



Digital Control Solutions
Your data under your control.

Regaining Control of Information Assets

A practical whitepaper for non-US organizations seeking data-resident cloud workspace, private AI, lower dependency risk, and open-source alternatives to de facto default platforms.

DCS helps non-US public-sector, regulated, and small-to-medium organizations reduce dependency, control AI risk, and move sensitive workflows toward environments they can govern, operate, audit, and change.

The goal is not a disruptive overnight replacement of Microsoft 365, Azure, Google Workspace, Google Cloud, or commercial AI tools. The goal is a safe migration path to controllable alternatives where data, cost leverage, and AI governance matter most.

AUDIENCE

Non-US public,
regulated, SMB

FOCUS

Dependency, cost, AI
control

VERSION

Draft v0.5 | 2026



Control is becoming a board-level and public-interest issue: where information lives, who can administer it, how AI can use it, and whether the organization can leave a platform without losing operational continuity.

The next phase of cloud strategy is control.

For many non-US organizations, the digital workplace has become a control problem: critical data, records, communications, and AI workflows sit inside platforms governed, priced, and roadmapped elsewhere.

Data residency alone does not solve that problem. Buyers also need vendor leverage, administrative control, export readiness, AI usage boundaries, cost governance, and trusted operations. The board-level question is no longer only where data is hosted. It is whether the organization can govern, audit, operate, control cost exposure, and leave a platform without losing continuity.

DCS proposes a practical model: **Assess, Implement, Manage**. Start with evidence. Implement OpenDesk and self-hosted Mistral private AI where they fit. Operate the environment with evidence, security, backup, and governance discipline.

Whitepaper Thesis

Data residency is the start of the conversation, not the end. A useful control strategy must combine location, jurisdiction, vendor dependency, cost, identity, access, records, export, operational evidence, and private AI governance.

- Keep familiar tools where they are still appropriate.
- Move sensitive workflows first.
- Use OpenDesk and Mistral AI as deployable solution foundations.
- Add Mistral-enabled private AI where governance matters.
- Measure savings through avoided premium licenses, reduced SaaS/cloud waste, governed AI token consumption, and controlled expansion.

29%

Estimated wasted cloud spend reported in Flexera's 2026 State of the Cloud research.^[17]

\$4.99M

Global average cost of a data breach reported by IBM's 2026 Cost of a Data Breach research.

\$69

Monthly per-user benchmark for Microsoft 365 E3 with Teams plus Microsoft 365 Copilot at public list pricing.^[13]

DCS is pro-control, not anti-cloud. The strongest business case is not ideological. It is a pragmatic move to reduce jurisdictional concentration risk, create migration leverage, improve governance, and lower avoidable spend on sensitive workflows, premium bundles, unmanaged cloud growth, and AI consumption.

A buyer-facing case for data-resident workspace and private AI.

01	The Dependency Problem	Why de facto default platforms create strategic exposure
02	Europe's Working Precedent	ZenDiS, openDesk, openCode, La Suite, Mistral, and AI control
03	The International Moment	Why jurisdictions need credible alternatives to default platforms
04	The Cost Case	License avoidance, AI add-ons, cloud waste, and migration economics
05	The DCS Reference Architecture	OpenDesk, Mistral, identity, records, and coexistence
06	The Delivery Model	Assess, Implement, Manage
07	Public Sector and Regulated Organizations	How DCS maps to accountability, evidence, and operational resilience
08	Public and Regulated Buyer Scenarios	Concrete first projects by organization type
09	Business Case and First Projects	Fixed-price services, solution costs, and managed services
10	Competitive Landscape	How DCS differs from incumbent and adjacent alternatives
11	Migration, Proof, and Appendices	Roadmap, proof artifacts, objections, architecture, and next step

DCS offer: fixed-price assessment and implementation services, deployable OpenDesk and Mistral AI solutions, and recurring per-seat managed services for the controlled environment.



Your digital workplace is now critical infrastructure.

The cloud productivity suite is no longer just email and documents. It is identity, storage, chat, video, records, workflow, search, compliance, endpoint management, automation, and increasingly AI.

