



ACF EN ACTION

acfstandard.com

ACF en Action applique l'Agentic Commerce Framework® à des entreprises réelles, à partir de sources publiques. Chaque cas montre qui reste responsable quand l'IA décide.

ACF-CS-027 · Case Study #027 · Édition 2026

OpenAI Operator

Comment laisser un agent agir pour vous sans lui confier les décisions qui doivent rester les vôtres ?

CARTE D'IDENTITÉ

SECTEUR	PAYS	TECHNOLOGIE	TYPE	AUTONOMIE	CONFIANCE
Commerce / IA	USA	Agent d'achat web	Encadré	encadré	Moyenne

OUTILS ACF ILLUSTRÉS DANS CE CAS

● ACF-01	● ACF-02	● ACF-03	● ACF-06	● ACF-00	● ACF-05
----------	----------	----------	----------	----------	----------

● mobilisé · ● à prévoir · 6 outils du Toolkit (4 mobilisés, 2 à prévoir, sur 17).

1. Résumé exécutif

Début 2025, OpenAI lance Operator, un agent capable de naviguer sur le web et d'agir pour le compte de l'utilisateur : remplir des formulaires, réserver, acheter. Ce n'est plus un agent qui se contente de répondre, c'est un agent qui fait. La décision déléguée est donc engageante : agir sur des sites réels, parfois dépenser de l'argent ou saisir des identifiants.

Lu au prisme de l'ACF, ce cas est un cas de référence sur la **zone non délégable**. Operator est conçu pour réserver à l'humain les décisions qui l'engagent : avant toute action sensible, il demande une confirmation ; pour saisir un identifiant ou un moyen de paiement, il rend la main à l'utilisateur ; sur les décisions à fort enjeu, il refuse. La confiance ne repose pas sur l'idée que l'agent ne se trompera jamais, mais sur le fait que les décisions engageantes ne lui sont pas accessibles seules. C'est le pendant exact du cas Chevrolet of Watsonville (ACF-CS-026), où un agent pouvait au contraire prétendre engager l'entreprise.

2. Contexte

Le commerce agentique fait émerger une génération d'agents qui n'informent plus seulement mais agissent : ils cliquent, remplissent, valident à la place de l'utilisateur. Cette bascule déplace la question de gouvernance. Tant qu'un agent se contente de répondre, l'erreur reste verbale. Dès qu'il agit sur des sites réels, elle peut coûter de l'argent, exposer des identifiants ou engager une décision irréversible. Operator illustre la façon dont un concepteur peut ouvrir cette capacité d'action tout en la bornant.

3. Sources publiques utilisées

- OpenAI, « Introducing Operator » (janvier 2025).
- OpenAI, « Computer-Using Agent » (documentation technique).
- Digital Commerce 360, « OpenAI debuts Operator, an AI agent with ecommerce applications » (2025).

4. Architecture IA reconstituée (à partir de sources publiques)

Operator (agent de navigation et d'action, lancé début 2025).

- Nature : agent qui pilote un navigateur pour exécuter des tâches à la place de l'utilisateur (comparer, réserver, acheter).
- Fonction : agir sur des sites réels, pas seulement répondre. Il prépare, remplit, propose, puis exécute sous conditions.
- Périmètre d'autonomie : autonome sur la navigation, la comparaison et la préparation d'un panier ; borné dès qu'une action engage l'utilisateur.

Zones réservées à l'humain (par conception) :

- avant toute **action sensible** (finaliser un achat, envoyer un message), l'agent **demande une confirmation** ;
- pour saisir un **identifiant** ou un **moyen de paiement**, l'agent passe en **mode reprise** (takeover) : il rend la main, l'utilisateur saisit lui-même, sans que l'agent capture l'information ;
- sur les **décisions à fort enjeu** (transaction bancaire, statuer sur une candidature), l'agent est entraîné à **refuser** ;
- sur les sites sensibles, il opère sous **supervision rapprochée**.

