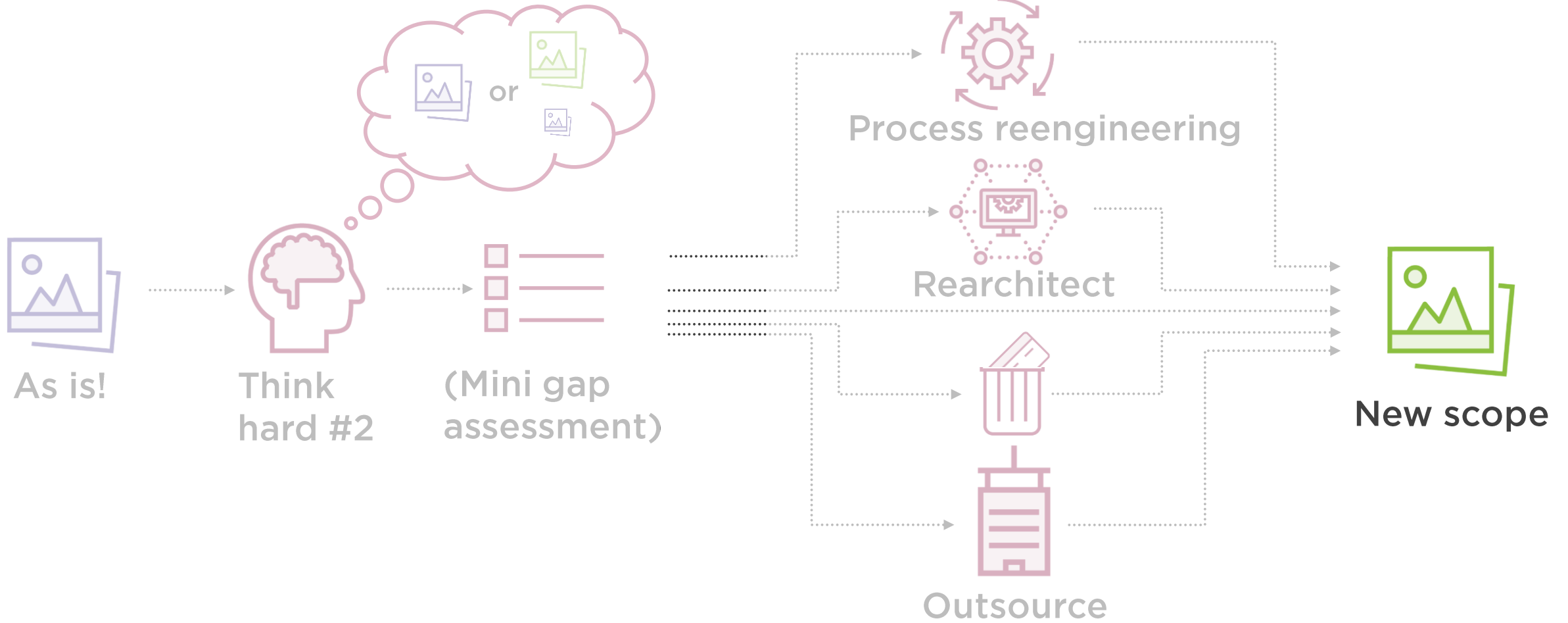
What do we need to change?



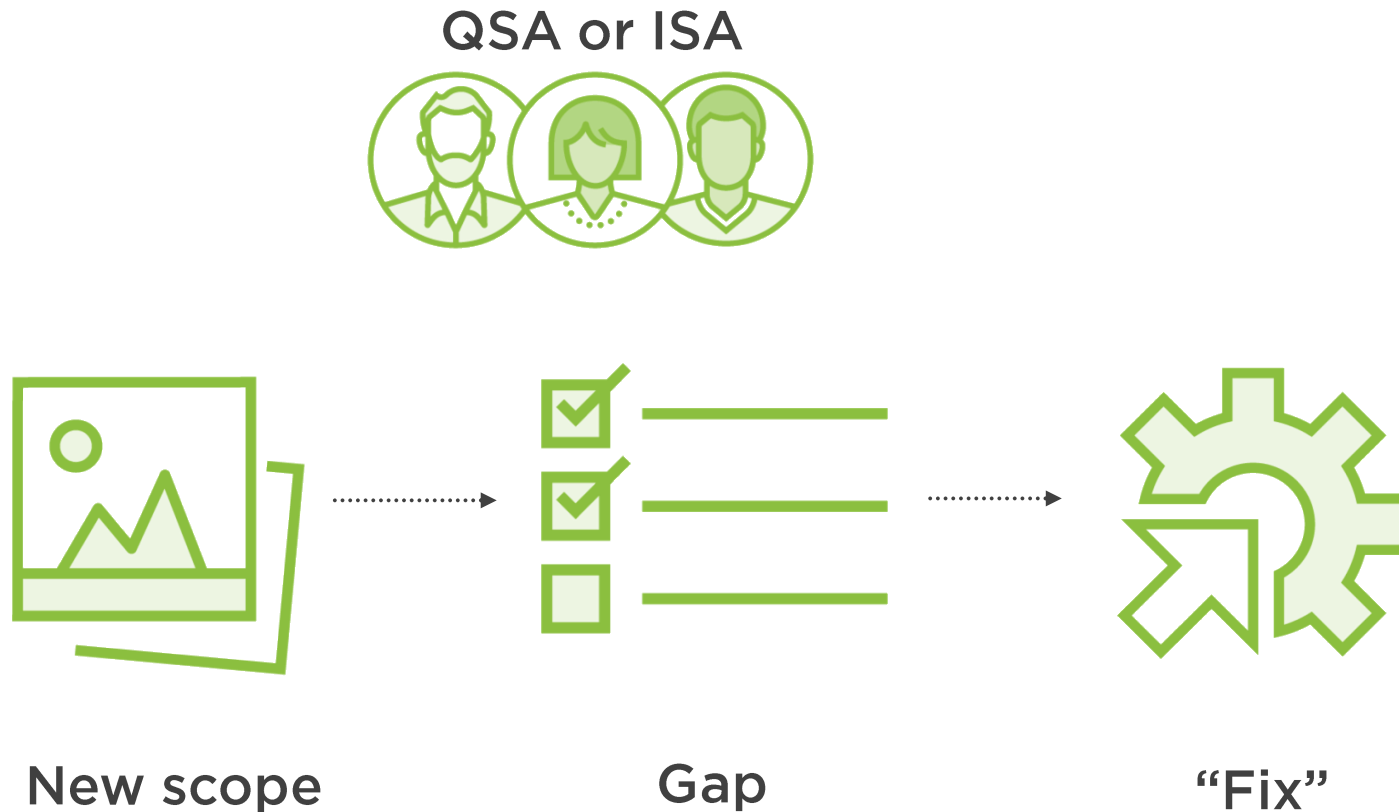
The hard work is here



Then one day ...



Remediation



You may not need this phase

Depends on:

How much PCI DSS?

How much change?

Could be the start of the real assessment



Scoping Matters