That consolidation creates convenience, but it also concentrates operational and geopolitical risk. Sensitive data and administrative access can sit inside foreign-governed ecosystems, even when providers offer so-called data-resident hosting. The organization may still rely on vendor-controlled roadmaps, standard contracts, support models, audit surfaces, AI features, and policy decisions beyond its practical influence.

The DCS position is simple: organizations should regain control where control matters most, without forcing users through unnecessary change.

Dependency shows up as five practical risks

- **Commercial lock-in:** contract, licensing, and feature bundling leverage sits with the platform vendor.
- **Operational opacity:** evidence often depends on vendor dashboards and assurances.
- **AI exposure:** assistants inherit access to collaboration stores and can create new leakage paths.
- **Exit friction:** records, links, permissions, workflows, and identities become hard to untangle.
- **Admin complexity:** configurations become more difficult for administrators and easier for users to misapply.

Data

Where content, metadata, indexes, backups, logs, support artifacts, and AI-derived outputs reside and who can access them.

Control

Whether the organization controls identity, admin access, retention, export, audit evidence, and operational policy.

Choice

Whether the organization can migrate, coexist, or reverse course without unacceptable disruption.

Default Platform Pattern	Control Concern	DCS Response
Microsoft 365/Azure and Copilot embedded into daily work	High switching costs across identity, files, Teams, compliance, and AI	Coexistence-first migration strategy for sensitive workflows and private AI
Google Workspace/Cloud and Gemini in shared collaboration spaces	Data-region coverage, admin policy, Drive sharing, and AI expansion complexity	Evidence-based assessment and staged migration to data-resident collaboration
Non-transparent AI services used directly by staff	Prompt, file, source, and output leakage outside governance boundaries	Private AI gateway with RAG, permissions, retention, and audit logging

Europe, led by Germany and France, is starting to turn digital autonomy into operating models.

Europe is no longer treating digital sovereignty as an abstract policy slogan. Germany's ZenDiS, openDesk, and openCode ecosystem shows how public institutions can package open-source tools into a recognizable workplace alternative.^{[1][2][3]}

openDesk is positioned as an office and collaboration suite for public administration, combining familiar workplace capabilities such as email, file storage, documents, chat, video, IAM, knowledge, projects, and tasks.^[2] openCode provides a shared platform for public-sector open-source software, reducing duplicated development and helping administrations share code and knowledge.^[3]

AI makes the autonomy question sharper. ChatGPT, Claude, Gemini, Grok, and China-based or other foreign-controlled AI services should be evaluated by evidence, not brand familiarity: which terms apply, who can access prompts and logs, whether content can train or improve models, which connectors can reach internal data, and who controls official or policy-shaping output.^{[20][21][22][23][24]}

DCS should point buyers toward controllable AI patterns, including Mistral-enabled private AI where models, retrieval indexes, logs, access controls, retention, and deployment location can sit inside customer-controlled or data-resident environments.^{[9][10]}

AI control questions

- Can sensitive prompts, files, and outputs be kept out of model training?
- Can users intentionally or accidentally leak restricted information?
- Do AI connectors overreach into mail, files, chat, or records?
- Can outputs shape public messaging without accountable review?
- Can logs, retention, routing, and costs be governed by policy?

GERMANY

ZenDiS

Public-sector center created to strengthen digital sovereignty and reduce critical dependencies on individual technology providers.^[1]

GERMANY

openDesk

Integrated workplace package for public administration built from established open-source components and available through openCode.^{[2][4]}

GERMANY

openCode

Shared software platform for administration-related open-source projects, quality checks, and community exchange.^[3]

FRANCE

La Suite

Open-source collaborative workspace led by DINUM and ANCT, with products for messaging, video, docs, files, spreadsheets, transfer, and email.^[6]

FRANCE

SecNumCloud

ANSSI's cloud qualification framework for higher technical, operational, and legal assurance for sensitive cloud uses.^[8]

EUROPE

100-Day Challenges

Franco-German and Dutch collaboration has addressed SSO, secure AI-powered collaboration, and document editing use cases.^[5]

The DCS insight: Other jurisdictions do not need to copy Europe word for word. They can adapt the pattern: package open-source workplace, private AI, data residency, managed services, and migration expertise into a buyer-friendly offer.