5. Cartographie ACF

 **Outils mobilisés** : ACF-01 (carte d'autonomie) · ACF-02 (matrice de criticité) · ACF-03 (constitution agentique).

En langage ACF, l'architecture se lit ainsi :

Élément ACF	Dans le déploiement Operator
Humain nommé (responsable)	L'utilisateur qui délègue la tâche : c'est lui qui confirme, reprend la main et répond des actions engagées.
Agent	Operator, qui navigue et agit sur des sites réels.
Plateforme	Le système d'agent d'OpenAI pilotant un navigateur.
Décision déléguée	La préparation et l'exécution des actions non sensibles (naviguer, comparer, remplir un panier).
Niveau d'autonomie	Autonome sur la préparation ; co-décision sur l'engageant (confirmation) ; repris ou refusé sur le sensible et le fort enjeu.
Zones non déléguables	Finaliser un achat, envoyer un message engageant, saisir un identifiant ou un paiement, trancher un cas à fort enjeu.
Règle / garde-fou	Confirmation avant d'engager, mode reprise pour les données sensibles, refus des décisions à fort enjeu, supervision sur sites sensibles.
Tiers de contrôle	L'utilisateur en supervision directe ; le concepteur qui inscrit les bornes dans le fonctionnement.
Traçabilité	Chaque action engageante passe par une confirmation ou une reprise humaine, ce qui laisse un point de contrôle explicite.

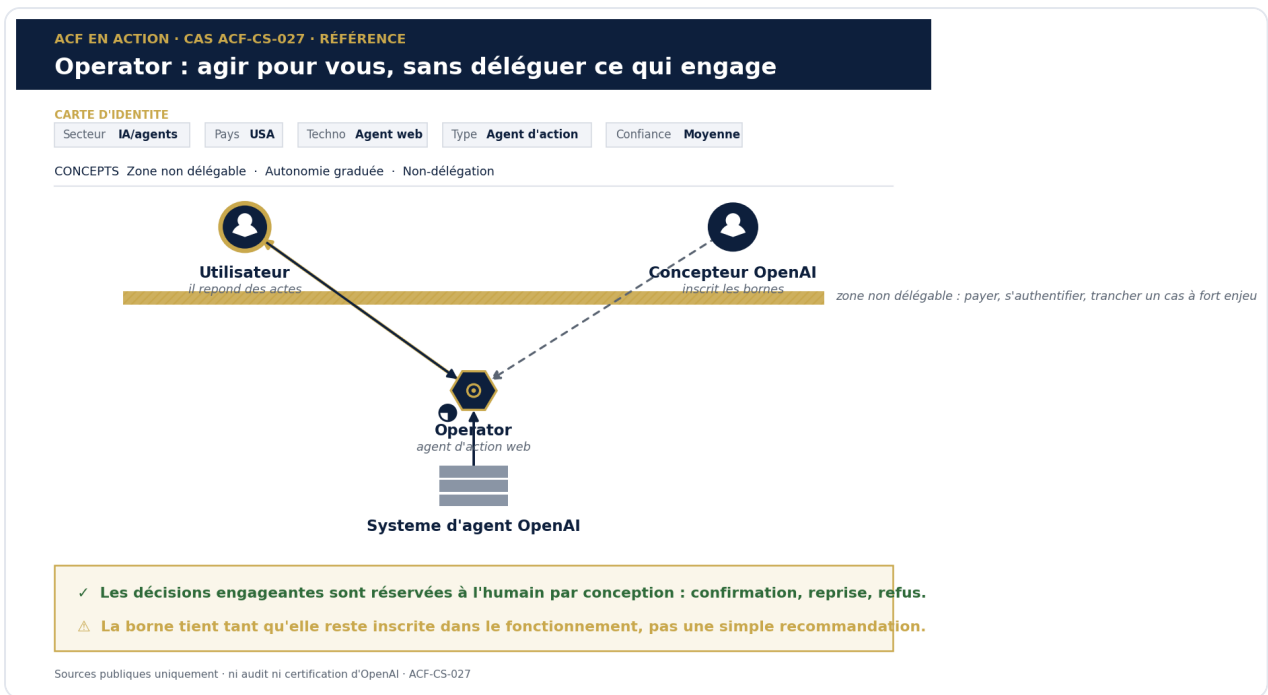
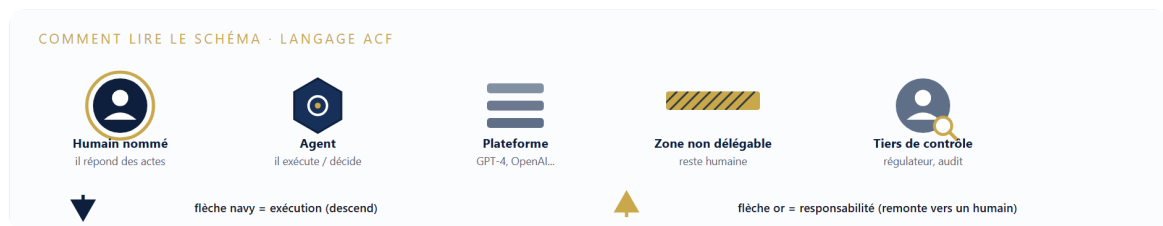


