

# Claude Cowork in a UAE insurer: what is allowed

**A CBUAE-licensed insurer may use Claude Cowork today, across most business functions.**

Nothing in UAE regulation prohibits it, and no approval is needed to start. The conditions come down to two plain questions: which documents the tool is allowed to read, and which of two setups the company runs.

## The two setups, referred to throughout this document:

- **Standard setup.** The company buys Claude for its staff. Documents stay on each employee's computer; when Claude works on a document, the text it reads is processed on the AI provider's servers in the United States. The provider signs the usual vendor data contract, keeps nothing for training, and deletes per the agreed retention terms.
- **Own-cloud setup.** The same product, but the AI processing runs through the company's existing Amazon or Google cloud account, using the cloud contract the company already has. Conversation content (prompts, documents, outputs) goes only to that cloud account and the employee's own device; the AI vendor receives none of it. In beta today, with general availability targeted for 9 July 2026 per Anthropic's documentation. One geography note: AWS offers Claude in its UAE region through a global routing arrangement, so the processing itself may run outside the UAE even though stored data and logs stay in-region; companies wanting geography-bounded processing configure a European endpoint instead.

The rule of thumb for the whole document: everyday business documents work in either setup, today. Documents with customer names and IDs belong in the own-cloud setup, or need one extra piece of vendor paperwork first.

1. Can Cowork be used in the company at all?.....	2
2. Which business functions can use it? .....	2
3. Can Cowork be connected to a folder on a company computer?.....	3
4. Can Cowork work on the files in those folders? Claims, the hardest case, as the example .....	3
5. Is any data transferred that the regulations do not allow? .....	4
6. Can files with customer names and IDs be put in a connected folder? .....	4
7. Can documents be checked for Sharia compliance? .....	5
8. Does the AI vendor keep the company's data or learn from it?.....	5
9. Can Cowork output be shared internally, with reinsurers, with customers?.....	6
10. Is CBUAE approval or notification needed?.....	6
11. Can Cowork be used inside the claims or underwriting process? .....	6
12. What does internal audit get? .....	7
The one-page summary for the board .....	7
About Axxion.....	8



## 1. Can Cowork be used in the company at all?

**Yes.** Any employee may use it for internal work today, in either setup.

**Basis:** No CBUAE regulation, circular, or the consolidated law (Federal Decree-Law No. 6 of 2025) restricts the use of AI productivity tools as such. Obligations arise from what data the tool processes (the UAE data protection law, PDPL), whether a regulated function is outsourced to it (CBUAE outsourcing rules), and whether it influences customer outcomes (CBUAE Guidance Note on Responsible AI/ML, 11 February 2026). None of the three is triggered by drafting, research, or analysis on documents without personal data.

## 2. Which business functions can use it?

**All of them, and most can start this week.** What matters is never the department; it is whether the documents contain customer names, IDs, or other personal details. Most insurance work runs on documents that contain none.

Function	Typical Cowork work	Verdict
Underwriting	Broker request triage, first-draft quotes, submission summaries	Yes today; fleet driver lists and medical census files follow question 6
Compliance and legal	Document screening (including Sharia compliance, question 7), regulation summaries, contract review	Yes today
Marketing and distribution	Content drafting, market monitoring, campaign analysis	Yes today; a person approves before publication
Finance and actuarial	Report drafting, reconciliations, portfolio analysis on aggregated figures	Yes today
HR and operations	Onboarding guides, procedure manuals, daily briefings	Yes today; individual employee files follow question 6
Claims	Estimate review, repair benchmarking, correspondence drafting	Yes today, once names and IDs are kept out of the working files (question 4)

**Basis:** PDPL attaches to personal data, never to a business function. A broker slip, a reinsurance treaty, a policy wording, and a board pack move through Cowork in either setup without any data-transfer question. The recurring exceptions across every function are the same three file types: identity documents, individual medical or salary information, and payment details. Those follow the conditions in questions 5 and 6; everything else starts now.



### 3. Can Cowork be connected to a folder on a company computer?

**Yes.** Connecting a folder moves no data anywhere. The files stay on the computer; nothing is uploaded in bulk.

**Basis:** Cowork runs in an isolated workspace on the user's own computer. Data leaves only when Claude reads a file to do a task, and then only the content of that file. The compliance decision therefore lives at the folder level: connecting a folder changes nothing; asking Claude to work on a file sends that file's content for processing, in whichever setup the company runs.

