# The Undo List

*Before an AI agent gets a permission it can't give back, list what it can do that can't be undone, and check the way back.*

On November 3, 2026, Apple's annual report gained a paragraph on AI agents. It says "some consequences, such as deleting data or completing transactions, may be difficult or impossible to reverse." This sheet is that sentence turned into a list you can check this week.

## Start with what you run

**The agents we run (pilots and vendor products count)** _____

**Who gave each one its access** _____

## List what can't be undone

For each kind of action, write which agents can take it today, without asking anyone. Then fill in what stands in front of it.

| ACTION | AGENTS TODAY | PERSON OR LIMIT | RESTORE, HOW FAST | WHO ANSWERS |
|---|---|---|---|---|
| *Example: Sends a message* | *Support reply agent* | *Drafts only, a person sends* | *None, a sent email stays sent* | *(a role and a name)* |
| *Example (hold): Deletes data* | *Cleanup script agent* | *None* | *Nightly backup, never tested* | |
| Deletes or overwrites data | | | | |
| Completes a transaction or payment | | | | |
| Sends a message outside the team | | | | |
| Changes production with no tested rollback | | | | |
| Anything else we couldn't take back | | | | |

PASS OR HOLD

**Pass a row if it has a named owner and either a restore you've timed in the last 90 days and kept where the agent's own permissions can't reach it, or, for anything that can't be restored, like a sent message or a payment, a person or a hard limit that acts before the agent does. Hold everything else. An untested backup counts as no backup, and a held row keeps the permission off until it passes.**

## Test one restore

Pick the row you'd least want to happen. Restore something from it this week and time it. Then ask whether the person closest to the work could do it without opening a ticket.

**What we restored, and how long it took** _____

**Could the agent's own permissions reach that backup?** _____

**Could the person closest to the work do it themselves?** _____

**Date we test again** _____

## Write the sentence down

Write your own line for the risk register.

**Our line for the risk register** _____

**Who owns it** _____

**Scope.** This is the order I'd go in. It isn't a security review and doesn't replace one. The Apple quote is from its Form 10-K filed with the SEC on November 3, 2026.

*I sell AI software. You don't need anything from me to fill this in.*

**Scan for more field kits**

Every worksheet and every issue of Enterprise Field Notes, free at benpickett.com

Ben Pickett

© 2026 Enterprise Field Notes