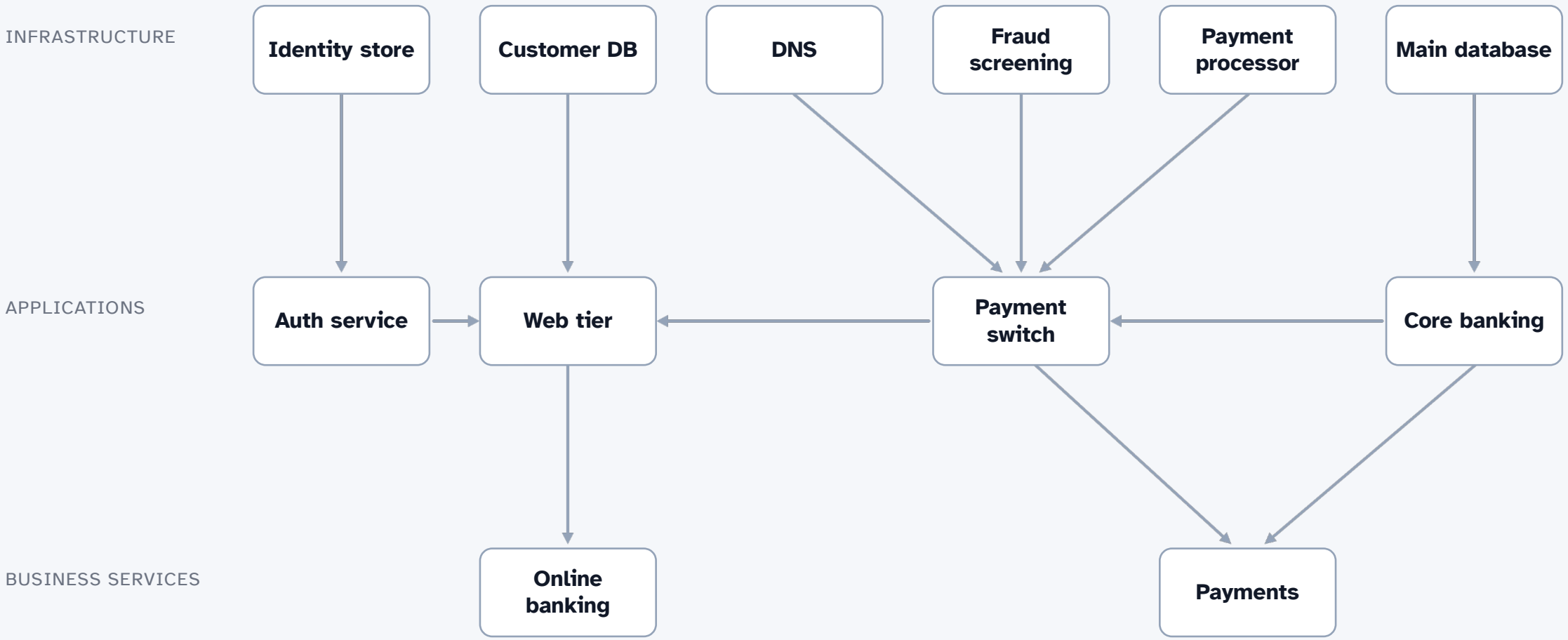
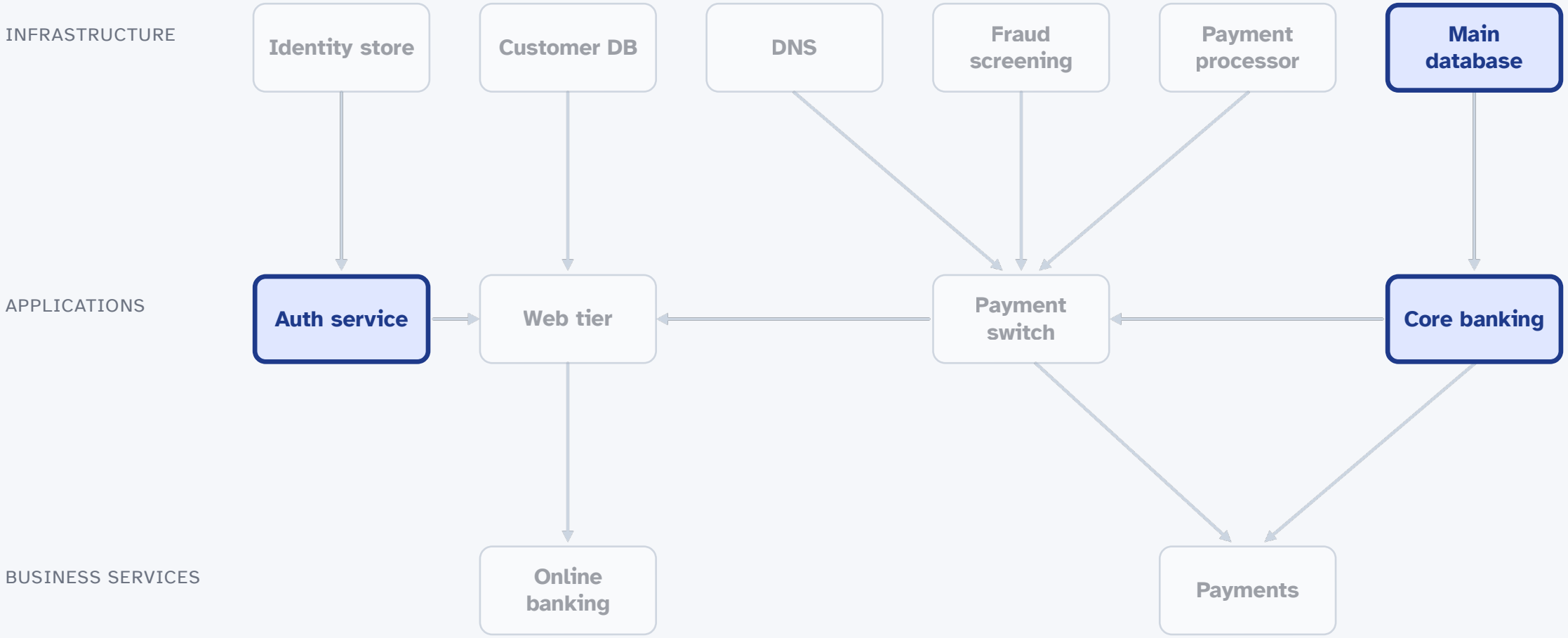
What Your Dependency Map Isn't Showing You

Denys Fiialko · DRI Canada Fall Symposium · Gatineau · November 12, 2026


INFRASTRUCTURE
Identity store
Customer DB
DNS
Fraud screening
Payment processor
Main database
APPLICATIONS
Auth service
Web tier
Payment switch
Core banking
BUSINESS SERVICES
Online banking
Payments



Which one would you take down for the biggest customer impact?

ROGERS · JULY 8, 2022

A configuration change.

Nationwide.

911 affected.