Jurisdictions need control strategies, not slogans.

Many countries, states, provinces, municipalities, and regulated sectors face the same pragmatic issue: critical information assets are increasingly inside platforms governed, priced, operated, and roadmapped outside the customer's jurisdiction.

Canada is one useful proof point. The Government of Canada has published material on data sovereignty and public cloud, including the limits of residency-only thinking and the relevance of privacy, contractual, technical, and operational safeguards.^[11] For federally regulated financial institutions, OSFI's B-10 guideline makes accountability, third-party risk, criticality, substitutability, access, data practices, monitoring, incidents, and exit planning board-level concerns.^[12]

DCS should position itself where those concerns become executable: data residency assessment, migration strategy, open-source workplace implementation, private AI, and managed operations.

High-fit international buyers

- Municipalities, states, provinces, and regional governments
- Indigenous, local, and community-governed organizations
- Education and healthcare-adjacent organizations
- Financial services and regulated professional firms
- Critical infrastructure operators and utilities
- Nonprofits handling sensitive resident, citizen, or client data

Public accountability

Public bodies must be able to explain how citizen, resident, student, employee, and operational data is controlled and protected.

Regulated accountability

Regulated firms remain accountable for outsourced services and must manage third-party risk across the relationship lifecycle.^[12]

AI accountability

AI raises new questions about prompts, source permissions, derived content, model logs, retention, and administrative access.

Buyer Pain Point	Why It Matters	DCS Whitepaper Position
Data residency claims are fragmented	Different services, metadata, logs, backups, support artifacts, and AI workflows may follow different paths.	Start with an evidence register instead of assumptions.
Platform configuration is complex	Admins can unintentionally weaken policy through roles, sharing, third-party apps, or feature enablement.	Assess control posture, not only location.
Exit is rarely tested	Records, permissions, formats, workflow history, links, and dependencies make migration harder later.	Build export and transition readiness into the target architecture.
AI demand is immediate	Employees will use AI whether governance is ready or not.	Provide private AI alternatives inside the governance boundary.



Control can also be a cost strategy.

Financial savings can be a real driver for DCS, but the claim should be evidence-based. The business case should not promise that open source magically costs less in every scenario. The stronger claim is that DCS gives organizations more levers: fewer unnecessary premium licenses, lower exposure to forced bundles, reduced waste, better migration leverage, and private AI economics for sensitive internal workloads.

Microsoft's public enterprise pricing provides a useful benchmark: Microsoft 365 E3 with Teams is listed at \$39/user/month and E5 at \$60/user/month, while Microsoft 365 Copilot is listed as a \$30/user/month add-on for eligible plans.^[13] Microsoft also published enterprise suite price increases effective July 1, 2026, including E3 and E5 changes.^[14]

AI also changes the cost model from per-seat licensing to variable consumption. Each prompt, file upload, retrieval query, rerun, agent loop, and model choice can consume tokens. Gartner warns that AI coding costs may overtake average developer salary by 2028 as token consumption rises; current reporting also shows enterprise AI budgets can be exhausted quickly when usage is unmanaged.^{[25][26]}

For a 1,000-seat organization, the difference between licensing every user for E3 plus Copilot and licensing only high-need users while moving selected workflows to DCS can become material.

Cost savings drivers

- Reduce all-user premium licensing where only some users need premium features.
- Avoid blanket AI add-ons for low-value or high-risk use cases.
- Govern token spend by workflow, model, user group, and data class.
- Reduce SaaS and cloud waste through assessment and rightsizing.
- Route routine AI work to lower-cost or private models where appropriate.
- Improve negotiating leverage by creating credible alternatives.

Scenario	Public List Benchmark	1,000 Users / Year	DCS Interpretation
Microsoft 365 E3 with Teams	\$39/user/mo	\$468,000	Baseline for a broad enterprise suite before AI add-ons and adjacent services.
Microsoft 365 E3 with Teams + Copilot	\$69/user/mo	\$828,000	Useful benchmark for blanket productivity-plus-AI licensing.
Microsoft 365 E5 with Teams + Copilot	\$90/user/mo	\$1,080,000	High-control Microsoft stack benchmark before other migration, backup, or consumption costs.
DCS target strategy	Customer-specific	Model per pilot	Use coexistence to move sensitive/high-cost workflows first, not every user on day one.