### 4. Can Cowork work on the files in those folders? Claims, the hardest case, as the example

**Yes, and even in claims the door is wider open than most compliance teams assume.** Claims holds more personal data than any other department, which makes it the useful test: if claims work clears, everything in the question 2 table clears more easily.

Look at what a claims team handles all day: damage photos, repair estimates, parts prices, labor rates, workshop invoices, chassis numbers, repair histories. That is data about vehicles, and the data protection law has nothing to say about where it travels. The personal part of a claims file is thin: the claimant's name, Emirates ID, phone number, and bank details, typically one intake page. Take that page out and work with claim numbers instead of names, and the file Claude reads is vehicle data, usable today in either setup with no extra paperwork.

Data in a motor claims file	What it is	Cowork-ready today?
Damage photos, repair estimates, parts and labor pricing, workshop invoices, repair history	Vehicle and repair data	Yes, no conditions
Chassis number (VIN), plate number	Vehicle data on its own; personal data only when the same file links it to a named driver	Yes, once separated from the identity page
Claimant name, Emirates ID, phone, bank details	Personal data	Yes, under the question 6 conditions
Injury and medical documents	Sensitive personal data	Strictest handling only

**Basis:** PDPL (Federal Decree-Law No. 45 of 2021) governs personal data only; data about a vehicle and its repair sits outside it entirely. A VIN or plate becomes personal data when it is linked to an identifiable person in the same file, which is why the separation step matters and why it is enough. The same logic runs through every function: an underwriting submission without its driver list, or an HR manual without employee records, needs no conditions at all. The practical control is a folder structure organized by data type, so users cannot point the tool at the wrong data by accident.



## 5. Is any data transferred that the regulations do not allow?

**No, provided the setup matches the data.** Three facts keep this manageable.

- **Only what Claude reads travels, and only for the task at hand.** There is no standing connection and no bulk copying. Each transmission is the content of the files Claude opens for one piece of work.
- **Ordinary business documents travel freely.** The rules restrict cross-border movement of personal data. Estimates, wordings, treaties, aggregated figures, and vehicle data are outside those rules, so the core of most departments' work raises no transfer question in either setup.
- **For customer data, both compliant routes are ordinary.** Either sign the standard data-protection paperwork with the AI vendor (the same kind of contract the company signs with every software supplier; the regulator is not involved), or run the own-cloud setup so customer data never goes to the vendor at all.

**Basis:** PDPL Articles 22–23 permit sending personal data outside the UAE only to countries the UAE Data Office recognizes as adequate, or under an approved safeguard such as contract clauses. The United States is on no published adequacy list, so identity documents or bank details processed there in the standard setup require the contractual safeguard. The own-cloud setup removes the question, with one honest limit for the compliance file: AWS offers Claude in its UAE region (me-central-1) only through global cross-region inference. Per AWS documentation, requests may be routed to any destination region, and prompts and outputs may be stored in opt-in regions for abuse detection; logs and audit trails stay in the source region. The defensible description is "data and logs held in-region, AI processing routed globally." Geography-bounded processing exists through the EU regional endpoints. Any vendor claiming "fully in-country AI" should be asked to prove it.

## 6. Can files with customer names and IDs be put in a connected folder?

**Yes, under one of two conditions.** Either replace names and ID numbers with claim or policy references before the files go in, or run the own-cloud setup with the vendor data contract signed. Raw customer files in the standard setup without that contract: **not yet.**

**Basis:** Same PDPL articles as question 5. Working with references instead of identities removes most of the transfer question, because analysis rarely needs to know who the customer is. Medical and injury data is classed as sensitive under PDPL Article 6 and gets the strictest handling in every case. Passwords and system credentials belong in no connected folder under any setup, on security rather than regulatory grounds.



## 7. Can documents be checked for Sharia compliance?

**Yes, today, with no conditions.** This is one of the cleanest first use cases a takaful operator can pick: policy wordings, product documents, marketing material, and correspondence screened for Sharia terminology and structure before they go anywhere.

- **The documents contain no personal data**, so they work in either setup with nothing extra.
- **The screening is exactly what the tool is good at:** checking terminology (contribution rather than premium, participant rather than policyholder), fund-structure references, and consistency across a document set, applied the same way every time.
- **The Sharia committee stays the authority.** Cowork screens and flags; the Internal Sharia Supervision Committee decides. The tool removes the manual reading burden, and the governance line stays exactly where CBUAE's takaful framework puts it.

