DeskBridge Presentation Notes and Explanations

Briefing notes for the DeskBridge presentation

DeskBridge

2026-07-04

DeskBridge Presentation Notes and Explanations

These notes are for staff, partners and clients using the DeskBridge deck. They explain what each slide means, how to talk about each point, and where the service boundary or caveat sits. They are not a substitute for a signed service design, proposal or contract.

Slide 1 - Controlled workspaces for accountable digital work

Managed access, support records, data-handling boundaries and evidence for teams that need control.

One-line explanation: DeskBridge is positioned as a managed operating layer for access, support, data handling and evidence, not just a remote desktop.

Detailed explanation: This opening line sets the frame for the whole presentation. DeskBridge is not being sold as another isolated software tool. The value is that access, support, workspace use, data-handling rules and evidence are brought into one controlled service boundary. For a client, this means the conversation should move beyond “can people log in?” to “who is allowed in, what can they do, how is support handled, what happens when they leave, and what proof exists afterwards?” This slide explains that DeskBridge is strongest where accountability matters: regulated work, client material, contractor access, audit pressure, insurance questions, or management needing confidence that access and support are not informal.

Controlled access

One-line explanation: Users should have named, approved access rather than shared, informal or unmanaged access.

Detailed explanation: Controlled access means the client can identify who has access, why they have it, what role they hold, and when that access should end. This covers employee access, contractor access, management access and support access. It also means access can be reviewed, revoked and evidenced. If a client asks whether DeskBridge simply gives everyone a login, the answer is no: access should be assigned against a role, approval, business need and expiry where appropriate. This is especially important for contractors, external suppliers and staff handling confidential information.

Governed workspaces

One-line explanation: The workspace should operate inside agreed rules for applications, data

movement, support and user behaviour.

Detailed explanation: A governed workspace is a working environment where the client and DeskBridge agree what is supported, what is allowed, and what is outside scope. This can include approved applications, access routes, file transfer rules, clipboard policy, print controls, AI tool use, browser behaviour, backup expectations and escalation routes. The point is not to make the workspace restrictive for its own sake. The point is to make it supportable and auditable. If a user or manager asks why a control exists, readers can explain that it protects both the client and DeskBridge by making the operating model clear.

Operational evidence

One-line explanation: DeskBridge is designed to leave records that show what was approved, changed, supported and reviewed.

Detailed explanation: Operational evidence is the proof trail created by the service: onboarding scope, access approvals, support tickets, change notes, backup/restore checks, access reviews, contractor expiry checks and exception records. Clients often discover too late that they cannot prove who had access, when something changed, or whether a support action was authorised. DeskBridge is designed to make those records part of the service. The explanation is that the evidence is not just for technical teams; it can also support management, insurers, auditors, boards and client due diligence.

Slide 2 - The problem

Most organisations already have tools. What breaks down is authority, supportability and evidence.

One-line explanation: The problem is usually not a lack of software, but a lack of controlled operation and proof.

Detailed explanation: Many organisations already use Microsoft 365, web hosting, laptops, SaaS tools, file stores and messaging systems. The weakness is often that nobody can clearly prove who owns access decisions, what support has changed, what devices hold data, or what happens when a worker leaves. DeskBridge should not be presented as “we replace every tool you already have.” The stronger message is that DeskBridge wraps working environments with authority, supportability and evidence. This helps clients who already have tools but lack control over how those tools are accessed and supported.

Unmanaged laptops and local data

One-line explanation: Data stored on unmanaged devices creates risk because it is hard to control, support, back up or remove.

Detailed explanation: When staff or contractors work from unmanaged laptops, the client may not know where client files, downloads, browser sessions, cached credentials or exported reports are stored. If the device is lost, sold, infected, shared with family, or used after a contract ends, the client may struggle to prove control. DeskBridge reduces this risk by moving more work into controlled workspaces and agreed access routes. The explanation should avoid claiming that all device risk disappears; instead, explain that DeskBridge gives the client a better-supported boundary for the work that is in scope.

Shared accounts and informal access

One-line explanation: Shared accounts make accountability weak because actions cannot reliably be tied to a named person.