Cost proof should be customer-specific. The DCS assessment should calculate current license utilization, premium-feature dependency, storage growth, AI demand, token consumption, duplicate tools, backup costs, support costs, and migration effort before making savings claims.

8%

Microsoft 365 E3 with Teams price increase listed for July 1, 2026.^[14]

29%

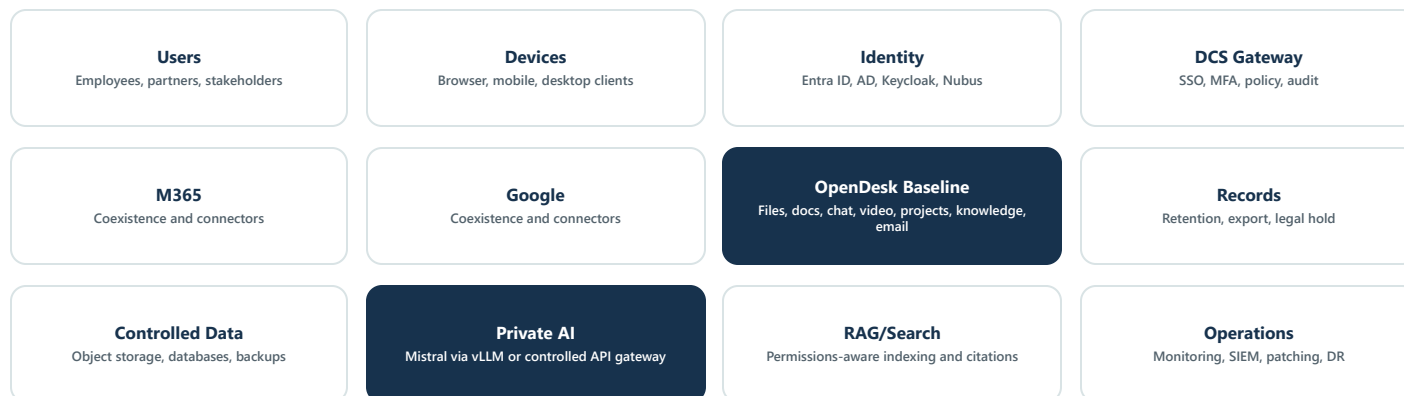
Estimated cloud waste reported in Flexera 2026 research.

2028

Gartner prediction for AI coding costs overtaking average developer salary as token use rises.^[25]

A data-resident workplace and private AI control layer.

DCS should be presented as a compatible control layer that can coexist with Microsoft 365 and Google Workspace while introducing open-source, data-resident alternatives for selected workflows.



OpenDesk Foundation

openDesk provides a relevant baseline because it bundles collaboration capabilities that users recognize: calendar, chat, contacts, documents, email, file storage, IAM, knowledge, notes, projects, tasks, and video calls.^[2]

The DCS model should stay modular: use openDesk where it fits, integrate carefully, and avoid full email migration until the customer is ready.

Mistral Private AI

Mistral documents self-deployment of models through inference engines such as vLLM, TensorRT-LLM, and TGI.^[9] Mistral also positions self-hosted enterprise deployment as a way to keep data within the customer's walls.^[10]

DCS should wrap private AI with identity, source permissions, prompt logging, retention, export, and human governance.



Access controls, records policies, and data residency should govern the AI, not the other way around.



Assess, implement, and manage.



The delivery model moves from evidence to controlled migration and then into managed operations.

PHASE 1

Assess

Run the DCS Data Residency Assessment to extract vendor-reported evidence, configuration posture, admin access, app grants, AI exposure, and migration candidates.

PHASE 2

Implement

Design a coexistence-first pilot using open-source workplace components, identity integration, controlled repositories, migration waves, and Mistral-enabled private AI.

PHASE 3

Manage

Operate the implemented environment with monitoring, support, patching, backup, access review, evidence reporting, AI governance, and continuous improvement.

