

Thank You for Your Data

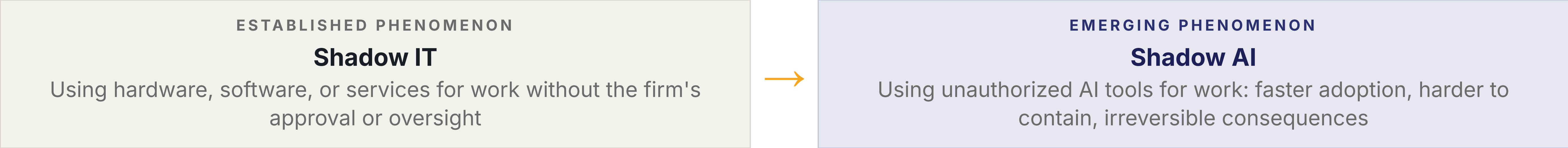
When and why employees use unauthorized AI tools in the workplace

Michael Mertel & Manuel Zall

Friedrich-Alexander-University Erlangen-Nuremberg · michael.mertel@fau.de | Julius-Maximilians-University Würzburg · manuel.zall@uni-wuerzburg.de



Motivation — The Rise of Shadow AI



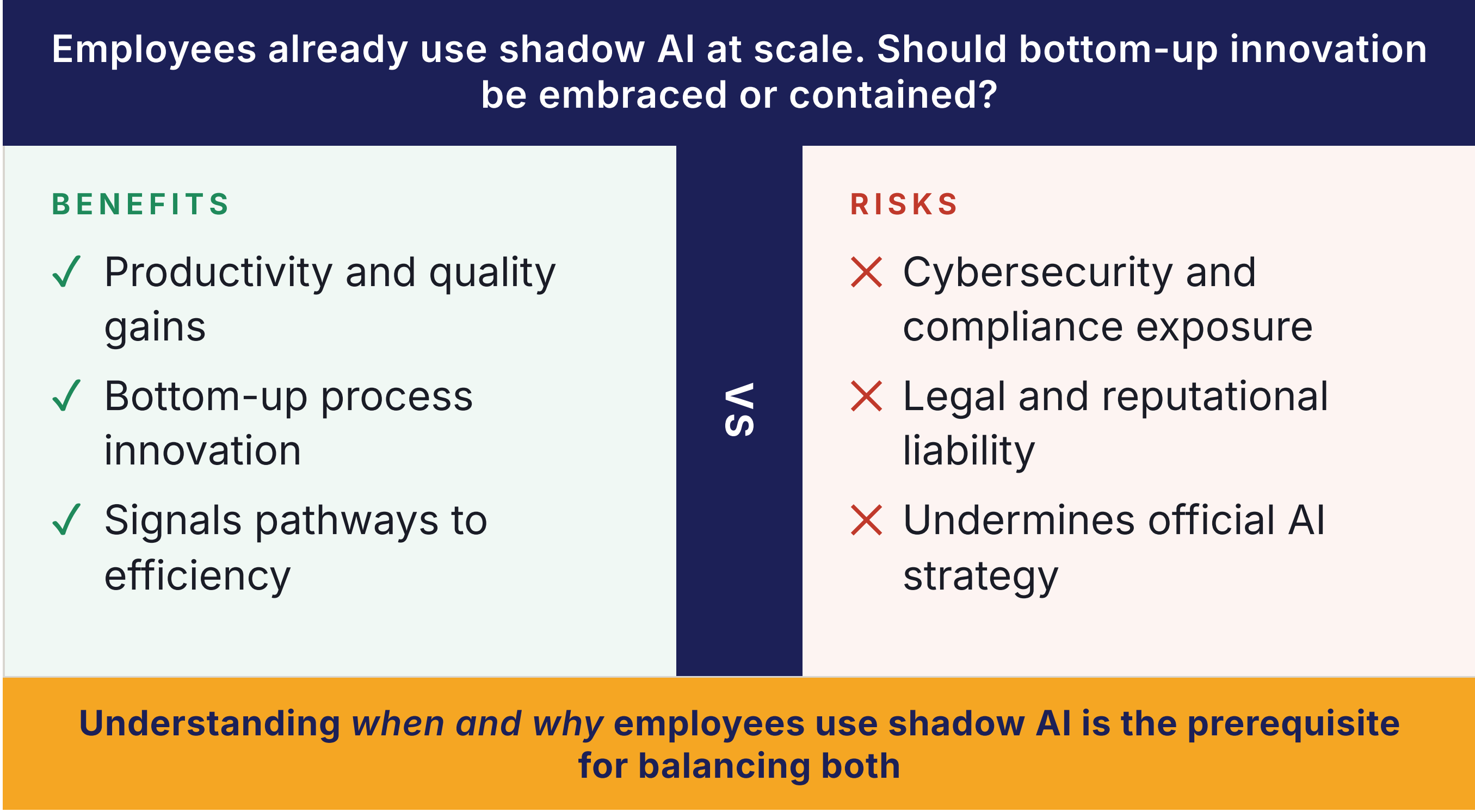
Shadow AI: the unauthorized use of AI tools by employees to perform work-related tasks outside a firm's approved IT stack, policies, security protocols, and compliance.

EXAMPLE An employee pastes customer records into ChatGPT to draft a report: already a GDPR violation, as personal data is sent to a third party without consent.