Detailed explanation: Shared accounts are common in small teams, admin functions and supplier

arrangements, but they create serious control problems. If several people know the same password, the client cannot confidently say who accessed data, sent a message, changed a setting or downloaded a file. Informal access also makes offboarding difficult because removing one person may affect everyone using the same account. DeskBridge positions named access and role ownership as the better operating model. If a client says shared access is convenient, readers should acknowledge that, then explain that convenience comes at the cost of accountability and evidence.

Contractors without clear expiry

One-line explanation: Contractor access should have a defined purpose, owner and end date.

Detailed explanation: Contractor and supplier access often starts for a valid reason but remains active after the project, invoice, or engagement has ended. This creates unnecessary exposure and makes later questions difficult to answer. DeskBridge supports the idea that contractor access should be named, approved, time-bound and reviewable. The explanation is that expiry is not only a security control; it is also a management control. It helps the client prove that external access is intentional, current and owned by someone inside the business.

Support changes without a durable record

One-line explanation: Support actions need records so clients can see what was changed, why, by whom and with what outcome.

Detailed explanation: In many businesses, support is handled through calls, messages or informal remote access. This may solve the immediate problem but leaves little durable evidence. Later, if a setting changed, a file moved, a user was added, or an incident occurred, the client may not know what happened. DeskBridge should be described as a service that expects support requests, changes and escalations to be recorded. The important point is that this protects the client and the support provider because actions can be reviewed rather than reconstructed from memory.

Named access and role ownership

One-line explanation: Every user and privileged role should have an identifiable owner and business reason.

Detailed explanation: Named access means each person uses their own identity, and role ownership means someone is accountable for why that access exists. This matters for normal users, managers, admins, contractors and support operators. It supports access reviews, offboarding, incident response and audit questions. If a client asks whether DeskBridge can mirror their existing messy access model, the answer should be that DeskBridge can review it, but the goal is to move towards named, owned and supportable access.

Workspace boundaries that can be supported

One-line explanation: DeskBridge needs a clear boundary so support can be reliable and commitments can be honest.

Detailed explanation: A supportable workspace boundary defines which applications, users, devices, data flows and support routes are in scope. Without this, expectations become unclear: users may assume every app, every device, every data store and every third-party issue is covered. DeskBridge should be sold as a managed service with defined boundaries, not an unlimited promise. This lets the client know what is included, what needs separate approval, and what requires redesign before deployment.

Offboarding and revocation evidence

One-line explanation: Clients need proof that leavers, contractors and expired access were removed

properly.

Detailed explanation: Offboarding is one of the clearest points where evidence matters. A client may need to prove that an employee, contractor or supplier no longer had access after a specific date. DeskBridge can support this with access removal records, expiry checks, review packs and support tickets. The explanation is that the value is not just removing access; it is being able to show that access was removed, when it was removed, and under whose instruction or policy.

Clear proof when challenged

One-line explanation: DeskBridge aims to give clients evidence they can use when a client, auditor, insurer or board asks questions.

Detailed explanation: Clients are increasingly asked to prove how they control data, access and support. Verbal assurances are often not enough. DeskBridge's evidence model is designed to help the client respond with records: access reviews, change logs, support tickets, backup/restore checks, exceptions and caveats. The wording should make clear that evidence depends on the agreed service design and the controls actually implemented. DeskBridge should not promise proof for processes that the client keeps outside the service boundary.

Slide 3 - Operating model

One accountable service boundary around people, devices, access, support, data and evidence.

One-line explanation: DeskBridge brings the main operating risks into one managed boundary instead of leaving them scattered.

Detailed explanation: This slide explains how DeskBridge should be understood commercially and operationally. Rather than treating identity, devices, access, support, data movement and evidence as separate problems, DeskBridge creates a single service boundary around them. That boundary makes responsibilities clearer: what DeskBridge manages, what the client approves, what users can do, and what evidence is produced. Readers should use this slide to explain why DeskBridge is different from buying licences or hosting alone.

Identity, MFA, roles, expiry and revocation

One-line explanation: Access control starts with named identities, stronger authentication, role assignment, expiry dates and removal.

Detailed explanation: This point covers the core access lifecycle. A user should be known, authenticated, assigned to an appropriate role, reviewed over time and removed when no longer needed. MFA and FIDO2 direction strengthen authentication, while expiry and revocation reduce stale access. The explanation should avoid saying every client will have the same authentication model from day one. The correct message is that these controls are selected and implemented as part of the service design and maturity path.