Figure 1 - OpenAI Operator en langage ACF (Language Card).



6. Analyse

Outils mobilisés : ACF-01 (autonomie) · ACF-02 (criticité) · ACF-03 (bornes par conception).

Ce que le déploiement fait bien (la conception de référence) :

- **La zone non délégable est inscrite dans le fonctionnement.** Operator ne demande pas à l'utilisateur de faire confiance : il réserve les décisions engageantes à l'humain. La borne n'est pas une recommandation que l'agent pourrait contourner, c'est une propriété de conception.
- **La criticité pilote l'autonomie.** Préparer et proposer relève d'une criticité faible : l'agent est autonome. Engager, payer ou trancher un cas à fort enjeu relève d'une criticité élevée : l'humain confirme, reprend la main, ou l'agent refuse. L'autonomie est graduée selon l'enjeu, pas uniforme.

- **La confirmation n'est pas un frein, c'est ce qui rend la délégation acceptable.** Parce que l'utilisateur sait qu'aucune dépense ni aucun envoi ne se fera sans lui, il peut confier tout le reste en confiance. C'est le point contre-intuitif du cas : borner l'engageant est précisément ce qui libère le délégable.

Ce que l'ACF nomme et généralise :

- une **constitution agentique** qui pose des bornes opposables : demander confirmation avant d'engager, rendre la main pour les données sensibles, refuser les décisions à fort enjeu ;
- une **matrice de criticité** qui classe, action par action, ce que l'agent peut faire seul et ce qui remonte à l'humain ;
- le principe transférable : les décisions engageantes restent humaines, par conception, quel que soit l'agent.

7. Toolkit ACF mobilisé

Cette grille indique les outils que l'analyse ACF mobilise (✓) pour lire ce cas de référence, et ceux à prévoir (→
SOON). Elle ne signifie pas que l'entreprise utilise l'ACF : elle montre quels instruments le référentiel apporterait.

Outil	Statut	Rôle dans ce cas
ACF-01 · Carte d'autonomie	✓	Situer chaque action (autonome / confirmation / reprise / refus)
ACF-02 · Matrice de criticité	✓	Classer les décisions par enjeu (préparer vs engager)
ACF-03 · Constitution agentique	✓	Formuler les bornes par conception
ACF-05 · Supervision	✓	Relier la supervision rapprochée des sites sensibles à un suivi
ACF-06 · Kill switch	→ SOON	Formaliser l'arrêt sur une action non prévue
ACF-08 · Registre des décisions	→ SOON	Tracer les confirmations et reprises à l'échelle