Source: CRTC, Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage (Xona Partners, July 2024)

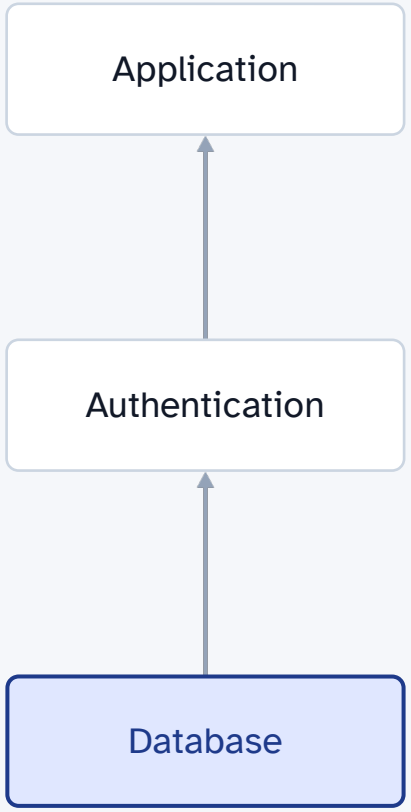
We normally ask: what does this system need to run day to day?

What will we need when this system is already broken?

The map isn't wrong.

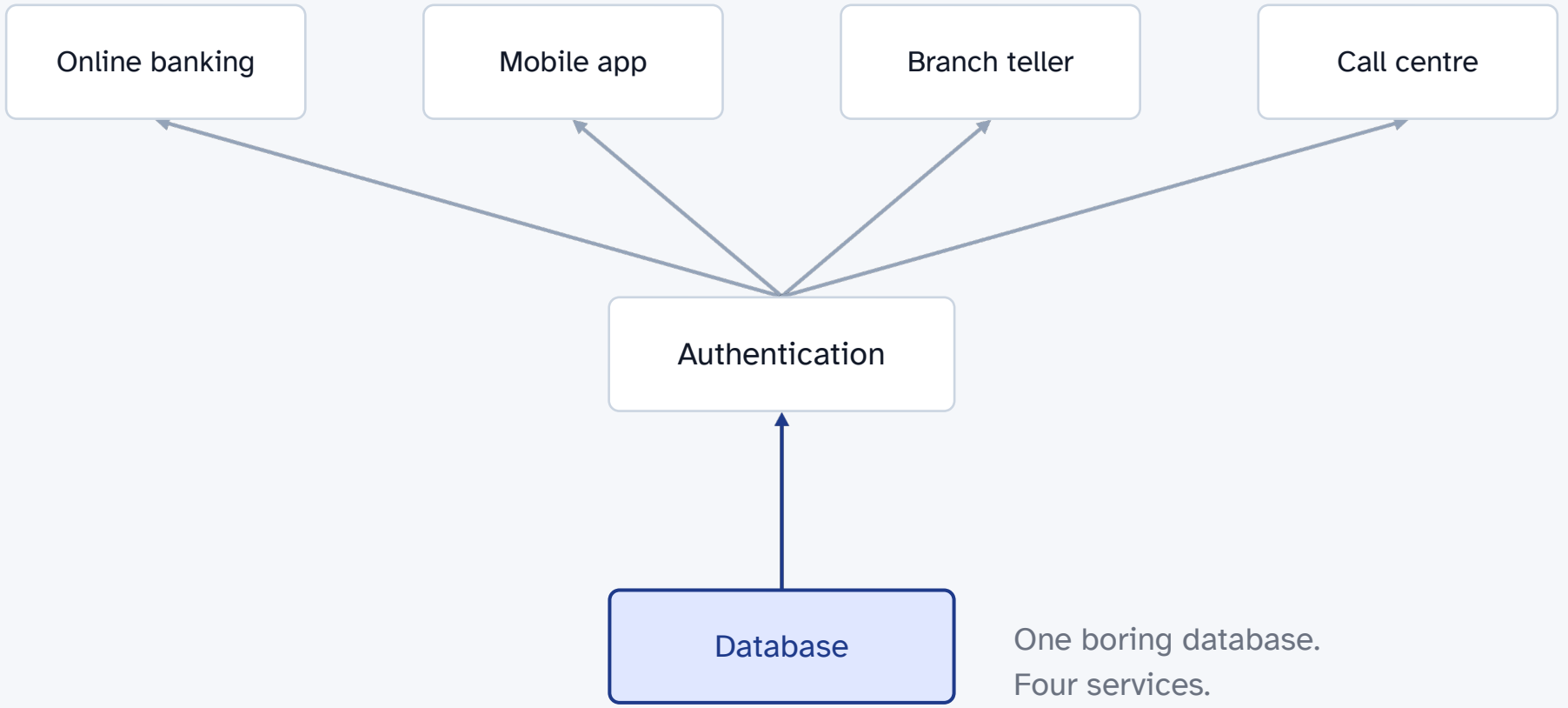
It stops too soon.

"We depend on authentication."



The application owner may not know this exists.
It's not their job to know.

Several applications. One authentication service.



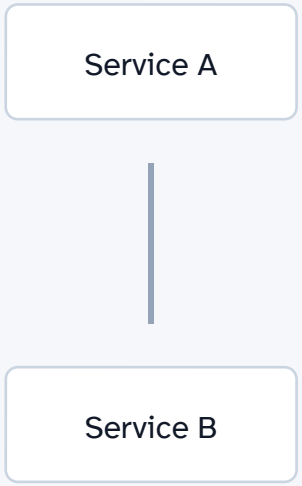
One boring database.
Four services.

> Failures don't care about the org chart.

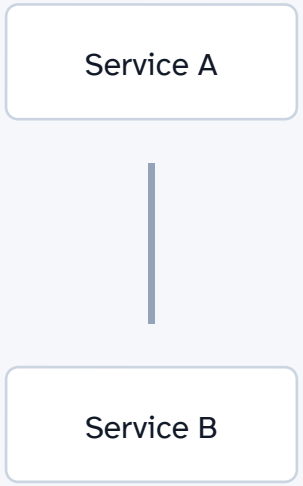
> We stop following the chain too early.

> A line says connected. It doesn't say how it breaks.

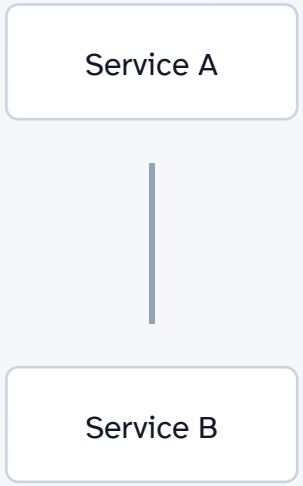
Three identical lines.