Approved applications and controlled sessions

One-line explanation: Users should work through approved applications and sessions that the service can support and evidence.

Detailed explanation: Approved applications are applications that have been reviewed for the client's use case, support needs and data-handling rules. Controlled sessions mean the way users connect and work is governed by policy rather than left entirely to local device behaviour. This makes support easier

and reduces uncontrolled data movement. If a client wants a new app, readers should explain that DeskBridge can assess and onboard it, but unsupported applications should not be assumed to be covered automatically.

Clipboard, file, print and AI handling by policy

One-line explanation: Data movement controls should be explicit rather than left to user habit or device defaults.

Detailed explanation: Clipboard, file transfer, printing and AI use are common ways sensitive information leaves a controlled environment. DeskBridge can apply policy around those behaviours, such as allowing, restricting, logging or requiring approval depending on the client model. This is especially relevant for professional services, contractors and AI-assisted workflows. The trade-off is: tighter controls can reduce risk and improve evidence, but may require user training and careful setup to avoid frustrating legitimate work.

Ticketed changes and traceable actions

One-line explanation: Changes should be requested, approved, carried out and recorded in a way that can be reviewed later.

Detailed explanation: A ticketed change creates a durable record of the request, approval, action, result and any exception. This matters for access changes, application changes, support actions, recovery events and administrative work. Traceability does not mean every action becomes bureaucratic; it means important changes are not invisible. The explanation is that this helps clients avoid “nobody knows who changed it” situations and supports evidence for audits, insurers and management.

Access, support, change and backup review packs

One-line explanation: DeskBridge can produce review packs that summarise key operational controls and evidence.

Detailed explanation: Review packs are structured evidence outputs. They may include access lists, expired contractor access, support records, change records, backup checks, restore checks, open risks and exceptions. The exact content depends on the package and service scope. The explanation is that these packs give managers a practical way to review the service and demonstrate control. They should not claim that every possible audit requirement is automatically satisfied; the pack supports assurance but does not replace a formal audit.

Client-safe records for audits, insurers and boards

One-line explanation: Evidence should be useful to non-technical stakeholders without exposing unnecessary internal detail.

Detailed explanation: Client-safe records are designed to give the client usable information without revealing secrets, internal infrastructure detail, tokens, private keys or other tenants’ information. This matters when records are shared with boards, insurers, auditors or external clients. The explanation is that DeskBridge aims to separate operational evidence from sensitive internal implementation detail. If deeper technical evidence is needed, that should be handled through an agreed disclosure process.

Slide 4 - Service fit

Best fit is where access, support and evidence matter as much as the desktop itself.

One-line explanation: DeskBridge is strongest where control and proof are business requirements, not

optional extras.

Detailed explanation: This slide qualifies the opportunity. DeskBridge is not only about giving someone a desktop. It is about giving the client a controlled way to operate work where access, support and evidence matter. This slide helps avoid forcing DeskBridge into poor-fit opportunities. The best clients will recognise the value of managed access, support records, data-handling rules and evidence. If a client only wants the cheapest possible remote access, they may not understand or value the service.

Professional services handling client material

One-line explanation: Professional firms need controlled handling of client files, communications and privileged access.

Detailed explanation: Accountants, consultants, legal teams, advisors and similar firms often handle sensitive client material. They may need to show that only authorised people can access it, that support is controlled, and that data is not scattered across unmanaged devices. DeskBridge fits because it can create a governed workspace and evidence model around that work. For client trust, the firm can better answer questions from its own clients about how access and support are managed.

Contractor-heavy teams with access expiry risk

One-line explanation: Teams using contractors need access that starts cleanly, ends cleanly and can be proven afterwards.

Detailed explanation: Contractor-heavy teams often have fast-moving access needs. People join projects, need access quickly, then leave or change role. Without clear ownership and expiry, access can remain active long after it is needed. DeskBridge is well suited to this because contractor access can be treated as a managed lifecycle: named user, role, approval, workspace, expiry, support route and revocation evidence. This should be positioned as operational control, not just cybersecurity.

Sensitive data workflows adopting AI cautiously

One-line explanation: AI use needs clear rules about which users, tools and data are allowed.