8. Questions de gouvernance (ce qu'un comité IA devrait se poser)

1. Pour chaque action d'un agent, avons-nous déclaré ce qu'il peut faire seul et ce qui remonte à un humain ?
2. Les décisions engageantes (payer, envoyer, s'authentifier) sont-elles réservées à l'humain par conception, ou seulement par recommandation ?
3. Un agent doit-il pouvoir statuer sur une candidature ou une transaction bancaire ? Où avons-nous placé le refus ?
4. Nos bornes sont-elles inscrites dans le fonctionnement de l'agent, ou l'agent peut-il les contourner ?
5. La confirmation humaine est-elle vécue comme un frein, ou comme ce qui rend la délégation acceptable ?

9. Enseignements généraux

Un agent qui agit ne devient pas dangereux parce qu'il agit, mais quand on lui rend accessibles seules les décisions qui engagent son utilisateur. Operator montre le chemin inverse : réserver l'engageant à l'humain, par conception, ce qui rend possible la délégation de tout le reste. La zone non délégable ne bride pas l'agent, elle rend sa délégation acceptable.

La leçon transférable : on délègue l'exécution, jamais la décision qui engage. Borner l'engageant est ce qui libère le délégable.

10. Ce que ferait l'ACF (conception de référence)

Formulation prescriptive et non critique : voici comment une organisation concevrait un tel agent directement avec le référentiel, quel que soit son secteur.

Si une organisation souhaitait déployer ce type d'agent d'action directement avec l'ACF, elle pourrait notamment :

- **cartographier** chaque type d'action sur l'échelle d'autonomie (ACF-01) et distinguer le préparatoire de l'engageant ;
- **coter** la criticité de chaque décision (ACF-02) pour fixer, action par action, ce qui reste humain ;
- **déclarer** dans une constitution agentique signée (ACF-03) les bornes par conception : confirmation avant d'engager, reprise humaine pour les données sensibles, refus des décisions à fort enjeu ;
- **relier** la supervision rapprochée des contextes sensibles à un suivi continu (ACF-05) ;
- **tracer** les confirmations et reprises dans un registre (ACF-08) dès que le volume d'actions le justifie.

Rien de tout cela n'est un reproche : c'est la manière dont l'ACF rendrait explicite, signable et auditable la conception qu'un agent d'action prudent applique déjà.

11. Cas similaires (transférabilité)

Ce cas n'est propre ni à OpenAI ni au commerce en ligne. Il est transférable à toute organisation qui déploie un agent capable d'**agir**, pas seulement de répondre :

-  assistants d'achat et de réservation
-  agents de service et back-office (RH, finance)
-  automatisation de tâches web en entreprise
-  agents personnels (voyage, administratif)
-  places de marché et paiement agentique
-  outils internes pilotant des systèmes tiers

Partout, le même schéma : un agent qui prépare et exécute à grande échelle, et une frontière (payer, s'authentifier, trancher un cas engageant) à ne jamais franchir sans un humain nommé. C'est ce qui fait de ce document un **cas de référence** : il illustre un concept, pas seulement une entreprise.

12. Confiance de l'évaluation

Moyenne. Le cas repose sur des sources publiques de première main (annonce et documentation d'OpenAI) et une couverture presse spécialisée. Les principes de conception rapportés (confirmation, mode reprise, refus des décisions à fort enjeu) sont documentés publiquement. En revanche, le détail interne de leur implémentation n'est pas public et peut évoluer d'une version à l'autre. L'analyse porte sur la logique de gouvernance affichée, sans incidence de ces détails sur la lecture proposée.

Guide enseignant

Objectif pédagogique. Faire comprendre la notion de zone non délégable par conception : les décisions engageantes restent humaines, ce qui rend possible la délégation du reste.

Déroulé de séance (90 min).