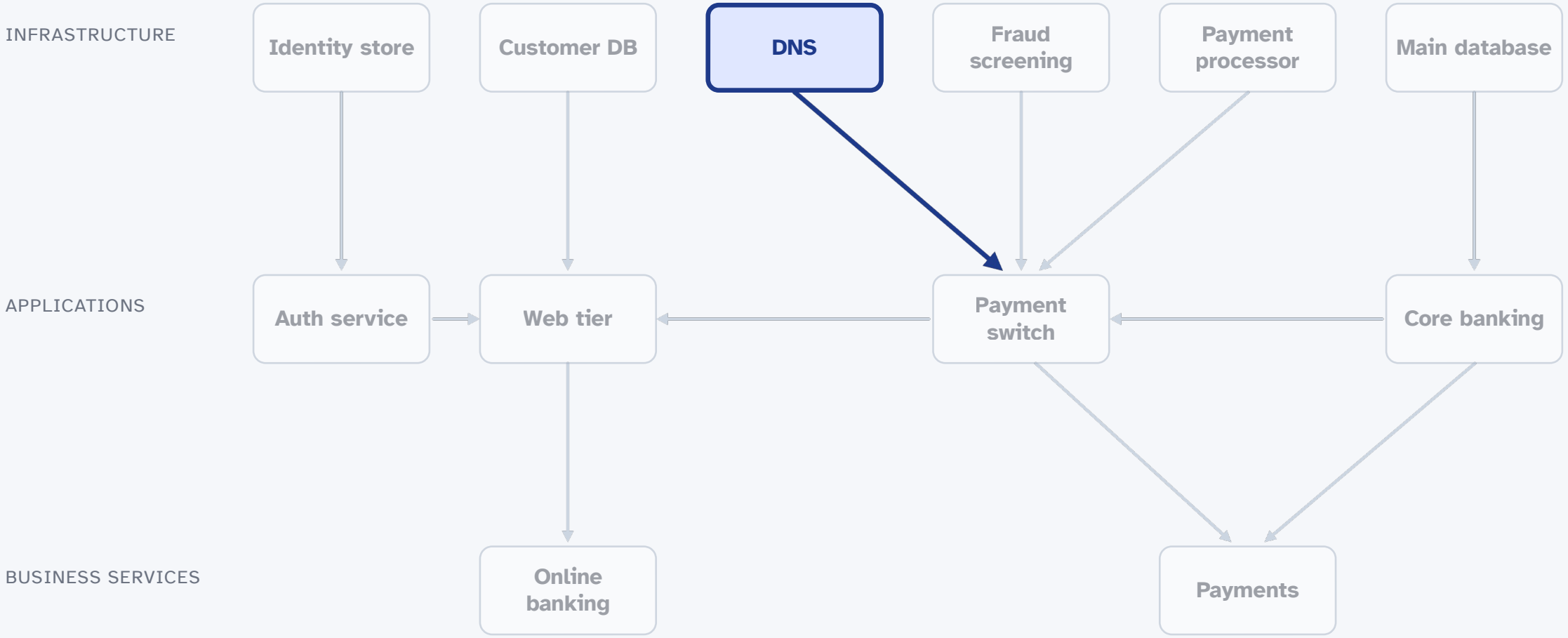
Fails immediately



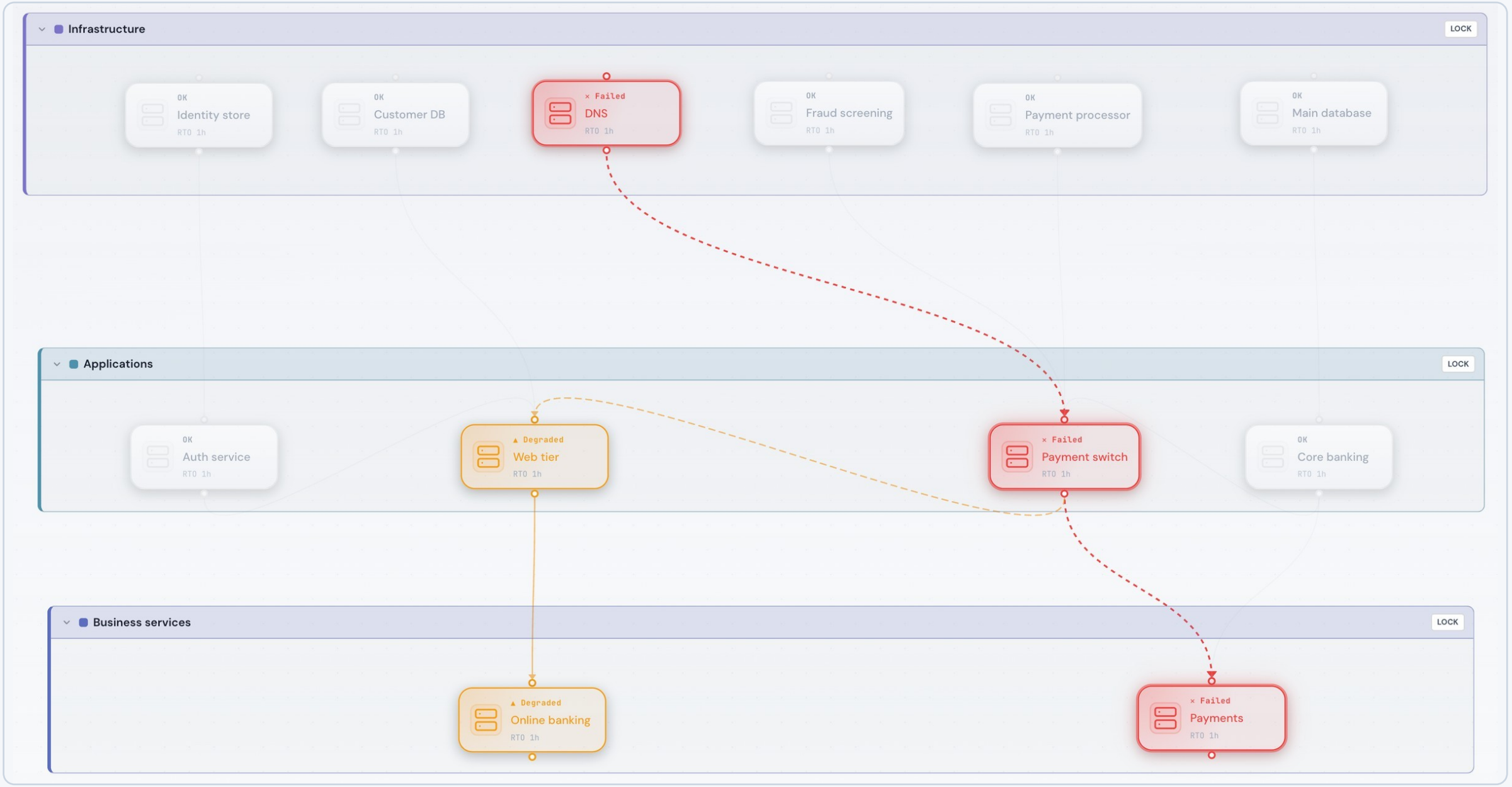
Keeps working for a while



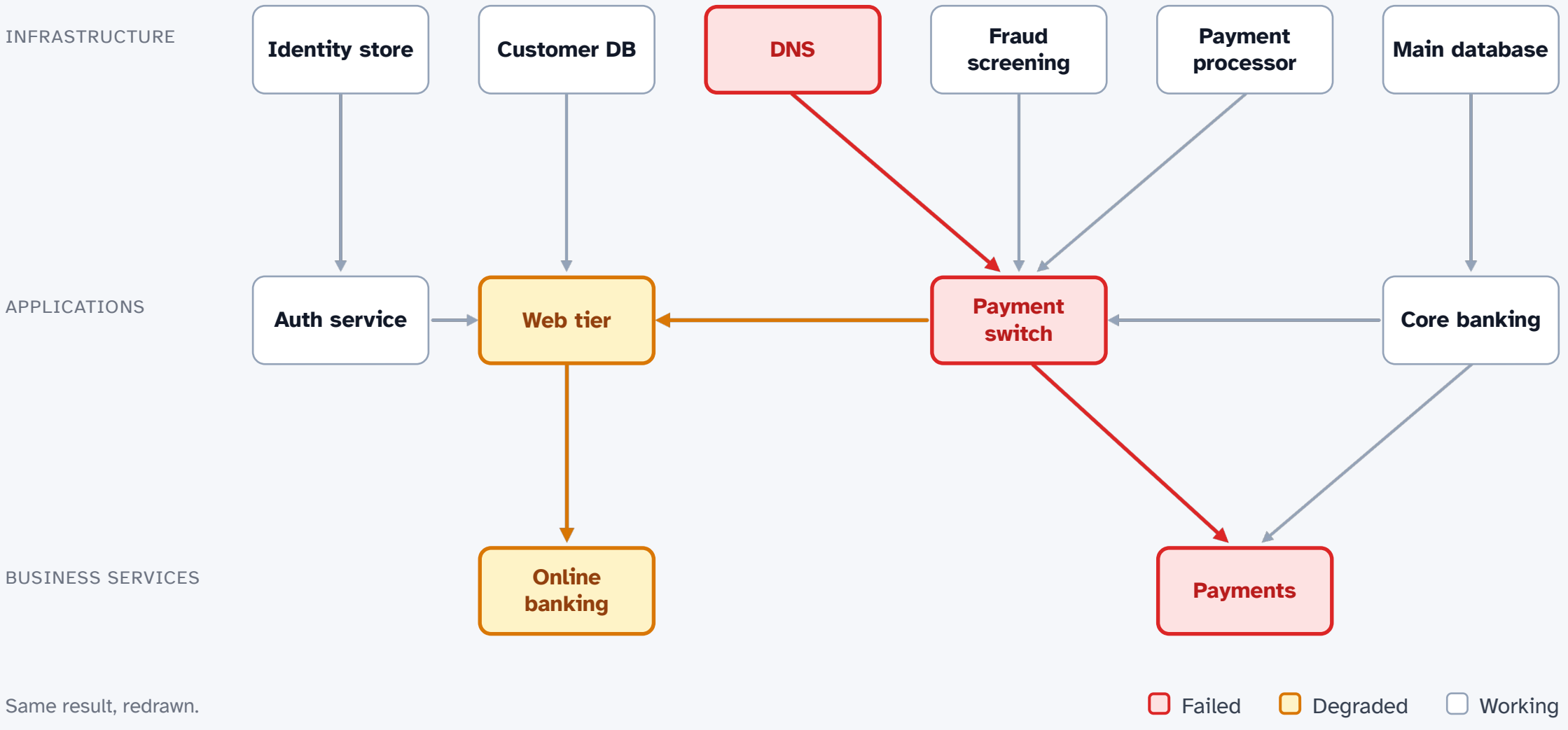
Loses one feature



DNS is how one system finds another. Boring infrastructure. Let's stop it.



Failcast, Oakridge stage model, DNS stopped.



Same result, redrawn.

What does it need to run?

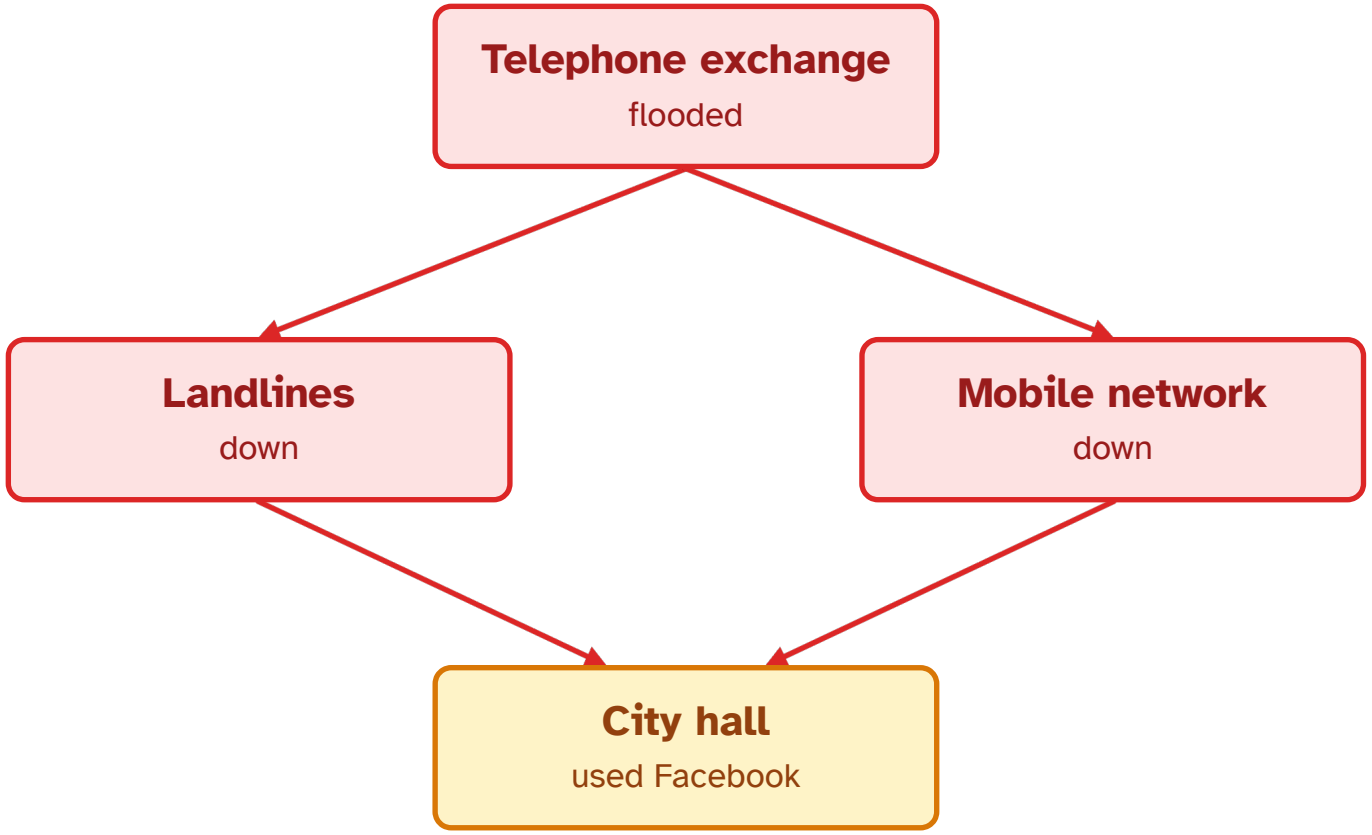
What happens if that disappears?

Is there another way to keep working?

Can the backup fail for the same reason as the primary?

PARMA · OCTOBER 2014 · FOUR PROVINCES AFFECTED

One flooded building. Both phone networks down.



Emergency radios
kept working

Never went through the exchange.

YOUR TURN

Your service. Three things. Two minutes.

TECHNOLOGY

One system the service cannot run without.

Payments: the payment switch.

PEOPLE

One person or team you would need.

Payments: the two on-call people who can fail it over.

RECOVERY

One thing you need to recover it during an outage.

Payments: the vendor portal where you tell the processor to hold transactions.

Don't overthink it. Just three things.

YOUR TURN

One question for each line.

YOUR LIST	YOUR PARTNER ASKS
TECHNOLOGY	What other service relies on that same technology?
PEOPLE	If that person or team is unavailable, who can step in?
RECOVERY	What has to be working for you to use that recovery tool during the outage?

“I don’t know” counts. Write down what you’d need to check.

YOUR TURN

Then keep asking: “And if that’s down too?”

YOU	My recovery tool is the vendor portal.
PARTNER	What has to be working for you to use it?
YOU	Our company login.
PARTNER	And if that’s down too?
YOU	Emergency accounts.
PARTNER	And if those are down too?
YOU	**I don’t know.**

Stop at “I don’t know.” Write it down. Then switch. Three minutes.

The BIA tells us what matters.

Simulation tests whether the system underneath can deliver it.

4 hours

is a target. It isn't evidence.

