# Agent Design Canvas

Name

**Purpose/Mission** 

#### **Triggers**

- When is the agent woken up?
- What does it do when woken up?

# **Knowledge & Context**

• What data does the agent need?

### **Outputs/Actions**

- What does the agent produce or do?
- What are the key deliverables?

# **Tools/Capabilities/Integrations**

- What capabilities does the agent need?
- What external systems does the agent need to talk to?
- What shared workspaces should the agent access?

#### What Can Possibly Go Wrong?

- What are the key risks & vulnerabilities that we need to
  address?
- Hallucination? Abuse? Data leakage? Cost?

#### **Human Collaboration**

- How and when are humans involved in this?
- When does the agent decide/act on its own, vs wait for human input/approval?
- When does the human trigger an agent, and when does an agent trigger a human?
- Division of responsibility between human & agent?
- Who interacts with the agent and how? One person? Multiple people?

# **Success Metrics/Indicators**

- How do we know it is working & adding value?
- After a change, how do we know if it became better or worse?
- How do we know if we are 'done' (or done enough)?