Detailed explanation: Many organisations want the productivity benefits of AI but are concerned about sensitive data leaving the business or being entered into unapproved tools. DeskBridge can help by wrapping AI-adjacent workflows with access control, approved tool lists, data-handling records, support tickets and evidence. The wording must not imply a partnership with any AI provider unless one exists. The message is that DeskBridge helps govern access and data handling around AI use.

Uncontrolled BYOD as the primary model

One-line explanation: DeskBridge is less suitable if the client insists that unmanaged personal devices remain the main control point.

Detailed explanation: Bring-your-own-device can be workable in some environments, but uncontrolled BYOD makes support, data control and evidence difficult. If the client wants all work to happen on unmanaged personal devices with no meaningful controls, DeskBridge cannot honestly provide the same assurance. The explanation is that DeskBridge can support access from different devices, but the protected work should happen through controlled workspaces and agreed policies. If BYOD remains central, the client may need redesign or a reduced assurance claim.

Informal shared-account working

One-line explanation: DeskBridge should not be positioned around shared passwords and informal account use.

Detailed explanation: Shared accounts undermine the evidence model because actions cannot be reliably tied to a named person. If a client refuses to move away from shared-account working, DeskBridge's ability to provide strong access evidence is limited. This should not be treated as normal. The risk should be explained, named access and role-based alternatives should be proposed, and any client exception should be recorded. This protects the service from making unsupported claims.

Projects needing unsupported sovereignty claims

One-line explanation: DeskBridge should only make sovereignty, residency or compliance claims that are supported by the signed design.

Detailed explanation: Some clients may want strong claims about national sovereignty, zero access, regulatory compliance or exclusive jurisdiction. These claims are sensitive and must be accurate. DeskBridge can discuss data residency, key custody, controlled access and regional operating models, but final claims depend on where services are hosted, who operates them, which key model is selected, which support route exists and what contract is signed. Readers must avoid implying government endorsement, guaranteed compliance or absolute sovereignty unless formally approved and evidenced.

Slide 5 - Data access assurance

Data residency answers where data is stored. Key custody answers who can decrypt protected data.

One-line explanation: Where data lives and who can decrypt it are related but separate questions.

Detailed explanation: Clients often ask "where is our data stored?" and assume that answers the whole security question. Data residency addresses location and jurisdiction. Key custody addresses who has the technical ability to decrypt protected data. A client can have data in a chosen region but still use provider-managed keys, or can hold keys themselves and accept operational limitations. Readers should use this slide to slow the conversation down and separate location, access, recovery and support trade-offs.

DeskBridge Managed Keys

One-line explanation: DeskBridge manages encryption and recovery controls as part of the service.

Detailed explanation: In the managed-key model, DeskBridge can provide normal managed-service support, recovery, migration and operational assistance because it has the necessary controlled ability to operate the environment. This is often the practical fit for smaller clients or clients that want DeskBridge to take responsibility for service continuity. It does not mean access is uncontrolled. It means privileged access must be governed by role control, approval, logging, support records and lawful operating requirements.

Best for normal managed-service support.

One-line explanation: This model works best when the client wants DeskBridge to support and recover the service without constant key-release steps.

Detailed explanation: Managed keys are operationally efficient. If a user needs recovery, a migration is needed, or an incident requires technical action, DeskBridge can respond through authorised procedures. The explanation is that this is the most straightforward managed-service model, but it has a caveat: the client is trusting DeskBridge's controls, staff processes, audit trail and contractual obligations. It is not the right model for a client demanding that DeskBridge has no technical ability to access protected data.

Caveat: DeskBridge may technically access protected service data for authorised support, recovery or lawful operation.

One-line explanation: The managed-key model carries a privileged-access caveat that must be disclosed.

Detailed explanation: This caveat is important. If DeskBridge operates the keys and support layer, there may be scenarios where authorised personnel could technically access protected service data. That access should be limited, approved, logged and justified by support, recovery, migration, security or lawful operation. The document must not tell clients “nobody at DeskBridge can ever access your data” when discussing managed keys. The honest answer is that access is controlled and auditable, not technically impossible.

Customer-Controlled Keys

One-line explanation: The client controls key release decisions while DeskBridge operates around that approval model.