WORKING

Does what the customer needs, at the capacity the business planned for.

DEGRADED

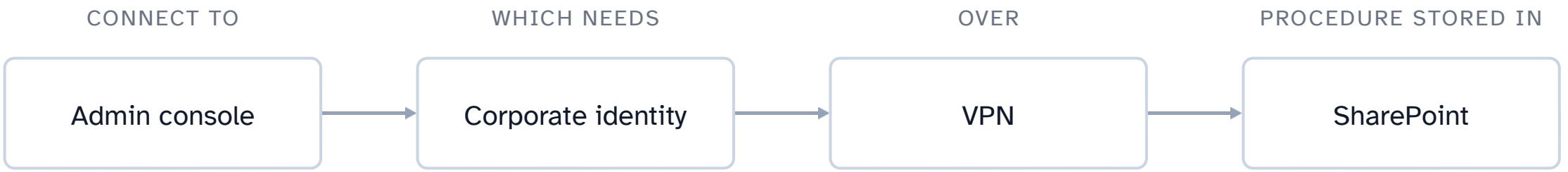
A contact centre open at thirty percent, or payments running with a control missing. Up on paper, not usable.

FAILED

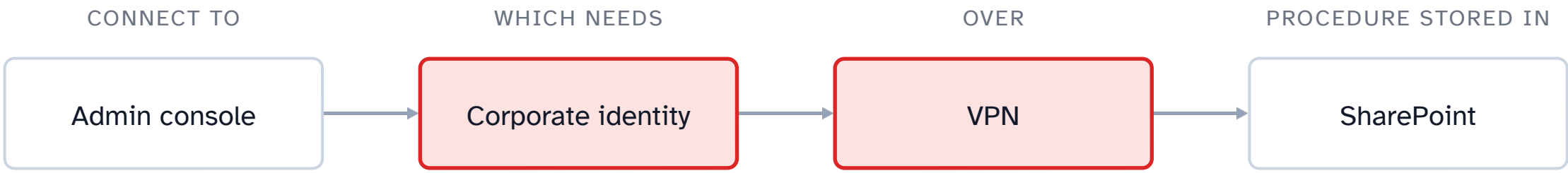
Nobody argues about this one.

Most of the interesting findings are in the middle one.

Authentication is down. Step one of the recovery plan: log in to the admin console.



Authentication is down. Step one of the recovery plan: log in to the admin console.



If the incident touches identity or the network, the recovery plan is down too.

How many of you have a recovery plan that needs your normal corporate login to open?

If one person's vacation changes your recovery time,

that person is on the map.

30 min

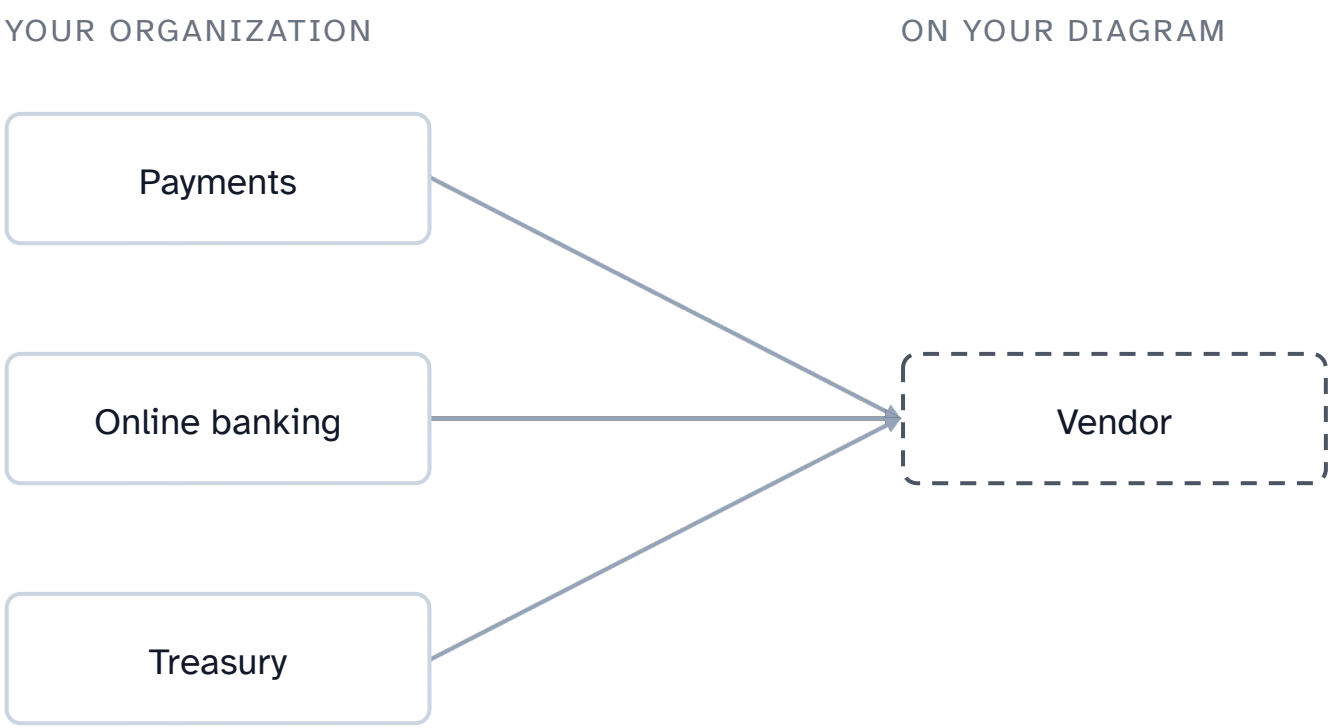
recovery when they're here

8 h

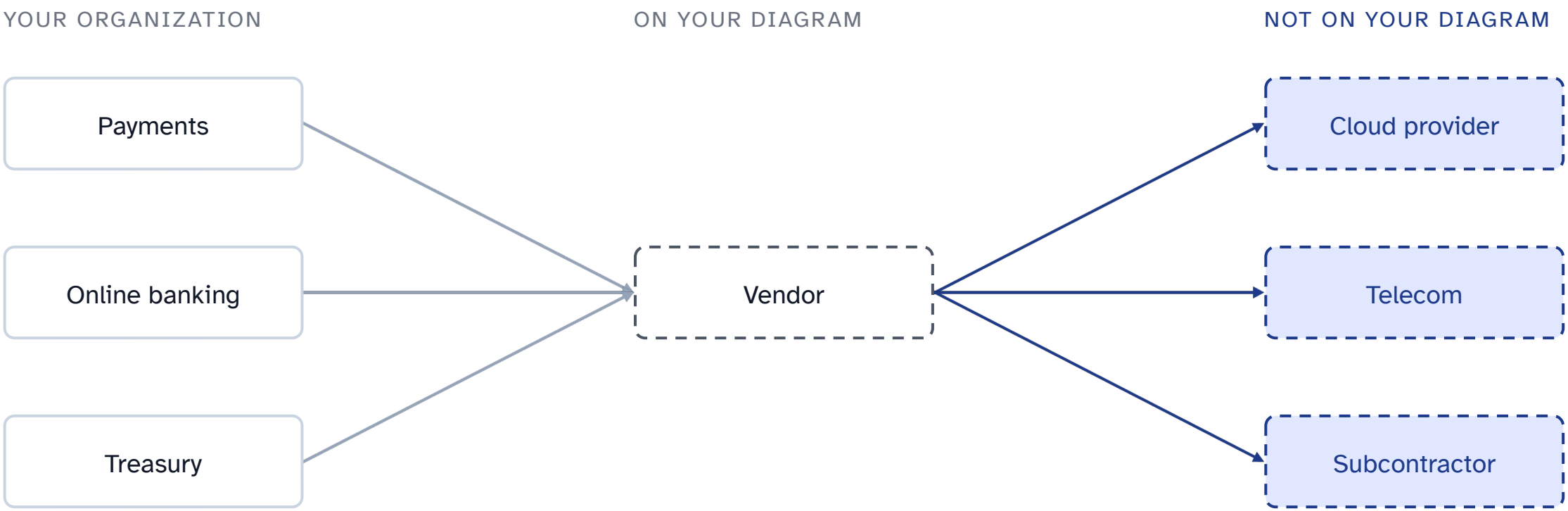
recovery when they're on vacation

Illustrative

The vendor doesn't stop at the edge of your diagram.