Phase	Primary Output	Executive Value	Technical Value
Assessment	Evidence register and migration roadmap	Shows where control is already acceptable and where it is weak	Creates tenant, data, app, role, AI, and portability baseline
Implementation	Controlled pilot and target architecture	Proves the path without disrupting all users	Validates identity, data, workflows, RAG, backup, and coexistence
Managed Services	Operating model and monthly evidence	Keeps control practical after go-live	Maintains patching, monitoring, access, recovery, and AI controls

Ownership without trusted operations is not control.

Open-source and data-resident infrastructure must still be run well. If the customer lacks operational capacity, an open-source alternative can become a new burden rather than a control strategy.

DCS Managed Services completes the model by operating the environment while leaving governance authority with the customer. This is especially important for smaller public bodies and regulated organizations that need evidence and resilience but cannot build a full platform operations team.

Managed methodology

Monitor, support, secure, protect, govern, and improve the implemented environment with a repeatable operating methodology.



The DCS Managed Services methodology keeps data-resident workspace and private AI environments reliable, governed, recoverable, and ready for controlled expansion.

Evidence

Monthly operating evidence, access reviews, backup status, restore tests, patch posture, and exception tracking.

Resilience

Monitoring, incident response, recovery planning, export readiness, and operational continuity.

AI Governance

RAG indexing, model lifecycle, source permissions, prompt/output controls, and usage review.



Control requirements are different when accountability cannot be outsourced.

Public-sector and regulated buyers have a different burden than ordinary commercial SaaS buyers. They must be able to explain decisions to citizens, clients, auditors, boards, councils, regulators, privacy officers, and procurement authorities.

OSFI's B-10 language is useful beyond financial institutions because it captures the broader shift: organizations remain accountable for third-party arrangements and must understand criticality, substitutability, data practices, subcontractors, incidents, monitoring, and exit.^[12]

Why DCS fits these sectors

- Evidence-based residency and control assessment.
- Procurement-friendly migration roadmap.
- Data-resident implementation options.
- Private AI for sensitive knowledge work.
- Managed services with monthly operating evidence.

Sector	Common Sensitive Workflows	DCS First Project
Municipality	Council records, bylaws, planning documents, HR, legal, resident-service files	Controlled council workspace plus policy/bylaw private AI assistant
School board	Board packets, HR, accessibility records, procurement files, student-adjacent administration	Board and administration workspace with export-ready records
Healthcare-adjacent nonprofit	Client files, program records, referrals, funder reports, privacy-sensitive collaboration	Data-resident collaboration and secure intake/document workflow
Financial services firm	Client files, regulated records, audit evidence, third-party access, board materials	Private AI over policy, risk, compliance, and procedure repositories
Legal/professional services	Client confidentiality, matter records, privileged communications, evidence bundles	Controlled client workspace and export-ready records repository
Indigenous/community government	Community records, grants, programs, member services, governance material, land files	Community-controlled knowledge workspace and records migration plan

Governance angle: DCS should not ask buyers to trust a slogan. It should give them artifacts: evidence registers, architecture diagrams, access reviews, backup proofs, AI policy mapping, and export plans.



Start where control, cost, and adoption overlap.

The best first DCS projects are not full-suite replacements. They are controlled, high-sensitivity workflows where the organization can prove value quickly while preserving coexistence with existing tools.

DCS should lead with a fixed-scope assessment and one practical pilot. The assessment creates the evidence; the pilot creates the reference case; managed services turns the pilot into a durable control environment.

Recommended first offer

DCS Data Residency Assessment

A fixed-fee engagement that maps vendor-reported residency, configuration, admin access, AI exposure, sensitive workflows, and migration candidates.

Commercial Component	Pricing Model	Buyer Benefit
DCS Assessment	Fixed price	Evidence register, cost model, AI/control findings, migration candidates
DCS Implementation	Fixed price by scope	Predictable pilot or phased deployment with acceptance criteria
Solution/runtime costs	Customer-specific	OpenDesk hosting, storage, backup, Mistral API or self-hosted inference costs
DCS Managed Services	Recurring per seat	Operations, support, security, backup, monitoring, evidence, and governance rhythm

Board workspace

Move board, council, committee, or executive records into a controlled collaboration space with export-ready records.

Private AI assistant

Deploy Mistral-enabled RAG over approved policy, procedure, bylaw, procurement, or compliance repositories.