1. (15 min) Lecture des **deux** cas du kit : Chevrolet (incident) et Operator (référence), sans les analyses.
2. (20 min) En groupes : lister ce qu'un agent doit réserver à l'humain, avec la criticité de chaque décision (fiches ACF-01 / 02).
3. (20 min) Atelier : rédiger les bornes par conception (fiche ACF-03) qui empêcheraient un agent d'engager seul.
4. (20 min) Comparaison Chevrolet / Operator : agent reprogrammable sans borne contre confirmation par conception.
5. (15 min) Synthèse : les décisions engageantes restent humaines ; c'est ce qui rend le reste délégable.

Questions d'examen possibles. Voir la section « Questions de gouvernance ».

Rappel : la correction du travail des étudiants est un acte pédagogique du professeur. Le présent guide fournit l'analyse de référence, pas une notation automatique.

Lab associé (ACF-LAB-027)

À partir de ce cas, l'étudiant produit :

- la carte d'autonomie des actions d'Operator (fiche ACF-01) : autonome, confirmation, reprise, refus ;
- la matrice de criticité de trois décisions (fiche ACF-02) : préparer, engager, sensible ;
- une Constitution agentique (fiche ACF-03) : trois bornes par conception, opposables ;
- une comparaison écrite avec le cas Chevrolet : ce qui change du côté des décisions réservées à l'humain.

Annexe - Fiches ACF complétées

Les fiches officielles du Toolkit mobilisées dans ce cas, remplies avec ses données publiques. À titre illustratif : une organisation du même profil peut les reprendre et les adapter.



OBJECTIF

Cartographier les actions d'Operator et fixer, pour chacune, le niveau d'autonomie selon ce qu'elle engage, pas selon sa fréquence. Rempli à partir des sources publiques.

1 ÉCHELLE DE MATURITÉ AGENTIQUE

0

Automatisation classique

Règles fixes, aucune autonomie.

1

Agents assistés

L'agent propose, l'humain décide.

2

Agents gouvernés

L'agent agit dans un cadre, sous supervision.

CIBLE ~80 %

3

Autonomie supervisée

L'agent décide seul ; contrôle a posteriori.

2 VOS DÉCISIONS CLÉS (rempli)

A Navigation et comparaison

ENJEU

Naviguer, comparer, préparer un panier

IMPACT

Réversible, sans engagement

ÉCHÉANCE

Continu

AUTONOMIE

Autonome

B Action engageante

ENJEU

Finaliser un achat, envoyer un message

IMPACT

Engage l'utilisateur : demande une confirmation

ÉCHÉANCE

À chaque action

AUTONOMIE

Co-décision (confirmation)

C Identifiant, paiement, fort enjeu

ENJEU

Saisir un identifiant, payer, trancher un cas sensible

IMPACT

Repris par l'humain ou refusé par conception

ÉCHÉANCE

-

AUTONOMIE

NON DÉLÉGABLE

Lecture : c'est cette gradation, inscrite **avant** le déploiement, qui réserve l'engageant à l'humain et rend le reste déléguable en confiance.



OBJECTIF

Trier les actions par **criticité**, jamais par fréquence. C'est l'outil qui sépare ce qu'Operator fait seul de ce qui remonte à l'humain.

1 LA FORMULE

$$\text{Criticité} = (\text{Impact} \times \text{Fréquence} \times \text{Irréversibilité}) \div 10$$

Seuils : < 15 **faible** · 15-25 **modérée** · > 25 **élevée**

2 LES ACTIONS COTÉES (rempli)

Type d'action	I	F	Ir	Criticité	Zone / autonomie
Naviguer / comparer	2	9	1	1,8	Faible - Autonome
Remplir un panier (préparer)	3	8	2	4,8	Faible - Autonome
Envoyer un message engageant	5	5	7	17,5	Modérée - Confirmation
Finaliser un achat	6	6	6	21,6	Modérée - Co-décision
Saisir identifiant / paiement	8	5	8	32	Élevée - Reprise humaine
Trancher un cas à fort enjeu	9	5	9	40,5	Élevée - Refus par conception

Un routage par **fréquence** aurait traité toutes ces actions de la même façon. Le routage par **criticité** isole payer et s'authentifier (32 ; 40,5) comme non déléguables : exactement les bornes qu'Operator inscrit par conception.