Detailed explanation: Customer-controlled keys create a stronger client approval boundary. DeskBridge may operate the service, but protected data access depends on the client releasing or authorising key use. This can be a good balance for clients that want more control but still need managed-service support. The explanation is that this model needs process discipline: who can approve key release, how approvals are recorded, what happens in an emergency, and how delays affect recovery or support.

Best where clients approve protected data access.

One-line explanation: This model fits clients that want DeskBridge to ask before protected data can be accessed.

Detailed explanation: Some clients will be comfortable with DeskBridge managing the platform but want their own nominated administrators or management to approve access to protected data. This is particularly relevant for sensitive client files, board material, legal data, regulated workflows or higher-assurance clients. The explanation is that the client takes on an active role in access governance. The benefit is stronger control; the trade-off is that support and recovery may depend on client availability.

Caveat: restore, migration, search and incident response may require client key release.

One-line explanation: Some service actions may be delayed or limited until the client releases the required key.

Detailed explanation: Encryption protects data, but it also affects operations. Restoring data, migrating files, indexing/searching content, investigating an incident or supporting a user may require temporary access to protected data. In a customer-controlled model, DeskBridge may not be able to complete those actions until the client approves key release. This should be presented as a trade-off, not a flaw. The client gets stronger custody control but must accept responsibility for timely approvals and recovery planning.

Customer-Held / Zero-Knowledge Keys

One-line explanation: The client holds the keys so DeskBridge cannot decrypt protected data in normal operation.

Detailed explanation: Customer-held or zero-knowledge key models provide the strongest custody boundary. DeskBridge may host, connect or operate surrounding services, but cannot decrypt protected data without the client’s key material. This model is attractive for highly sensitive data or clients with strict custody requirements. It must be clear that zero-knowledge applies only to the protected data and design in scope. Metadata, operational logs, identity records or unencrypted workflows may still exist

depending on the service design.

Best for the strongest custody boundary.

One-line explanation: This model is for clients who value data custody separation above convenience.

Detailed explanation: Customer-held keys are appropriate when the client's priority is preventing provider-side access to protected data. It may suit board-level material, highly sensitive professional records, strict contractual controls or future high-assurance environments. The explanation is that this is a stronger boundary but not always the best default. If the client expects DeskBridge to recover everything quickly, search all content, migrate data on demand and investigate incidents independently, zero-knowledge may conflict with those expectations.

Caveat: lost keys may mean unrecoverable data; some server-side features may be unavailable.

One-line explanation: If the client loses the keys, DeskBridge may not be able to recover the protected data.

Detailed explanation: This is the main zero-knowledge trade-off. Strong custody means DeskBridge cannot bypass the client's key control. If keys are lost, destroyed or withheld, protected data may be permanently unrecoverable. Some features may also be reduced because the server cannot read protected content. Examples can include server-side search, content inspection, automated migration, certain backup validation methods and some incident response actions. The explanation is that key safes, recovery procedures and client governance are essential if this model is selected.

Slide 6 - AI and sensitive data

DeskBridge can wrap AI and sensitive-data workflows with access control, approvals, support records and evidence.

One-line explanation: DeskBridge helps clients govern how people use sensitive data and AI-related workflows.

Detailed explanation: This slide positions DeskBridge as a control layer around AI and sensitive work, not as a claim of owning or endorsing a specific AI platform. The value is that users, contractors, tools, data movement and exceptions can be handled through access control, approval records and evidence. The explanation is that many AI risks are human workflow risks: who copied data, who approved the tool, which dataset was used, and what record exists afterwards. DeskBridge helps create the operating discipline around those questions.

User and contractor access to governed workflows

One-line explanation: AI and sensitive workflows should be limited to named users and contractors with approved access.

Detailed explanation: Sensitive workflows become risky when anyone can access them informally. DeskBridge can help place those workflows behind named access, roles, MFA direction, contractor expiry and supportable workspace boundaries. This helps the client prove who was allowed to use the workflow and under what conditions. The explanation is that access governance is often the first step before discussing advanced AI controls.

Approved tool and data-handling records

One-line explanation: Clients need records of which tools are approved and how data is allowed to be

handled.

Detailed explanation: Organisations may use AI tools, web tools, SaaS platforms, file-sharing services and internal systems. The risk is not just the tool itself; it is whether the client has approved its use for specific data. DeskBridge can support approved-tool lists, data-handling rules and evidence of exceptions. The explanation is that this gives management a clear answer when staff ask “can I use this tool with this data?”