WHY SHADOW AI CONSEQUENCES ARE MORE SEVERE

- 1 Irreversible data ingestion. Data entered into public AI is ingested into external models, a process that cannot be reversed.
- 2 **Inscrutable outputs.** LLMs hallucinate and produce plausible-but-false content, silently corrupting decisions.
- 3 **Widespread unmonitored adoption.** Industry reports indicate that 71–90% of employees already use unauthorized AI tools for work.

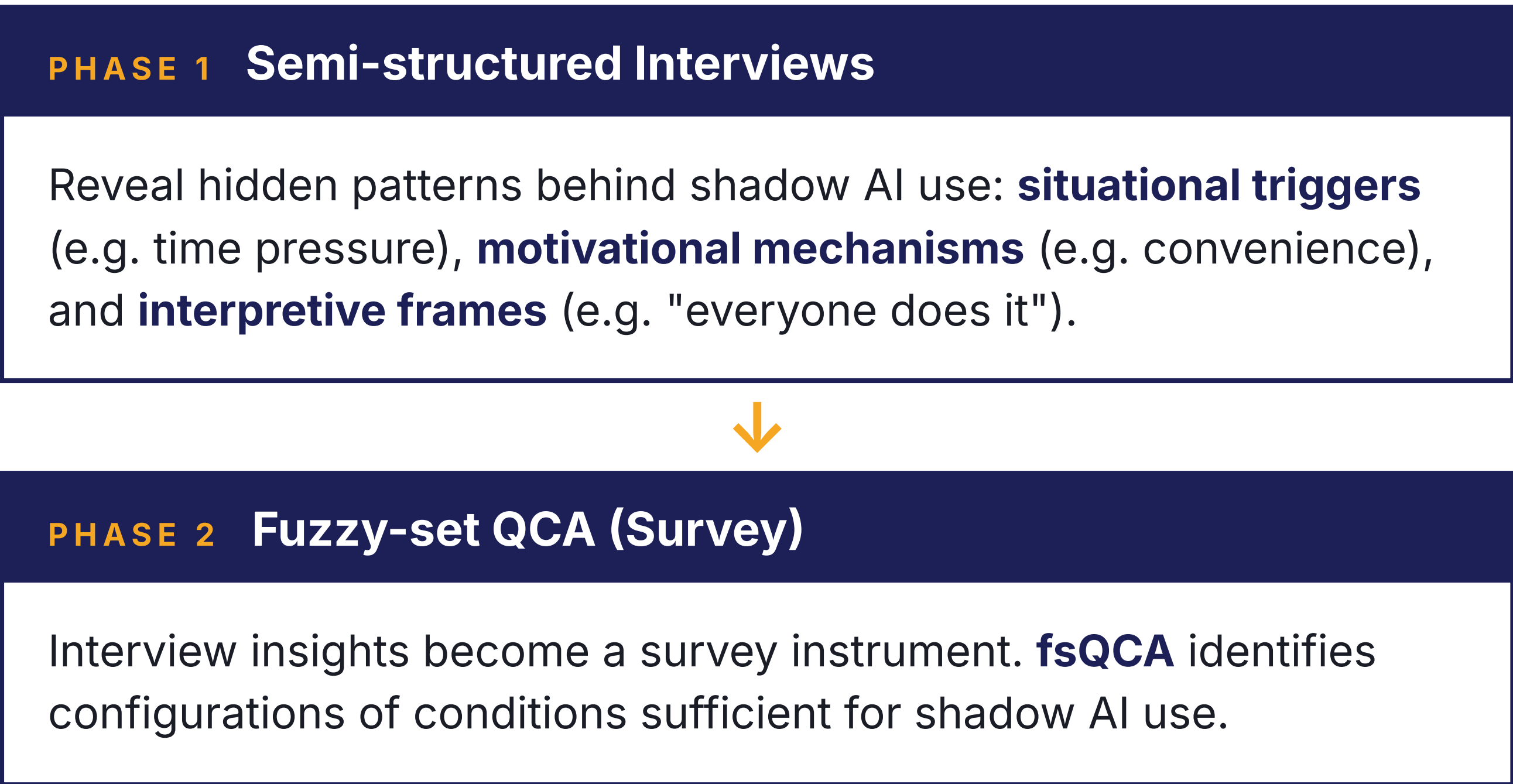
THE ORGANIZATIONAL DILEMMA



02 Approach

RESEARCH QUESTION
Which combinations of influencing factors lead employees to use unauthorized AI tools at work?

We adopt the **theory of workarounds** (Alter, 2014) — deliberate adaptations that bypass obstacles in a work system. They can seed bottom-up innovation yet also increase risk, making them a central mechanism of shadow AI.



Equifinality	Conjunctural	Asymmetry
Multiple pathways to the same outcome	Factors combine in specific configurations	Causes of use ≠ inverse of non-use

03 Outlook & Open Questions

These questions are a **starting point for the roundtable discussion** — we welcome any further directions and feedback.

- Q1

Sampling. Criterion-based purposive sampling across organizations, or a case-based design with richer context?
- Q2

Social desirability. How do we minimize under-reporting of policy misconduct in interviews?
- Q3

Quantitative angle. Which approaches — survey, trace data, network/API logs — best capture the phenomenon?
- Q4

Theoretical lens. Beyond workaround theory and sensemaking, which perspectives help theorize shadow AI?
- Q5

Study architecture. Retain the sequential multi-method design, or split into standalone papers?
- Q6

Policy design. How could a paper on effective, safe AI policy be conceptualized?
- Q7

Intervention design. How could an intervention study (method, setting, experiment) be conceptualized?