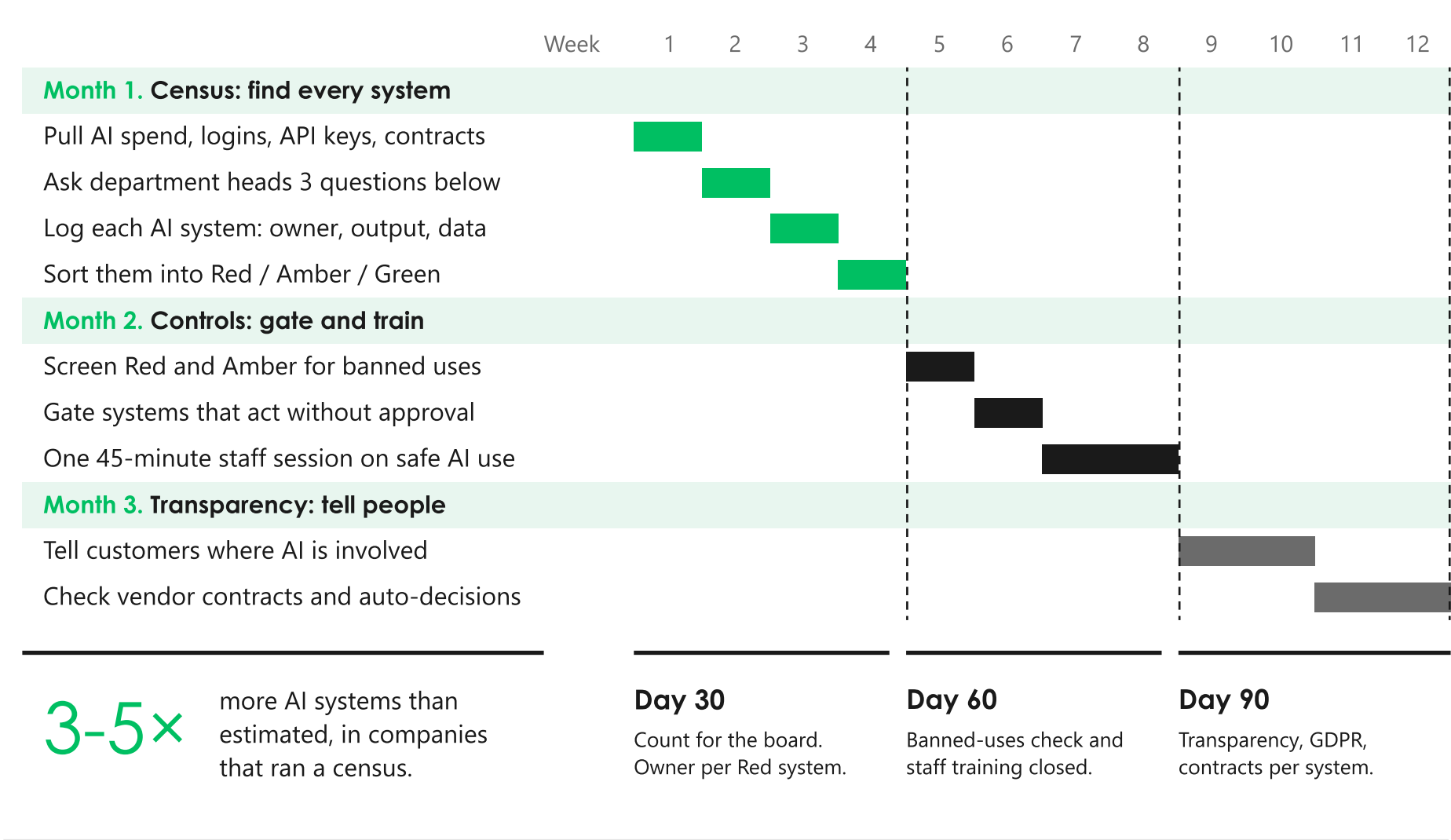


Know every AI system you run.

The 90-day plan from the webinar. One person, part-time.
You are not auditing anyone: say that first, every time you ask a question.

The plan, week by week

Want help running it? We'll set up the census with you. engagement@edvantis.com



Three questions for department heads

Don't use the word "AI" until they do.

1

Where does software shape a decision or a deliverable someone relies on?

2

What happens to that output:

- a person checks it,
- it goes to a customer,
- or the system acts on it?

3

What got noticeably faster or cheaper here in the last two years, and why?

Sort every AI system into a tier

Red

Affects a person's life outcome, or acts on production, money or customers without approval. Gets a named owner.

Amber

Touches personal data, or its output reaches a customer, or it acts, with a human approving.