Role, expiry and exception evidence

One-line explanation: Sensitive workflow access should show who had access, when it expired and which exceptions were approved.

Detailed explanation: Role, expiry and exception evidence helps the client demonstrate control over sensitive workflows. Roles show why access exists. Expiry prevents stale access. Exceptions record where normal policy was adjusted and who approved it. This is especially useful for contractors, temporary projects, restricted datasets and AI trials. This should be positioned as practical governance rather than abstract compliance.

Client-controlled key options where required

One-line explanation: Higher-sensitivity workflows can use stronger key custody if the client accepts the operational trade-offs.

Detailed explanation: For some AI or sensitive-data workflows, the client may want DeskBridge to have limited or no ability to decrypt protected data. Customer-controlled or customer-held keys can support that direction. This links back to slide 5: stronger key custody can improve assurance, but may limit support, search, migration, restore and incident response. The right model should be chosen during service design, not improvised during a client discussion.

No implied partnership or endorsement

One-line explanation: DeskBridge should not imply a partnership with an AI vendor, government body or third party unless formally agreed.

Detailed explanation: This protects DeskBridge from overstating relationships. The discussion should cover capabilities and operating controls, not imply endorsement by another organisation. If a client asks whether DeskBridge is partnered with a named AI company, cloud provider or government project, the answer should be factual and limited to what is formally agreed. The service can support governance around tools without claiming ownership, partnership or endorsement.

No unsupported sovereignty or compliance claims

One-line explanation: Sovereignty and compliance claims must match the actual signed architecture and control model.

Detailed explanation: AI and sensitive-data discussions can easily move into strong claims about sovereignty, regulation, residency or zero access. Claims must stay tied to evidence. DeskBridge can design for data residency, access control, key custody and evidence, but final claims depend on the client’s selected model, region, hosting, support route and contractual terms. Unsupported claims create commercial and legal risk.

Final scope depends on signed service design

One-line explanation: The presentation explains capability direction; the contract defines the actual service.

Detailed explanation: Every client environment is different. Users, applications, data sensitivity, support requirements, key custody and reporting expectations must be confirmed in a service design before DeskBridge commits to specific controls. Readers should use this point whenever a client asks “will it definitely do X?” The correct response is that DeskBridge can assess and design for the requirement, then confirm it in writing if it is supportable.

Unsafe shortcuts are refused and recorded

One-line explanation: DeskBridge should not silently accept unsafe workarounds that undermine the control model.

Detailed explanation: Clients may ask for quick fixes such as shared accounts, bypassing MFA, unmanaged exports, unrestricted contractor access or undocumented support changes. DeskBridge’s position is that unsafe shortcuts should either be refused or formally recorded as exceptions with risk ownership. The explanation is that this is part of the value: DeskBridge is not just there to say yes; it is there to help the client operate responsibly.

Slide 7 - Client outputs

The service is designed to leave management evidence, not just a working login.

One-line explanation: DeskBridge output includes records and review material, not only access to a desktop.

Detailed explanation: A working login is necessary, but it is not enough for clients who need control. DeskBridge aims to produce useful operational evidence: onboarding decisions, access records, support tickets, change records and periodic review packs. Readers should use this slide to explain why DeskBridge is a managed service. The client receives an operating model and evidence trail, not merely credentials.

Onboarding scope

One-line explanation: Onboarding defines what DeskBridge is responsible for before the service goes live.

Detailed explanation: Onboarding scope records users, roles, applications, data locations, devices, suppliers, access routes, support contacts, key custody choices and exclusions. This prevents misunderstandings later. The explanation is that discovery and onboarding are part of the control model. If something is not scoped, it may not be supported or evidenced.

Users, roles, applications, data, devices and key custody decisions.

One-line explanation: These are the main design decisions that shape the client’s DeskBridge service.

Detailed explanation: Each listed item affects risk and support. Users determine identity and access. Roles determine permissions. Applications determine compatibility and support. Data determines handling rules and backup. Devices determine connection assumptions. Key custody determines who can decrypt protected data and how recovery works. The explanation is that these decisions are made deliberately so DeskBridge can provide a reliable and honest service.

Controlled access

One-line explanation: The client should be able to see and review who has access and why.