Secure data room

Create a data-resident workspace for legal, procurement, resident-services, client, or regulated collaboration.

Value Lever	How to Measure	Buyer Outcome
License avoidance	Users not requiring premium AI or full-suite features for selected workflows	Lower exposure to blanket per-seat uplift
SaaS/cloud waste	Unused licenses, duplicate tools, unmanaged storage growth, overlapping AI tools	Reduced waste and clearer procurement baseline
Risk reduction	Fewer uncontrolled repositories, fewer privileged access exceptions, fewer shadow AI paths	Better audit and privacy posture
Portability	Export readiness, open formats, tested backups, documented runbooks	Higher negotiating leverage and lower exit risk
Productivity	Search time saved, meeting summary time saved, policy lookup speed, support deflection	Private AI value without uncontrolled data exposure

The strongest DCS business case starts with evidence, proves one useful controlled workflow, validates the cost baseline, and then expands only where users, governance, and cost data support the move.



DCS is not a reseller story. It is a control strategy.

Most alternatives solve only one part of the problem: licensing, infrastructure, open-source deployment, AI tools, or local support. DCS should position itself as the service layer that turns deployable components into a governed operating model.

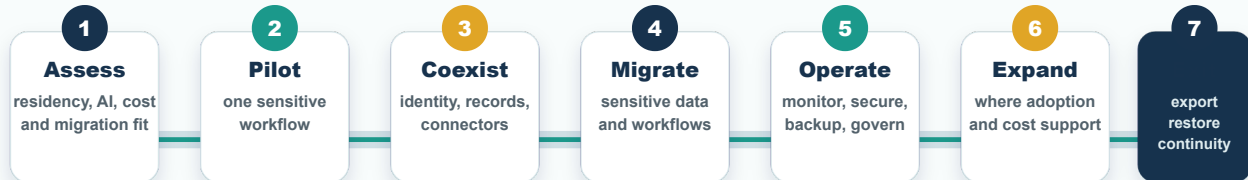
Alternative	Strength	Limit	DCS Difference
Microsoft/Google status quo	Familiar, mature, integrated, broadly supported	Dependency, cost escalation, policy complexity, AI exposure, exit friction	Coexistence-first alternative path for sensitive workflows
Local MSP	Operational support and buyer relationship	Often resells the same default platforms	Managed control environment with evidence and migration roadmap
Pure open-source integrator	Technical deployment skill	May lack business case, governance, adoption, and managed operations model	Assess, implement, and manage as one repeatable offer
Cloud reseller	Procurement convenience and discounts	Can deepen dependency on default hyperscale platforms	Cost leverage through credible alternatives and selective migration
Private AI vendor	AI specialization	May not address workspace, records, email, and migration	Mistral-enabled AI inside a broader data-resident workspace architecture
EU-style sovereign cloud vendor	Jurisdictional and infrastructure assurance	May not fit non-US local markets or SMB budgets directly	Adapt the European pattern for local jurisdictions and practical first projects

Positioning line: DCS helps buyers keep what works, prove what should move, and operate the new environment without becoming their own platform company.

A practical path beats a theoretical replacement.

Practical Migration Path

Start with evidence, prove one controlled workflow, then expand where cost, risk, and adoption data support it.



DCS principle: do not force a full-suite replacement first.
Prove value in controlled workflows and grow from evidence.

Assess, pilot, coexist, migrate sensitive workflows, operate, expand, and test exit readiness.

Proof Artifacts

Assessment report, residency evidence register, architecture diagram, migration roadmap, cost model, pilot environment, governance runbook, and monthly operations report.

Migration Discipline

Coexist first, preserve user continuity, test export/restore, document policy decisions, and avoid full-suite migration until evidence supports it.

Success Measures

Reduced uncontrolled data paths, lower premium-license exposure, governed AI usage, successful restore tests, and user adoption in the pilot workflow.

Delivery model: fixed-price assessment, fixed-price implementation by scope, solution/runtime costs as customer-specific pass-through or platform pricing, and recurring managed services per seat.



OpenDesk, Open-Xchange, and Mistral fit into a governed coexistence model.

