

SECURITY AND DATA BRIEF

cb5 AI Value Blueprint and AI Value Pilot: what cb5 touches, where it lives, and what cb5 asks of IT

For IT and security leads · Prepared by: cb5

This brief is for the IT or security lead who will be asked, "Is this safe to do here?" It describes how cb5 handles data and access in a Blueprint and a Pilot, the controls built into the work, and what cb5 will ask IT for and when. The SOW and the Master Services Agreement (MSA) govern; where this brief and the SOW differ, the SOW wins.

1. The Blueprint: people and process, not systems

The Blueprint studies how work gets done. It does not build anything, and by default cb5 does not need access to production systems.

What cb5 touches	How	What cb5 does not do
Interviews [45–60 minutes each]	Teams or in person. Notes are taken by the cb5 analyst	No recording without the participants' consent
Day-in-the-life shadowing	Screen share or side by side, with the employee driving	cb5 does not sign in to the customer's systems
A 3–5 day time study	A simple log the participants fill in	No monitoring software; no individual performance reporting
Org charts, team sizes, volumes, salary bands or loaded rates	Provided by the business and finance	No payroll or HR records for individuals
20–50 sample documents for document-heavy processes	Redacted as needed, shared through a folder the customer controls	No bulk exports, no production data feeds
Systems list and current Microsoft licensing	Two or three sessions with the IT Liaison	No technical security testing or penetration testing [out of scope]

If a finding can only be confirmed with production access, cb5 will ask IT first, in writing, and the timeline may change (SOW Template A, assumption A4).

Findings are about processes, not people. Interview notes stay with cb5 so staff can speak openly. Quotes in the report are anonymous unless the speaker approves.

2. The Pilot: your tenant, your identities, staged rings

Principle	What it means in practice
Built in your tenant	The solution is built in the customer's Microsoft 365, Power Platform or Azure environment, under the customer's agreements and licenses. cb5 doesn't host the solution

Principle	What it means in practice
Lower environment first	Build and testing happen in a development or test environment. Nothing reaches production until it has passed the rings below
Your identities	cb5 staff sign in with named accounts the customer issues (member or guest, per IT's standard), under the customer's MFA and Conditional Access
Least privilege	cb5 gets access only to the environments, sites, libraries, mailboxes and systems in scope, by the need-by dates agreed at kickoff. Service accounts or app registrations are named, owned and documented
Production stays with you	The customer approves every production change in writing before cb5 makes it (SOW Template B, assumption A9). Without that approval, cb5 does not deploy
Staged rings	Alpha (IT and project team, lower environment), beta (3–5 pilot users), then pre-production on the production configuration. Each ring ends with a go/no-go that the customer decides, against a threshold agreed up front

3. Where data lives, and what happens at close

Data	Where it lives	At close
Blueprint working files (workbook, maps, report drafts)	A shared folder in the customer's tenant or in cb5's Microsoft 365 tenant, agreed at kickoff	Final report and workbook delivered to the customer. cb5 deletes customer data it holds within the period the MSA or SOW sets after acceptance
Interview, shadowing and time-study notes	cb5's Microsoft 365 tenant, limited to the engagement team	Kept by cb5 as working papers for the period the MSA sets, then deleted. Not shared in raw form
Pilot sample documents and test data	The customer's tenant	Removed from any cb5 workspace at the end of the pilot (SOW Template B, section 11)
The solution, its logs and stored data (e.g., Dataverse tables, SharePoint lists, transcripts)	The customer's tenant	Stays with the customer, under the customer's retention policies. Retention for AI interactions is decided with the customer's legal and records owners (data and security checklist, section 9)
cb5 accounts	The customer's directory	Removed or disabled by IT at the end of hypercare, or earlier on request

cb5 sets up each engagement's Teams and SharePoint workspace to one standard: named guests only, no anonymous links, and guest access removed at close (engagement workspace).

cb5 will confirm deletion in writing on request. cb5 will not put customer data into any AI tool or service the customer has not approved for that data.