Detailed explanation: Controlled access is both a technical and management output. The client should

know which users exist, which roles they hold, who approved them, whether MFA direction applies, and when access expires. This supports offboarding and review. The explanation is that access control is not a one-time setup; it is part of ongoing service operation.

Named users, roles, approvals, MFA direction and expiry

One-line explanation: These elements turn access from an informal login into a governed lifecycle.

Detailed explanation: Named users create accountability. Roles keep permissions aligned with business need. Approvals show authority. MFA direction strengthens identity assurance. Expiry reduces stale access. Together, these controls create a managed access lifecycle. Readers should be ready to explain each element in plain terms and relate it to common client risks such as leavers, contractors, shared passwords and privilege creep.

Support record

One-line explanation: Support should leave a record of request, action, outcome and escalation.

Detailed explanation: A support record gives the client and DeskBridge a shared view of what happened. It can cover user issues, access requests, application problems, recovery actions, incidents and changes. This helps avoid disputes and supports management review. Readers should emphasise that support records are a feature of the service, not an administrative burden.

Ticketed requests, change notes, outcomes and escalation evidence.

One-line explanation: The important parts of support should be captured in a durable, reviewable form.

Detailed explanation: Ticketed requests show what was asked. Change notes show what was altered. Outcomes show whether the issue was resolved. Escalation evidence shows when something needed higher attention or client approval. This structure is valuable when a client later asks why something changed, how long it took, or whether a request was authorised. It also helps DeskBridge improve service quality over time.

Monthly evidence

One-line explanation: Monthly evidence gives management a regular view of access, risk and operational health.

Detailed explanation: Monthly evidence is intended to turn operations into a reviewable management rhythm. Depending on scope, it can include access review, contractor expiry, backup/restore checks, open support patterns, risks, exceptions and recommendations. The explanation is that the exact pack depends on package and service design, but the principle is that the client should not have to wait for a crisis to understand their control position.

Access review, contractor expiry, backup/restore and risk summary

One-line explanation: These checks help clients see whether the service is still controlled and supportable.

Detailed explanation: Access review checks who still has access. Contractor expiry checks whether temporary access should end. Backup/restore checks give confidence that recovery is not only assumed. Risk summary highlights known issues, exceptions and decisions needed. The explanation is that these are practical management controls. They help clients show they are actively managing the environment rather than trusting that everything is fine.

Slide 8 - Next step

DeskBridge confirms fit before deployment: users, access risk, applications, data handling, support needs and evidence expectations.

One-line explanation: DeskBridge should not be deployed properly until the operating scope and risks are understood.

Detailed explanation: The final slide turns the discussion into an action. Before deployment, DeskBridge needs to understand who will use the service, what risks exist, which applications matter, how data is handled, what support is expected and what evidence the client needs. This slide moves the client towards a workspace review rather than promising a generic setup. This protects both sides and produces a better proposal.

Confirm operating scope and client responsibilities

One-line explanation: The client and DeskBridge must agree what is included and what the client remains responsible for.

Detailed explanation: Operating scope defines DeskBridge responsibilities, client responsibilities, supported users, supported apps, data boundaries, support hours, escalation routes, exclusions and dependencies. The client may still be responsible for internal approvals, user behaviour, legal decisions, key custody, third-party licences or data classification. The explanation is that clear responsibilities prevent later confusion and make the service supportable.

Select the data access assurance model

One-line explanation: The client must choose the right balance between support convenience and key custody control.

Detailed explanation: The data access assurance model determines whether DeskBridge manages keys, the client controls key release, or the client holds keys in a stronger zero-knowledge model. This decision affects recovery, migration, search, incident response and support speed. Clients should understand the trade-offs and avoid treating the strongest sounding model as automatically the best. The right choice depends on risk, operations and tolerance for recovery limitations.

Map applications, users, suppliers and support routes

One-line explanation: DeskBridge needs to know who works where, with which tools, and how support should flow.

Detailed explanation: Mapping applications, users, suppliers and support routes creates the practical service design. It identifies what needs to be available, who needs access, which suppliers or contractors are involved, which systems are in scope, and who approves changes or support. This also exposes gaps before go-live, such as unsupported applications, unclear ownership or missing access expiry. This should be presented as a controlled onboarding step.