**Basis:** The CBUAE Takaful Insurance Regulation and Sharia governance standards place responsibility for Sharia conformity with the operator's ISSC; nothing in that framework restricts using software to prepare and pre-screen documents for the committee's review. The AI Guidance Note's human-oversight expectation is satisfied by design, because the committee's decision is the human gate.

## 8. Does the AI vendor keep the company's data or learn from it?

**No.** The vendor does not use company data to train its models, keeps it only as long as the contract says, and in the own-cloud setup never receives it in the first place.

**Basis:** Under Anthropic's commercial terms the insurer remains the owner and controller of its data; Anthropic acts as a processor on the insurer's instructions, the standard vendor relationship compliance already manages for every software supplier, papered the same way (data processing agreement, no-training clause, breach-notification terms). Anthropic also offers zero-data-retention arrangements for some products; whether one applies to a given Cowork deployment should be confirmed with Anthropic during contracting. In the own-cloud setup, Anthropic states there is no conversation egress to Anthropic on the AWS and Google routes: prompts, documents, and outputs go only to the company's configured cloud endpoint, conversation history stays on the employee's device, and the only vendor contact is the application download plus technical telemetry that is scrubbed of content and can be disabled. The equivalent guarantee does not apply on the Microsoft Foundry route, where Claude runs on Anthropic infrastructure.



## 9. Can Cowork output be shared internally, with reinsurers, with customers?

**Yes, with one rule: a person signs off before anything reaches a customer.** Internal circulation and reinsurance submissions need nothing special; they are staff work product like any other.

**Basis:** The output belongs to the company; no vendor term restricts business use. The constraint comes from the CBUAE Guidance Note, which treats an insurance claim as a high-impact decision: AI may draft and recommend, but a named person must approve before any customer-affecting action, and the customer may request a plain-language explanation or human review (Consumer Protection Regulation, Article 8 complaint route).

## 10. Is CBUAE approval or notification needed?

**No for everyday use; yes if a core regulated process runs on it.** Staff drafting and analysis needs no regulator contact. Making the tool part of how claims or underwriting decisions get made calls for early engagement with CBUAE and, where the activity is material, its non-objection.

**Basis:** CBUAE requires prior non-objection for outsourcing material business activities, and supervisory guidance expects early engagement on material cloud plans. Where the materiality line sits is a judgment per use case; drafting support sits below it, a tool inside the claims decision chain sits above it. Direction of travel is worth noting: the Insurance Brokers' Regulation (C 1/2024, Article 17.6) bans brokers from outsourcing any activity offshore and requires client data in-country with 10-year retention. Those are broker-scope rules, but the clearest signal of where supervision is heading for the wider sector.

## 11. Can Cowork be used inside the claims or underwriting process?

**Yes, with the controls regulators expect of any decision-support AI.** A person approves every decision, the deployment is on the company's AI register, it is tested yearly for bias, and it can be switched off in minutes by revoking access.

**Basis:** The CBUAE Guidance Note of 11 February 2026 holds high-impact AI to its strictest standard and makes accountability non-delegable: the institution answers for AI operated by its vendors and TPAs (outsourcing section). "The AI said so" is not a defensible answer to a supervisor; each deployment needs a written description of what it does, what data it uses, and how output is validated.



## 12. What does internal audit get?

### A full evidence trail.

- **Usage logs** tied to the company's own login system, so every action maps to a named employee.
- **The folder access list**, the single most auditable control: which data types the tool can reach, reviewable quarterly.
- **The AI register entry** with owner, data categories, risk rating, and oversight model, as the Guidance Note expects.
- **The vendor data contract and setup configuration** as evidence of the lawful transfer basis.
- **The company's own cloud logs** in the own-cloud setup.

**Basis:** FDL 6/2025 Article 130 puts AI use inside the institution's governance and internal-controls envelope; the items above are what an examiner or internal auditor asks for first. One caution belongs in the audit file: attacks hiding malicious instructions inside received documents have been demonstrated against desktop AI tools (a January 2026 case caused data theft via a rigged file), so folders that receive unscreened third-party documents stay disconnected, and the tool's internet access stays limited to approved destinations.