4. Microsoft 365 and Copilot: what to confirm

Microsoft describes these points in its own documentation. They change, and product names change, so confirm each one in current Microsoft documentation and your agreements before relying on it.

- **Permissions.** Microsoft 365 Copilot and agents grounded on Microsoft 365 content generally show a user only content that user can already open. That makes **oversharing the main risk**: if a file is shared too widely, AI can surface it to everyone who has access. The pilot checks permissions on every source before the first ring.
- **Processing and training.** Microsoft states that, for its enterprise Copilot offerings, prompts and responses are processed within its Microsoft 365 service boundary and are not used to train foundation models. Microsoft also lists the model providers it uses

as subprocessors. Confirm the current position for the licenses you hold.

- **Features that leave the boundary.** Web search grounding, third-party connectors and agents, and external models can send data outside the tenant. Each one is identified and turned on or off by decision, not by default.
- **Residency.** Tenant data location, Power Platform environment region and Azure regions are checked against your requirements.
- **Audit and retention.** Audit logging, retention and eDiscovery for AI interactions depend on your licenses and settings. They are confirmed before go-live.

5. Responsible-AI controls built into the Pilot

Control	Where it happens
Use-case risk review. Every pilot candidate gets a Low, Medium or High tier based on data sensitivity, decision impact, affected people, regulation, accuracy needs, bias and security. The tier sets the required controls and approvers	During Blueprint scoring, completed before the first ring
Data and security checklist. Identity and access, oversharing, sensitivity labels and DLP, residency, connector governance, logging, agent publishing, external sharing, retention	Started during Blueprint scoring; completed before go-live by the IT Liaison and the cb5 Solution Architect
Human review. A person reviews, edits or approves wherever the output affects money, customers, employees or legal matters. No automated decisions about people	Designed in the pilot charter; tested in every ring
Permission (oversharing) tests. Test accounts with and without access to each source; a user without access must see nothing from it	Alpha ring; the pass mark is 100%, and a failure is a no-go
Untrusted-input tests. Emails, files or web content with embedded instructions; the solution must not follow them or take unplanned actions	Every ring where the solution reads untrusted input; a failure is a no-go
Accuracy on real samples. 20–50 real samples with a pass threshold, for Medium and High tiers	Alpha ring, re-run in pre-production
Rollback. A cutover and rollback plan, and a named owner who can disable the solution	Go-live checklist and hypercare

These checks are recorded on the ring go/no-go scorecard. The customer makes every go/no-go decision. cb5 assists with outcomes the customer controls and does not guarantee them.

6. What cb5 asks IT for, and when

When	Ask	Typical time
Before the Blueprint	Name an IT Liaison; confirm whether engagement files live in your tenant or cb5's	30 minutes
During the Blueprint	Systems inventory and licensing session; data and security conversation; feasibility and risk review of the shortlist	3–5 hours in total
Before the Pilot starts	Named accounts for cb5, access to the lower environment and in-scope sources, licenses for the pilot group, a pilot security group	Per the need-by dates set at kickoff
Early in the Pilot	Risk review approval, permissions review of the pilot content, the data and security checklist with the Solution Architect	As set in the Pilot SOW
Each ring	Join the go/no-go review; approve production changes in writing	30–60 minutes per ring

When	Ask	Typical time
Close	Remove cb5 access; confirm who owns the solution, its monitoring and its logs	30 minutes

7. What this brief does not claim

- cb5 makes no certification or compliance claim about itself in this brief. If your vendor process needs one, ask, and cb5 will answer in writing.
- The Blueprint is not a security audit or penetration test. It is a feasibility and risk view for the opportunities it finds.
- Microsoft's commitments are Microsoft's. cb5 helps configure and test the controls your tenant and licenses provide; your security team owns the policy.

Questions: Chris Crandall, Principal Consultant · cb5 · ccrandall@cbfive.com · 410-698-2706 · www.CBFIVE.com

Chris Crandall · Principal Consultant · cb5 · ccrandall@cbfive.com · 410-698-2706 · www.CBFIVE.com
 Microsoft Solutions | Systems Integration | IT Consulting