OBJECTIF Définir la constitution de l'agent : identité, principes permanents et zones absolument interdites. Fiche remplie avec les données publiques du cas.

1 IDENTITÉ & MISSION DE L'AGENT

NOM DE L'AGENT

Operator (agent d'action web, OpenAI)

RESPONSABLE (DDAO)

L'utilisateur qui délègue la tâche

MISSION PRINCIPALE

Naviguer, comparer et exécuter des actions non sensibles pour l'utilisateur

PÉRIMÈTRE

Préparation autonome ; confirmation, reprise ou refus dès qu'une action engage

2 PRINCIPES FONDAMENTAUX

- 1 Demander une confirmation avant toute action engageante
- 2 Rendre la main (mode reprise) pour saisir un identifiant ou un paiement
- 3 Refuser les décisions à fort enjeu (transaction bancaire, candidature)
- 4 Opérer sous supervision rapprochée sur les sites sensibles

EXEMPLES DE PRINCIPES

- Respecter le cadre légal et sectoriel
- Protéger les données et la confidentialité
- Rester transparent, toute décision traçable
- En cas de doute, escalader plutôt que décider

3 ZONES INTERDITES (ABSOLUES)

- 1 Finaliser un achat ou envoyer un message sans confirmation humaine
- 2 Capturer un identifiant ou un moyen de paiement de l'utilisateur
- 3 Statuer seul sur une décision à fort enjeu

EXEMPLES D'INTERDITS

- X Engager une dépense au-delà d'un seuil sans validation
- X Communiquer des données personnelles à un tiers
- X Modifier seul ses propres règles ou son périmètre

Constitution lue à partir des sources publiques. Ces bornes ne sont pas des recommandations : elles sont inscrites dans le fonctionnement de l'agent, ce qui les rend opposables.



OBJECTIF Définir les signaux qui bloquent une action ou basculent vers un humain. Fiche remplie avec les déclencheurs pertinents pour le cas.

1 DÉCLENCHEURS

Signal	Seuil	Action
Action engageante non prévue	Hors périmètre confirmé	Blocage, demande de confirmation à l'utilisateur
Site ou contexte sensible	Détecté	Passage en supervision rapprochée ou reprise humaine
Décision à fort enjeu sollicitée	Transaction bancaire, candidature	Refus par conception

2 PROCÉDURE

- 1 Qui décide l'arrêt : l'utilisateur (responsable), borné par le concepteur
- 2 Comment : blocage de l'action, demande de confirmation, mode reprise ou refus
- 3 Test régulier des bornes sur les actions sensibles
- 4 Journalisation de chaque confirmation et reprise (ACF-08)

C'est précisément ce blocage, armé sur toute action engageante, qui réserve à l'humain payer, s'authentifier et trancher un cas à fort enjeu.

Disclaimer

Cette étude est réalisée **exclusivement à partir d'informations publiques**. Elle ne constitue **ni un audit, ni une certification, ni une évaluation officielle** d'OpenAI. Elle applique le référentiel ACF à des fins pédagogiques et illustratives. Aucune donnée interne, confidentielle ou non publique n'a été utilisée. Les marques citées appartiennent à leurs détenteurs respectifs.

Sources

- OpenAI, *Introducing Operator* (janvier 2025) - <https://openai.com/index/introducing-operator/>
- OpenAI, *Computer-Using Agent* (documentation) - <https://openai.com/index/computer-using-agent/>
- Digital Commerce 360, *OpenAI debuts Operator, an AI agent with ecommerce applications* (2025)

ACF Case Study ACF-CS-027 · v1 · document de travail, à relire avant toute diffusion publique.