The vendor doesn't stop at the edge of your diagram.



Each BIA shows one manageable third party. Across the organization: concentration.

Most can name their providers. Very few can trace them.

1 in 4

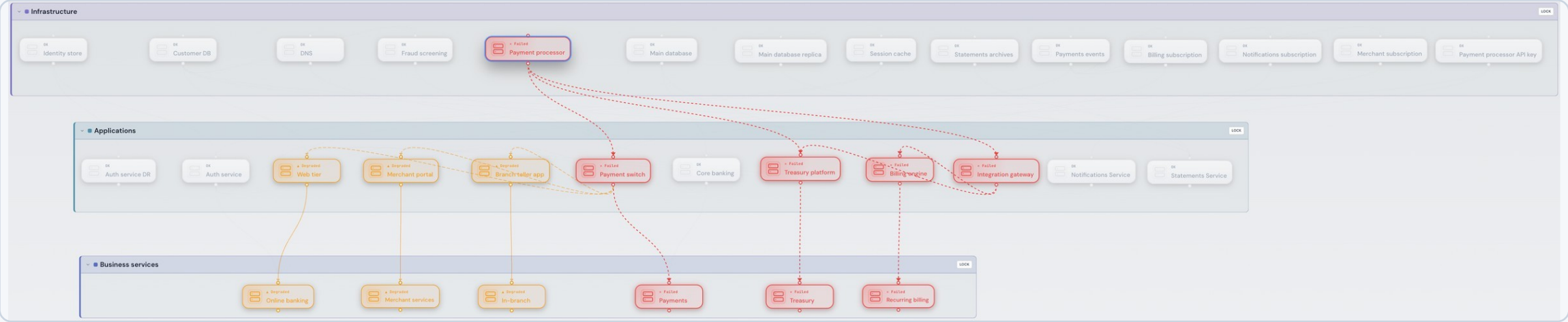
can trace fourth and fifth parties end to end, process by process.

30+

processes under a single provider, in one bank. Nobody owned that view.

Source: McKinsey & Company, Inside the Strategy Room, September 2026. Figures approximate, as stated on the podcast.

Fail the payment processor. Six business services. Four critical.



FAILED **Payments**

Critical

FAILED **Treasury**

Critical · via Integration gateway

FAILED **Recurring billing**

via Integration gateway

DEGRADED **Online banking**

Critical

DEGRADED **In-branch**

Critical

DEGRADED **Merchant services**

Standard

The vendor register lists two. **Two paths run through a gateway nobody declared.**

Failcast, Oakridge full model

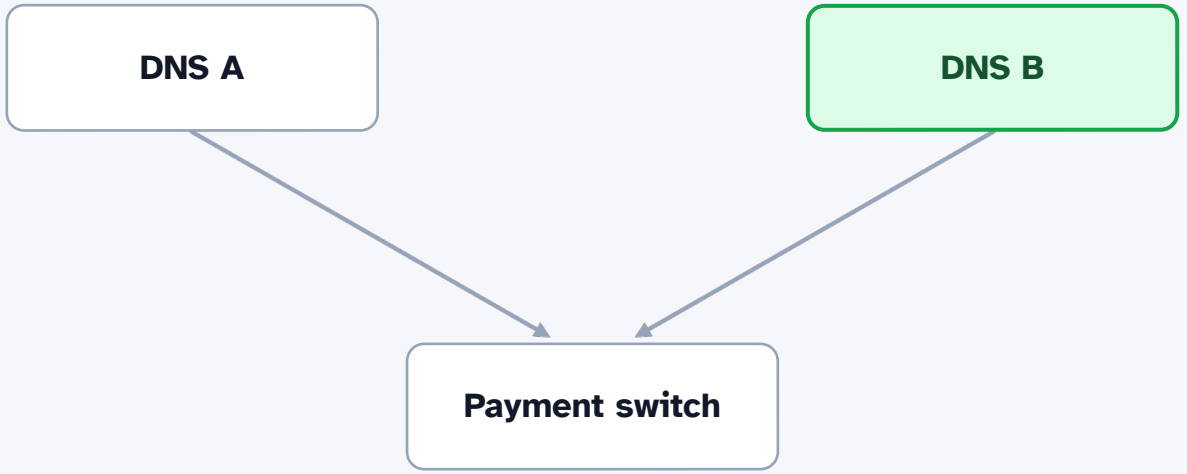
Guideline E-21 expects you to understand your critical operations end to end,

and to test severe but plausible failures, not just document them.

OSFI Guideline E-21, Operational Risk Management and Resilience: Principle 6 (map internal and external dependencies) and Principle 8 (severe-but-plausible scenario testing)

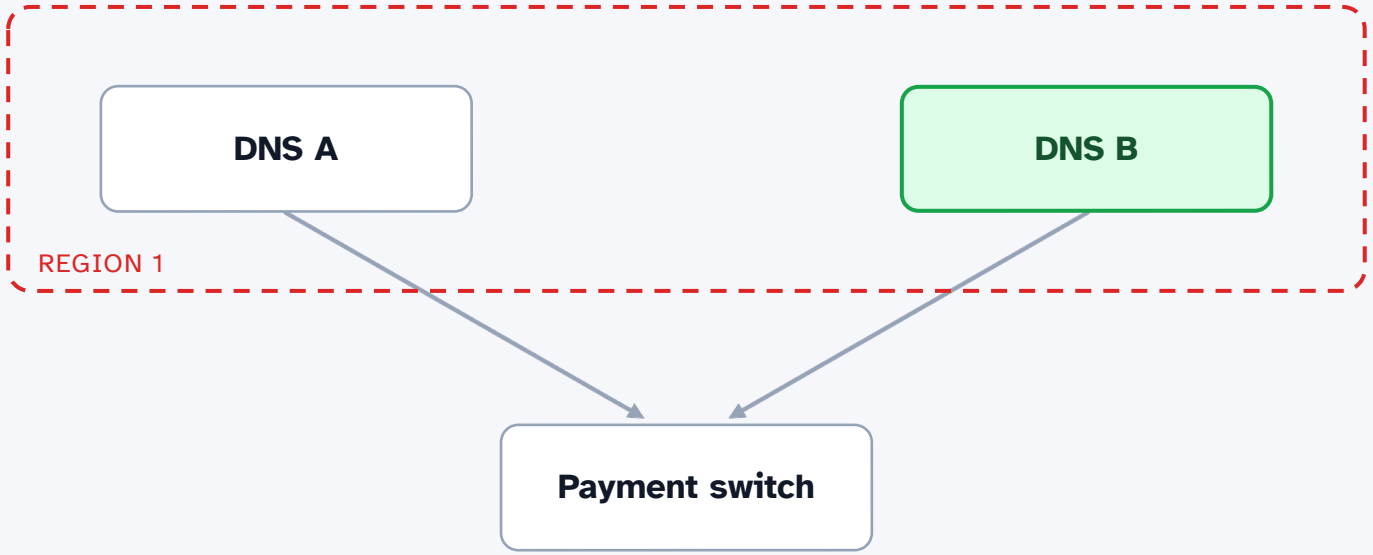
DNS took the customer. So Oakridge adds a second DNS.

