Agentic Expense Reporting System

Presented by: Christopher O'Hara, PhD

STEP 1: Review the Current System Documentation

No written response needed.

STEP 2: Find and Fix a Bug

Location *(e.g., Which system step, decision, component, or data is the problem?)*	The bug occurs at the point where Agent 1 writes the extracted data into the spreadsheet's "data" tab.
Problem *(e.g., What should happen, and what is actually happening?)*	The intended behavior is that Agent 1 should only save verified values from the receipt images. In practice, the system sometimes writes incorrect or fabricated information, such as totals or dates, when the receipt is unclear or unreadable.
Solution *(e.g., How could the system be improved to resolve the issue?)*	The fix is to introduce simple validation rules before saving. Totals must be valid numbers, dates must match a proper format, and receipts must correspond to the reference list. If a required field cannot be verified, the system should mark the record as "Needs Review" instead of saving false information.

STEP 3: Add Human Review

Location *(e.g., Where in the system should the human be consulted?)*	The human review step should be placed after Agent 3 has completed its analysis but before the expense report is sent to the third-party payment service. Also, human review prior to this Agent could lead to situations where errors occurred after human review was given.
Decision *(e.g., List the possible decisions the human could make)*	At this stage the human reviewer can either approve the expense, reject it, or request clarification from the employee.
Data *(e.g., What data will the human need to make the decision and where will they get it?)*	To make an informed decision the reviewer needs to see the original receipt images, the extracted totals and categories, the outcome of the policy checks, and the employee's role and purpose for the expense.

STEP 4: Ensure Customer Privacy

Location *(e.g., Which parts of the system could compromise customer privacy?)*	The parts of the system that could compromise privacy are the receipt images, the rows of the spreadsheet that contain names and emails, the HR data used by Agent 3, and the payment information sent to the third-party service.
Solution *(e.g., What specifically would you change to protect customer privacy?)*	To protect privacy, EU employee data should be stored on EU servers. All data should be encrypted at rest and transferred over secure connections. Sensitive values such as card numbers should be masked in both the user interface and in logs. Access should be restricted with role-based permissions so that only authorized staff can view the information. Finally, retention rules should be defined so that personal data is deleted when it is no longer needed.

STEP 5: Extend the Workflow

Capability *(e.g., What new capability do you want to add?)*	To allow an employee to export their transaction history to a spreadsheet.
Location *(e.g., Which system step, decision, component, or data (or combination of several elements) would you add or change?)*	This can be achieved by adding a reporting function that reads from the existing spreadsheet and generates a new file, such as a CSV or Google Sheets. The existing workflow of Agents 1, 2, and 3 does not need to be changed.
Business Value *(e.g., How would this new capability improve your business?)*	The business value of this extension is that employees and managers will be able to review and share past expenses more easily. This reduces the number of support requests, saves time for staff and administrators, and improves both transparency and trust in the system.

STEP 6: Estimate Operational Cost Drivers

(Place an "x" in the appropriate cells)

	Flat and low, regardless of volume	**Flat and high, regardless of volume**	**Highly variable, depending on volume**
Database	X		
Spreadsheet		X	
Mobile Web and Camera	X		
Agent 1			X
Agent 2			X

Agent 3			**X**
Private infrastructure		**X**	
Payment service			**X**