DCS REFERENCE ARCHITECTURE

Coexist and migrate sensitive workflows, then operate under customer control.

Existing environment

Microsoft 365/Azure, Google Workspace/Cloud, legacy apps, endpoints, user communities, records stores

DCS control and coexistence layer

SSO, MFA, policy gateway, migration connectors, retention/export rules, audit logging, routing decisions

- identity
- policy
- connectors
- audit
- export

Data-resident DCS solution zone

OpenDesk workplace services plus self-hosted Mistral private AI, governed by customer policy

- Open-Xchange
- Nextcloud
- Collabora
- Element/Jitsi
- Records
- Mistral/RAG

Monitoring, SIEM/logging, backup and restore testing, patching, vulnerability management, runbooks, evidence packs

DCS should deploy openDesk on Kubernetes-based data-resident infrastructure, use Open-Xchange for email/calendar/contact capabilities, and start with self-hosted Mistral private AI for sensitive workflows.

OpenDesk Baseline

Workplace services including documents, files, communication, projects, knowledge, identity integration, and Open-Xchange email strategy.^{[27][28]}

Private AI

Self-hosted Mistral models, RAG/search, prompt logging, source permissions, retention, token policy, and model-routing controls.^{[9][10][29]}

Operations

Monitoring, SIEM/logging, backup, restore testing, patching, vulnerability management, and evidence packs for monthly governance.



The objection is usually right. The answer is a controlled path.

Likely Objection	Careful DCS Response
User adoption	Do not start with all users. Start with familiar workflows, training, champions, and coexistence.
Compatibility	Use M365/Google coexistence and migration connectors; define what stays, what moves, and what waits.
Support maturity	Pair deployable open-source solutions with DCS managed services and monthly evidence reporting.
Open-source risk	Assess component maturity, patch cadence, support model, backup, monitoring, and exit plan.
Security	Security depends on architecture and operations, not slogans. Include MFA, logging, backup, restore tests, and access reviews.
Cost uncertainty	Use fixed-price assessment and implementation scopes; separate solution/runtime costs from per-seat managed services.
Email migration difficulty	Use Open-Xchange carefully, with coexistence, phased mailbox groups, archive/retention planning, and rollback criteria.
Why not configure M365 better?	Often you should. DCS starts with assessment and coexistence, but gives the buyer a credible alternative where control matters most.

Legal and compliance language: DCS should not claim to eliminate all jurisdictional, privacy, procurement, or AI risk. It should claim to reduce dependency, improve evidence, create customer-controlled operating options, and support customer-specific legal/compliance review.



Start with a DCS Data Residency and AI Control Assessment.

A realistic first customer story should show a narrow, useful move: one buyer, one sensitive workflow, one measurable reduction in dependency, and one operational proof package.

Example placeholder: A regional public-service organization used M365 broadly but moved board materials, policy documents, and internal procedure search into a DCS-controlled workspace with private AI. Users kept everyday email and calendars during the pilot, while the organization gained export-ready records, AI usage logs, backup evidence, and a migration roadmap.

2-4 week assessment deliverables

- Current-state dependency and residency map.
- AI exposure and token-spend findings.
- Cost model and candidate workflow shortlist.
- Target architecture and migration roadmap.
- Fixed-price implementation proposal.

Before	After Pilot	Evidence Produced
Sensitive records spread across default collaboration spaces	Controlled workspace for board/policy records	Residency register, access review, export test
Staff experimenting with unmanaged AI tools	Mistral-enabled private AI over approved sources	Prompt policy, source permissions, usage report
Cost discussion based on license list prices only	Customer-specific model for licenses, hosting, AI, and managed services	Cost model and expansion criteria

Recommended next step: start with a DCS Data Residency and AI Control Assessment, then decide whether the first implementation should be a board workspace, private AI assistant, secure data room, or email/workspace coexistence pilot.

Sources for the whitepaper.

This draft uses official sources where possible. Video references were used as context for the ZenDiS/openDesk category and should be reviewed more deeply if direct quotes or transcript-based claims are added in a later version.