Are we safe now?

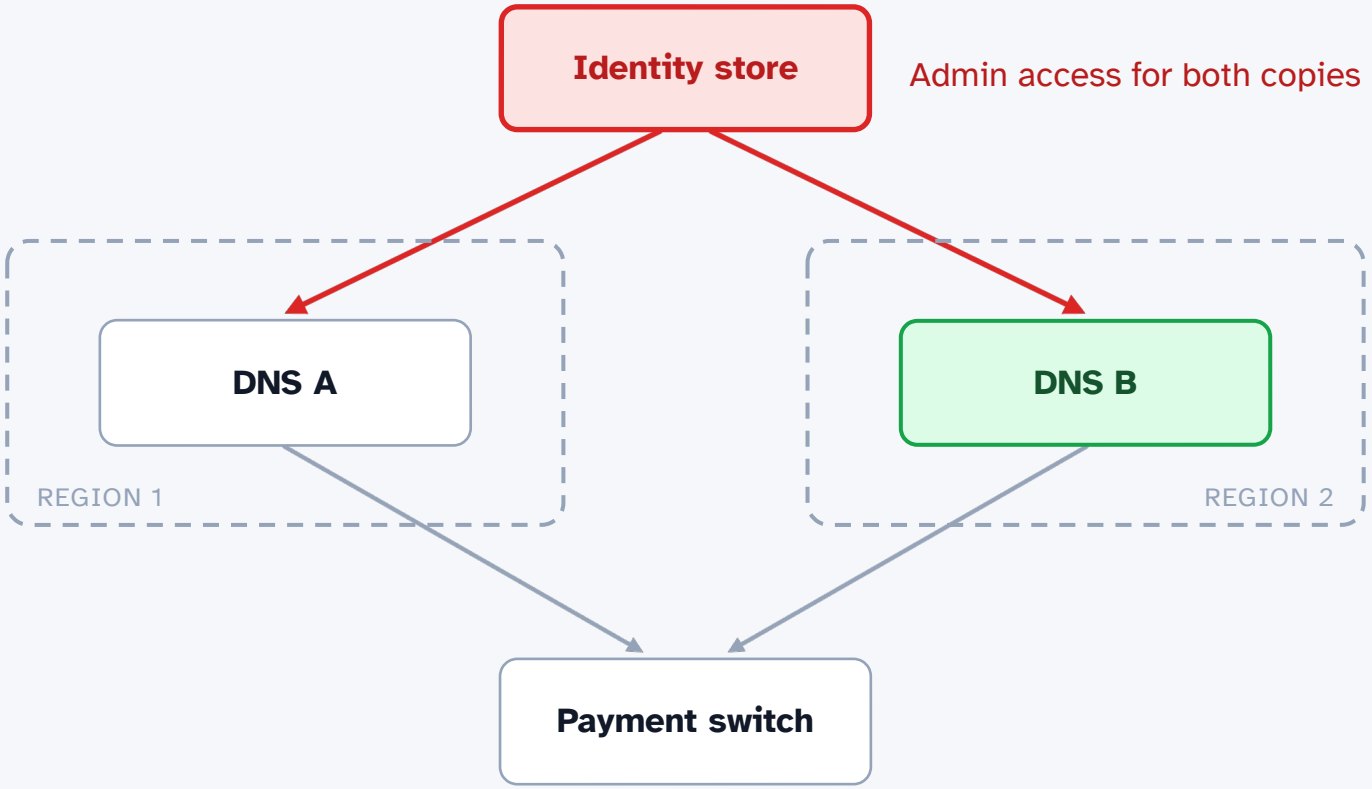


Both copies are running in the same region.

Covered if one server fails. Not if the region does.



Both keep answering. Nobody can log in to fix them.



PART THREE · KEEPING THE MAP TRUE

A dependency map is a hypothesis.

Every incident, exercise and major change is a test of it.

"Even if we build this whole model,

six months from now it'll be out of date."

A quarterly reminder is the wrong tool for something that changes every week.

DON'T MAINTAIN THE MAP.

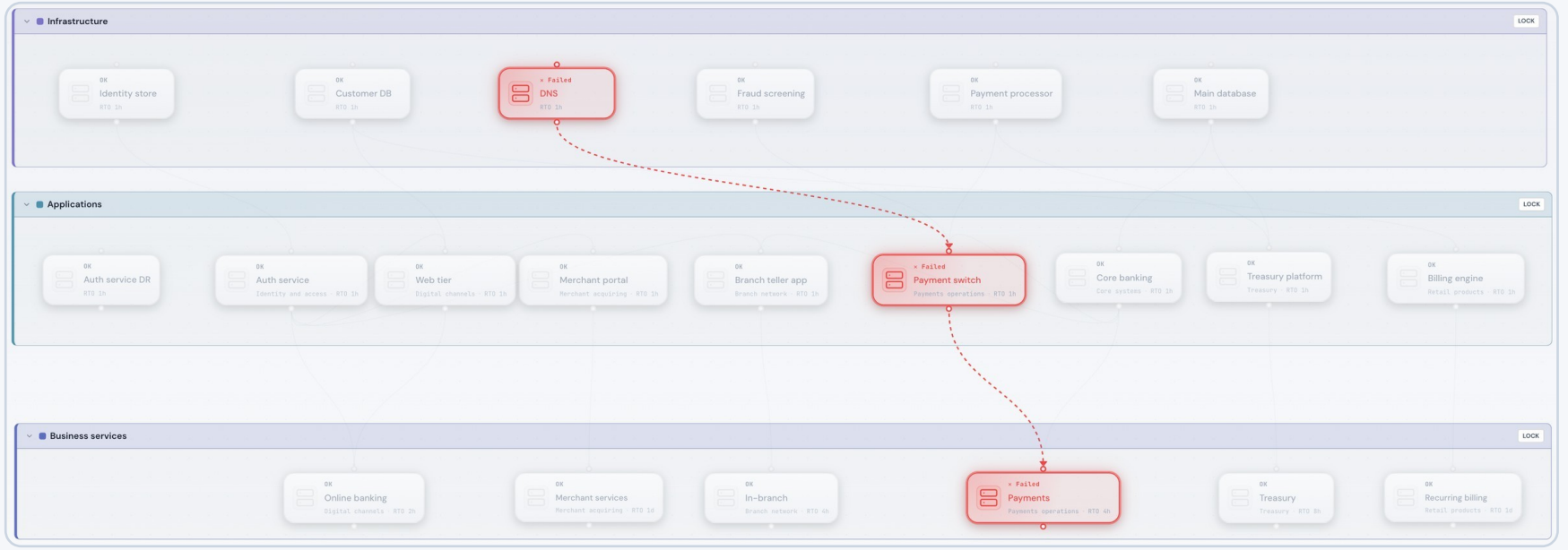
MAINTAIN THE CHANGES.

