

WWRF HUDDLE 2026 · SESSION 3

Many Disciplines, *One Trust Framework*

Technical controls, real context, meaningful accountability

Bilge Baykurt

Security Governance Manager, Paycell

THE CORE CHALLENGE

Same system. Different conclusions.

SECURITY

“The control worked.”

LEGAL

“What does that mean
for our obligation?”

RISK

“What is still
uncertain?”

BUSINESS

“Can we actually use
it?”

CUSTOMER

“Did it work for me?”

The **secret sauce** is a common language—with standards kept alive by culture, training and awareness, and the right metrics.

With the right metrics in place, everyone should understand what the evidence shows and doesn't show, what we still don't know, and what we can actually decide

A WRONG METRIC

Measuring activity is not measuring outcome.

WHAT THE TEST SHOWS

```
test: human_escalation  
status: PASS  
"Request for human support created."
```

Metric: *a request was created.*

WHAT ACCOUNTABILITY ASKS

- Did it escalate when it should have — or only when asked?
- Did the request reach the right person?
- Did they have enough information?
- Did they have time and authority to intervene?
- **Was the customer's problem solved?**

A better metric: *did the customer reach a person who could help — and was the problem solved? A metric should follow the process to the end — not only the system*

FROM ADVICE TO ACTION

Authorization is not trust.

“I recommend this action.”



“I have taken this action.”

✓ AUTHENTICATED

✓ AUTHORISED

✗ STILL WRONG

Context before measurement — this is how we choose the metric.

What is it doing · who is affected · what authority · what it depends on · what if wrong

The level of assurance follows the impact of the action.

BY DESIGN · BUILT IN, NOT ADDED

Architecture is a governance decision.

Each choice changes what you can control, observe and verify.

OWN MODEL

YOU CONTROL

Data, training, every change.

YOU CAN SEE

Everything — if you build the logging.

STILL YOURS

No one else checks your work. Build the evidence yourself.

OPEN MODEL

YOU CONTROL

How you run it — not how it was trained.

YOU CAN SEE

Its behaviour — not its origins.

STILL YOURS

Verify what you adopt. Own how you use it.

THIRD-PARTY PLATFORM

YOU CONTROL

The contract and the configuration.

YOU CAN SEE

Inputs and outputs — not everything in between.

STILL YOURS

Where data goes. What the provider can change.

You can outsource capabilities. **You cannot outsource accountability.**

Reassess on meaningful change — the model, the data, a dependency, the people affected, the agent's authority — not when a date appears. ***Do not monitor everything. Know what matters.***

BY DESIGN · PEOPLE OUTSIDE THE ROOM

Know who uses the service. *Design protection for them.*



CHILDREN



OLDER PEOPLE



LIMITED DIGITAL SKILLS



LANGUAGE BARRIER

Each of them needs different processes and different features.

PLANNED FROM THE START — EVERY STEP



PRODUCT DESIGN



SECURITY MEASURES



COMMUNICATION



AWARENESS

*Like privacy by design: **decide it at the very start** — not after launch.*

WHAT WOULD HELP THE WHOLE SECTOR

A sectoral view.

TODAY

01

No comprehensive AI regulation yet. The sector is careful — and looks to international good practice for reference.

AHEAD

02

As the rules become clear, adoption will grow. And — as in the EU — I believe sandboxes will follow, where the sector can test together, under the authority.

*One trust framework does not mean one opinion. **It means one language — shared across the sector.***

Thank you.

After the benchmarks, the controls, the standards and the approvals — one question remains.

Did it produce a better outcome for the person affected?

Bilge Baykurt

Security Governance Manager, Paycell