- [1] ZenDiS, **Co-creating Digital Sovereignty**. Used for ZenDiS mission, public-sector independence, and dependency framing.
- [2] openDesk, **The office and collaboration suite for public administration and Product**. Used for openDesk capabilities and public administration positioning.
- [3] ZenDiS, **What we offer**. Used for openCode positioning as a central public-sector open-source platform.
- [4] openCode, **openDesk software entry**. Used for openDesk availability and public administration framing.
- [5] openDesk, **Strategic partnerships for digital autonomy**. Used for Germany-France-Netherlands collaboration, 100-Day Challenges, secure AI collaboration, and sovereign LLM context.
- [6] La Suite Numerique GitHub, **La Suite numerique**. Used for French open-source collaborative workspace components and public-agent audience.
- [7] DINUM / numerique.gouv.fr, **France's digital public innovations**. Used for trusted cloud, open tools, and public-sector AI context.
- [8] ANSSI, **Recommendations on hosting sensitive information systems in the cloud**. Used for SecNumCloud and sensitive cloud assurance framing.
- [9] Mistral Docs, **Self-Deployment**. Used for self-hosted model deployment through vLLM, TensorRT-LLM, and TGI.
- [10] Mistral AI, **Enterprise AI platform**. Used for enterprise deployment, self-hosting, and private AI control positioning.
- [11] Government of Canada, **Data Sovereignty and Public Cloud White Paper**. Used as one public-sector example of data sovereignty, residency, and public cloud control concerns.
- [12] OSFI, **Third-Party Risk Management Guideline B-10**. Used for third-party accountability, monitoring, risk, and exit framing for regulated organizations.
- [13] Microsoft, **Microsoft 365 enterprise plans and pricing**. Used for Microsoft 365 E3/E5 and Copilot public list benchmarks accessed August 3, 2026.
- [14] Microsoft Licensing Resources, **2026 Microsoft 365 pricing and packaging updates**. Used for July 1, 2026 price-change percentages and new prices.
- [15] Google Workspace, **Pricing and plan features**; Google Cloud, **Gemini Enterprise**. Used for Workspace data-region features, Enterprise positioning, and Gemini access model.
- [16] IBM, **Cost of a Data Breach Report 2026**. Used for global average breach cost and AI-driven attack growth statistics.
- [17] Flexera, **2026 State of the Cloud**. Used for estimated wasted cloud spend and cost-management context.
- [18] IBM, **Cost of Data Breach: shadow AI**. Used for shadow AI breach cost and unsanctioned AI risk context.
- [19] Video references reviewed: **ZenDiS YouTube channel**, **openDesk sovereign workplace playlist**, and public ZenDiS/openDesk interviews and presentations surfaced in search results. Used as category context; no transcript-specific claims are made in this draft.
- [20] OpenAI, **Enterprise privacy and data use for model performance**. Used for business-data and individual-service training distinction.
- [21] Anthropic Privacy Center, **Commercial data training policy**. Used for Claude commercial-product data-use framing.
- [22] Google Workspace, **Generative AI in Workspace Privacy Hub**. Used for Gemini Workspace data protection and connector/data-region caveats.
- [23] xAI, **Privacy Portal**. Used for Grok opt-out and model-training control framing.
- [24] OWASP, **Top 10 for Large Language Model Applications**. Used for prompt injection, sensitive information disclosure, model denial-of-service, and excessive agency risks.
- [25] Gartner, **AI coding costs and token consumption**. Used for token-driven AI cost-control framing.
- [26] Business Insider, **Burning through your AI budget?**. Used for enterprise AI budget visibility, model-routing, and unmanaged token-spend examples.
- [27] openDesk GitLab, **Deployment automation and openDesk docs, technical workflow**. Used for Helm/Helmfile-based Kubernetes deployment readiness and implementation requirements.
- [28] Open-Xchange/OX, **Open platform for business communication**. Used for Open-Xchange email, calendar, collaboration, public-sector, and control positioning.
- [29] Mistral Docs, **Vibe CLI install and setup**. Used for Mistral local/compatible API and developer-tool deployment context.

Drafting note: Before this becomes a final market asset, DCS should add a short legal/compliance review, replace generic cost assumptions with local reseller or customer-specific pricing where possible, and decide whether to use "data-resident" or "customer-controlled" as the primary headline frame.