Put the review inside change management, vendor onboarding and incident review.

WHAT THE CMDB DECLARES

3 failed or degraded

1 business service



CMDB PLUS INFRASTRUCTURE CONFIG

9 failed or degraded

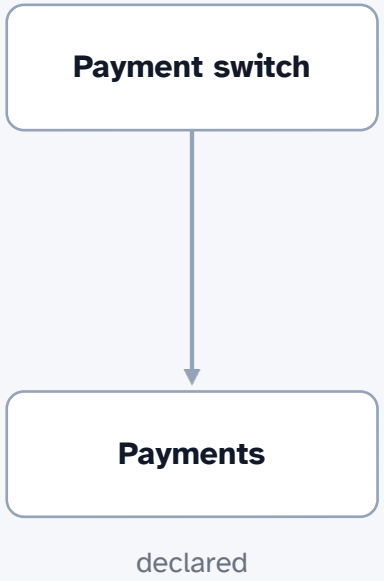
4 business services



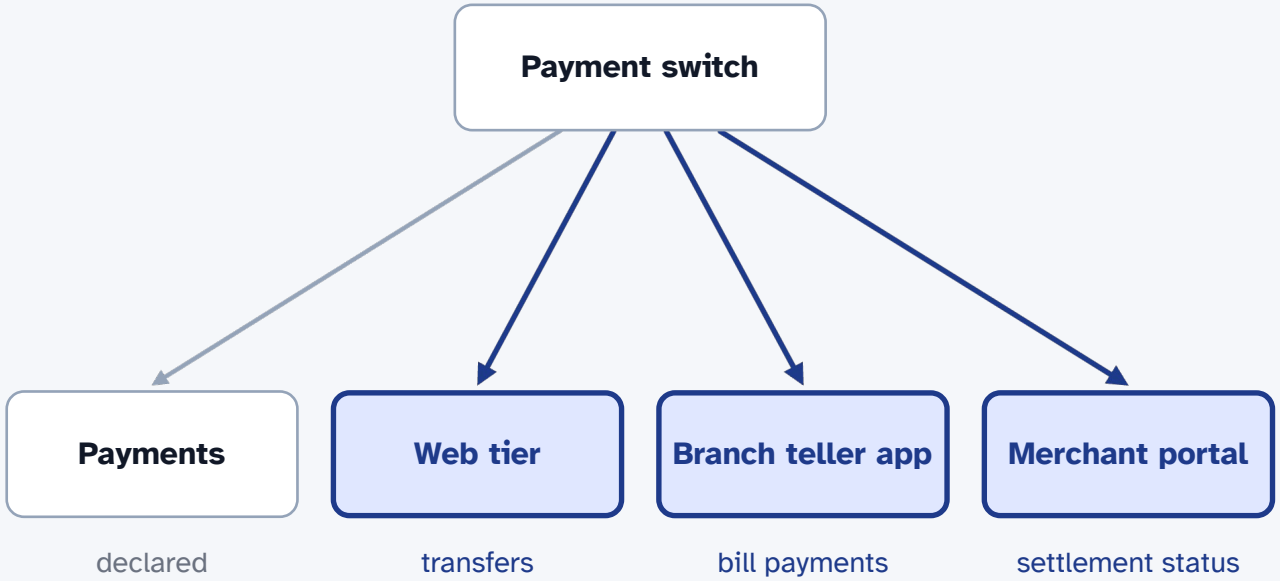
Failcast, Oakridge, same DNS failure on both. Counts as Failcast reports them, DNS included.

Where the gap comes from: one box.

CMDB: ONE CONSUMER

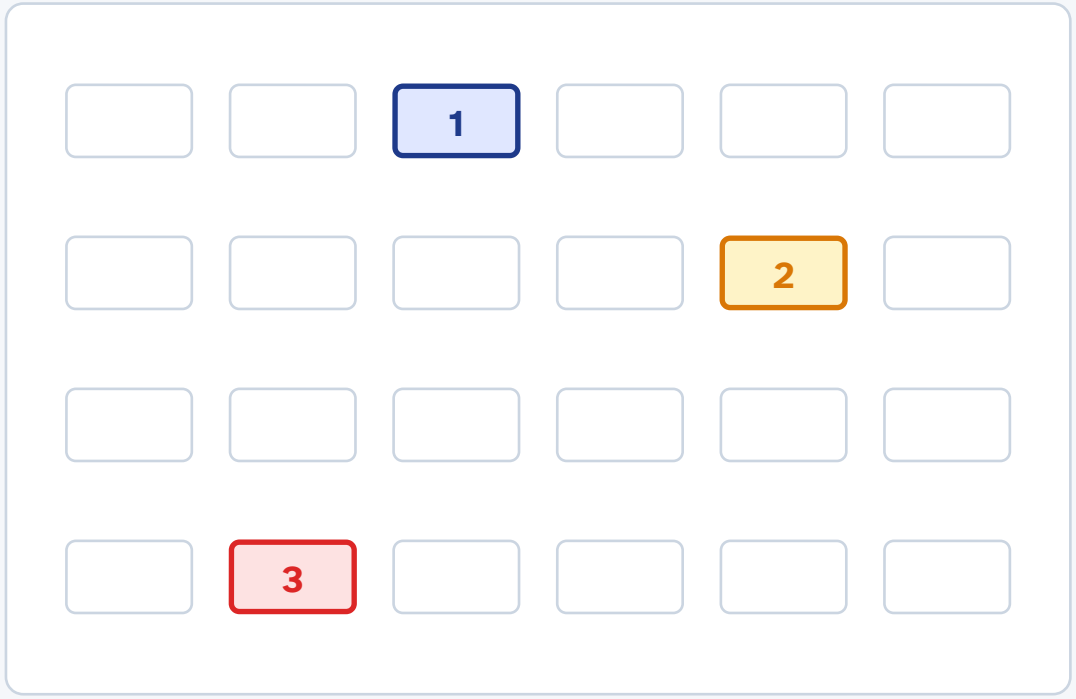


INFRASTRUCTURE CONFIG: FOUR CONSUMERS



The teller line went in in March. The change was approved. The map was never updated.

Every relationship says how we know it.



1 Observed last week, in the cloud configuration.

2 Confirmed by its owner. June.

3 Copied from a diagram in 2024. Nobody has looked since.

Should we trust those three equally?

Some call this a digital twin.

No bank has built one yet.

Their own advice for starting: one well-understood process, bottom up, with what you already have.

On Monday

1. Pick one critical business service.
2. Ninety minutes with its architect and the ops person who gets paged.
3. Trace what's under it: technology, people, third parties, recovery tools.
4. Break one component. What fails? What degrades? Can the backup carry it?
5. Compare with the RTO in your BIA. Where they disagree, you have a finding.

One service. One failure walkthrough. One afternoon.

If one core dependency went down, could you trace what happens two or three steps further?

Could you name the shared component under it with the biggest blast radius?

Do you know when those links were last checked against reality?

1. The map isn't wrong. It stops too soon.
2. Your BIA tells you what matters. Test the assumptions underneath it.
3. Don't maintain the map. Maintain the changes.

DON'T JUST MAP IT.

BREAK IT.

1. The map isn't wrong. It stops too soon.
2. Your BIA tells you what matters. Test the assumptions underneath it.
3. Don't maintain the map. Maintain the changes.

Worksheet and slides

failcast.io/dri

DON'T JUST MAP IT. BREAK IT.

Denys Fiialko

denys@failcast.io