Produce a controlled proposal with caveats and evidence plan

One-line explanation: The proposal should state what DeskBridge will do, what it will not do, and what evidence will be produced.

Detailed explanation: A controlled proposal protects the client and DeskBridge by making commitments clear. It should include scope, pricing, responsibilities, exclusions, caveats, implementation steps, evidence outputs and any dependency on client decisions. Readers should avoid vague proposals that promise everything. A strong DeskBridge proposal is commercially clear and operationally honest.

Commercially clear proposal

One-line explanation: The client should understand pricing, scope, setup effort and ongoing service commitments.

Detailed explanation: Commercial clarity means the client knows what they are buying, what is included, what costs extra and what assumptions pricing depends on. It reduces the risk of later disputes or margin loss. It should be clear that pilot pricing, discounted pricing or at-cost deployments are clearly framed as such and not accidentally presented as the normal full-service value.

Confirmed caveats and exclusions

One-line explanation: Any limits, dependencies or unsupported areas should be written down before deployment.

Detailed explanation: Caveats and exclusions are not negative; they are part of responsible service design. They might include unsupported apps, client-held key recovery risk, unmanaged device limitations, third-party dependencies, compliance boundaries or support-hour limits. The explanation is that documenting exclusions helps avoid unsupported claims and protects the client from assuming controls exist where they do not.

Evidence plan before deployment

One-line explanation: The client should know what evidence they will receive before the service starts.

Detailed explanation: Evidence should not be an afterthought. Before deployment, the client should understand what access records, support records, review packs, backup evidence, audit records or assurance outputs will be produced. This allows management, auditors or insurers to confirm whether the evidence meets their needs. Readers should use this point to connect the commercial proposal to the client's governance requirements.

Supportable operating boundary

One-line explanation: DeskBridge should only commit to a service boundary that can be operated, supported and evidenced.

Detailed explanation: The supportable operating boundary is the final discipline in the review process. It defines where DeskBridge can confidently deliver, what needs redesign, and what should be excluded. This boundary prevents overpromising and gives the client a realistic service. The closing message is: DeskBridge is strongest when the client wants a controlled, accountable, evidence-backed operating model rather than an informal collection of tools.

Slide 9 - DeskBridge Helpdesk

Support becomes part of the control boundary

One-line explanation: DeskBridge includes helpdesk capability, but the stronger value is that support is connected to the workspace, access, approval and evidence model.

Detailed explanation: This slide answers the question "is DeskBridge also a helpdesk?" The correct answer is yes, but not only a helpdesk. A normal helpdesk records problems and support requests. DeskBridge connects support to the managed working environment: the user, workspace, endpoint, access state, policy, approval record, change history and audit evidence. This makes support more valuable because it becomes part of the controlled operating model rather than a separate ticket queue.

Traditional helpdesk

One-line explanation: A traditional helpdesk usually records the issue, owner, status and closure.

Detailed explanation: Traditional helpdesk systems are useful because they create a support record. They can normally show who raised an issue, what the problem was, who handled it and whether it was closed. That is helpful, but it often starts after something has gone wrong and may not connect to the wider security or access context. It may not prove whether the user was authorised, which workspace was involved, what policy applied, whether a change needed approval, or whether the action affected data movement or permissions.

DeskBridge helpdesk

One-line explanation: DeskBridge helpdesk links support activity to users, workspaces, endpoints, access, changes and client-safe evidence.

Detailed explanation: DeskBridge helpdesk is part of the managed service boundary. A support request can be linked to the user, tenant, workspace, endpoint, access policy, approval requirement, change action and final evidence record. This matters for small companies because it replaces informal IT support with a more professional managed route. It matters for larger companies because it supports governance, compliance, security review, contractor management and management reporting. It matters for government and regulated organisations because support becomes a recorded, authorised and reviewable action inside a controlled environment.

Client-safe evidence for audits and management

One-line explanation: Helpdesk records can support audit, management review and client assurance without exposing unnecessary internal detail.

Detailed explanation: DeskBridge helpdesk evidence should be useful to management, auditors, insurers and authorised client administrators. The client should be able to see support status, request history, change outcomes and relevant evidence without seeing passwords, tokens, raw logs, private infrastructure detail or another tenant’s data. This is the same principle used across DeskBridge: evidence should prove control while protecting sensitive operational detail.