### The one-page summary for the board

Use	Allowed?	What it takes
Drafting, research, analysis on ordinary business documents (all functions)	Yes, today	Company subscription, vendor data contract, organized folders
Sharia compliance screening of wordings and documents	Yes, today	Nothing extra; the Sharia committee remains the deciding authority
Broker request triage and underwriting submission work	Yes, today	Driver lists and census files handled per question 6
Claims and portfolio analysis on files using claim numbers instead of names	Yes	A documented method for keeping identities out of working files
Files with customer names, IDs, and bank details	Yes, conditionally	Vendor data contract signed, or the own-cloud setup; medical data gets the strictest handling
Inside the claims/underwriting decision chain	Yes, with controls	Person approves each decision, AI register entry, yearly bias test, switch-off procedure; CBUAE engagement where the activity is material
As the official record of policies and claims	No	Official records stay in the company's in-country core systems; Cowork works on copies and outputs



## About Axxion

Axxion Claims Settlement Services L.L.C. is the UAE's first dedicated motor third-party administrator. From Dubai, Axxion manages the full motor claims lifecycle for insurance partners: first notification of loss, surveying, repair coordination, quality control, recovery, and settlement. The company serves UAE insurers across both large and small-to-medium carriers and is preparing to extend into Saudi Arabia and the wider GCC.

**Compliance by design.** Axxion was built to operate inside a tightening regulatory environment. The Central Bank of the UAE absorbed insurance regulation in 2020 and consolidated the framework under Federal Decree-Law No. 6 of 2025, which brings TPAs and loss adjusters explicitly inside the CBUAE perimeter. Every claim Axxion handles passes through formal compliance gates covering UAE PDPL data protection, policyholder-consent requirements, settlement-authority bands, sanctions screening, and audit-trail completeness. Compliance is not an overlay; it is the operating substrate.

**The Axxion Intelligent Operating System (AIOS).** The Claims OS that Axxion presents to insurer partners runs on the AIOS, a unified operating layer orchestrating a seven-stage claims pipeline across surveying, estimation, repair coordination, quality control, recovery, settlement, and reporting. The AIOS integrates human operators with structured AI-assisted decision points at every stage. Insurers receive cleaner data, faster cycle times, lower per-claim cost, and a complete audit trail, without giving up control over their portfolio.

Axxion is led by Managing Director and Co-Founder [Frederik Bisbjerg](#). Frederik has spent over two decades in international insurance in operating and transformation roles, with a particular focus on motor claims, distribution, and AI-enabled insurance models. He has been a public voice on insurance modernization in the GCC and writes regularly on the operational shifts reshaping motor underwriting. Axxion is the operating expression of his thesis: that disciplined claims operations, built on AI-enabled but human-led decisioning, will define the next decade of competitive advantage in motor insurance.

**More information:** Managing Director and Co-Founder Frederik Bisbjerg · [f@axxion.co](mailto:f@axxion.co) · [www.axxion.co](http://www.axxion.co)

*This briefing is an advisory overview prepared by Axxion Claims Settlement Services L.L.C. and does not constitute legal advice. Regulatory positions cited: Federal Decree-Law No. 45 of 2021 (PDPL) Articles 6 and 22–23; Federal Decree-Law No. 6 of 2025 Article 130; CBUAE Insurance Brokers' Regulation (C 1/2024) Articles 15–17; CBUAE Consumer Protection Regulation (Circular No. 8 of 2020) Article 8; CBUAE Guidance Note on Consumer Protection and Responsible Adoption and Use of AI/ML (11 February 2026); CBUAE Regulation Regarding Takaful Insurance (effective 30 December 2022). Product facts reflect Anthropic's published documentation as of 4 July 2026. The own-cloud deployment (Claude Desktop on third-party inference: AWS Bedrock, Google Vertex AI) is in beta with general availability targeted 9 July 2026 per Anthropic's documentation ([claude.com/docs/third-party/claude-desktop/overview](https://claude.com/docs/third-party/claude-desktop/overview)); the no-conversation-egress statement applies to the AWS and Google routes only. AWS regional processing behavior per AWS Bedrock cross-region inference documentation. Product terms change and should be confirmed against the vendors' current documentation before contracting. Outsourcing materiality and record-keeping obligations vary by license category and should be confirmed with qualified UAE counsel. The list of recognized adequate jurisdictions is maintained by the UAE Data Office and must be checked at the time of any transfer decision.*