Green

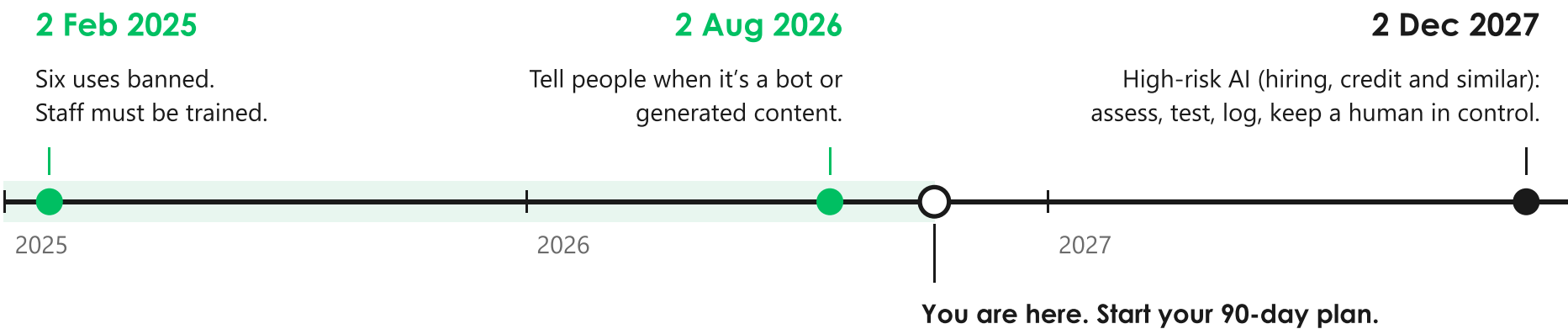
Internal, no personal data, a human checks everything.

The highest-risk system is usually one nobody bought as AI. It arrived as a feature in a tool you already had.

Two of three EU AI Act deadlines are already behind you.

The EU regulates before a system ships. The US applies existing law after the harm.

EU AI Act on the calendar The EU AI Act reaches you without an EU entity: if your AI’s output reaches EU users, it applies.

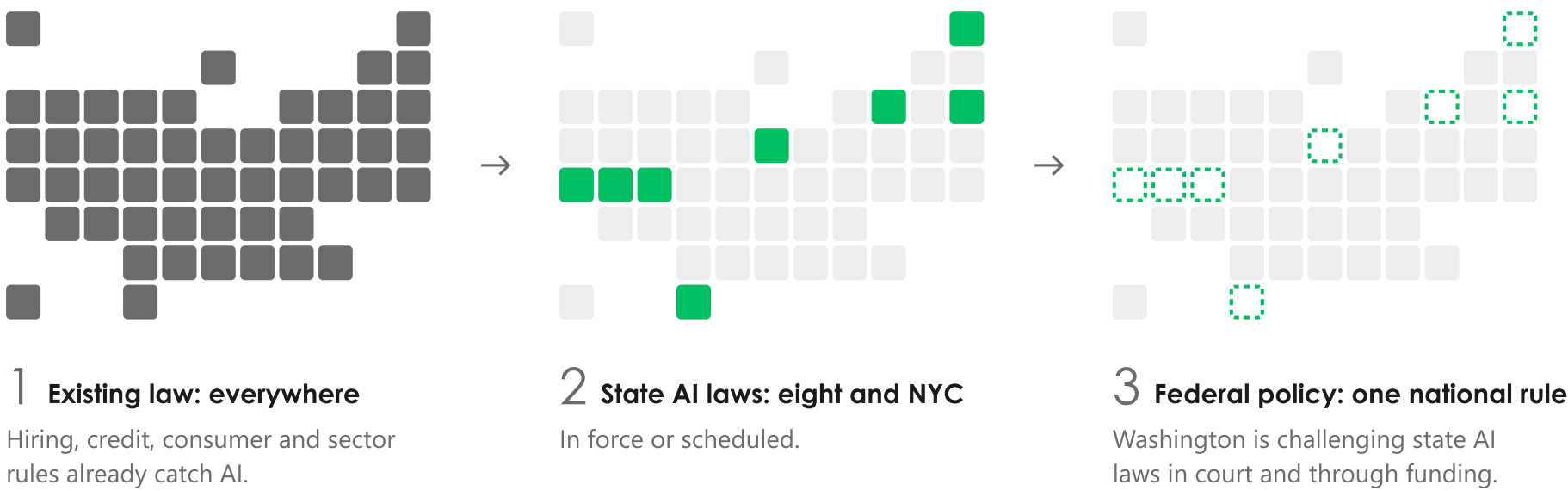


The six banned uses Check every Red and Amber system against this list. Keep the dated record of the check.

- ❌ Social scoring
- ❌ Manipulative or exploitative techniques
- ❌ Emotion recognition at work or in education
- ❌ Untargeted face-image scraping
- ❌ Biometric sorting by protected traits
- ❌ Predictive policing of individuals

7% of global turnover: the penalty ceiling for a banned practice.

United States: three layers, left to right



Most of this isn't new. It's the same controls you'd demand of any part of the business that can act on its own.