



PLAYBOOK

# Le Playbook de la Data Room PME

Construire une salle de données contrôlée, traçable et révocable pour la due diligence.

LANGUE

**FR**

STATUT

**RELEASE CANDIDATE**

EVIDENCE CUTOFF

**24 September 2026**

REFERENCE

**P03**

# Le Playbook de la Data Room PME

## Objectif

Construire une VDR qui permet la diligence **sans transformer la confidentialité en chaos opérationnel**.

Le résultat attendu est un espace où chaque document possède un propriétaire, une version, un niveau d'accès et une trace d'utilisation.

## 1. Workflow

Classify -> Prepare -> NDA -> Grant -> Review -> Q&R -> Update -> Revoke/Expire -> Evidence export

| Gate | Question                                | Sortie                           |
|------|-----------------------------------------|----------------------------------|
| V0   | Quel type d'information existe ?        | classification T0/T1/T2          |
| V1   | Le dossier est-il prêt ?                | index + owners + versions        |
| V2   | La contrepartie peut-elle accéder ?     | NDA + qualification + permission |
| V3   | Le périmètre est-il proportionné ?      | ACL + expiry + download policy   |
| V4   | La diligence est-elle traçable ?        | Q&R + logs + issues              |
| V5   | L'accès peut-il être fermé proprement ? | revoke + evidence pack           |

## 2. Structurer les dossiers par question de diligence

Une architecture utile peut couvrir : corporate, finance, tax, commercial, contracts, people, assets/operations, technology/cyber, permits/compliance, transaction documents.

Ne créez pas 100 dossiers vides. La structure doit suivre la complexité réelle du dossier.

## 3. Index documentaire minimum

Chaque ligne : document\_id, title, domain, owner, source\_date, version, evidence\_status, tier, download\_allowed, access\_group, expiry, supersedes.

## 4. Permissions

Principe deny by default.

Rôles typiques : seller core team, buyer core team, buyer advisers, expert scoped, clean team, compliance. Un administrateur technique n'a pas de droit de lecture métier par défaut.

## 5. Sécurité

ISO/IEC 27001 fournit un cadre de gestion de la confidentialité, intégrité et disponibilité. Pour une VDR : chiffrement en transit/au repos, MFA/SSO lorsque disponible, ACL, logs, sauvegarde, résilience, protection contre malware et contrôle du téléchargement.

Ne revendiquez aucune certification que la plateforme n'a pas effectivement obtenue.

## 6. Q&R

Chaque question reçoit : ID, document lié, domaine, auteur, date, priorité, réponse, source de réponse, statut et owner.

Transformer en issue lorsque la réponse révèle un risque matériel ou une contradiction.

## 7. Révocation

Tester la révocation avant d'ouvrir le deal. La propagation doit couvrir : session active, URL courte, téléchargement si contrôlable, index de recherche, accès expert, et couche IA permission-aware.

## 8. Clean Team

Utiliser seulement lorsqu'une information requiert un périmètre séparé. Le protocole doit définir membres, données, finalité, durée et format de restitution.

## 9. Low bandwidth

Prévoir : PDF optimisé, viewer progressif, pagination, reprise, possibilité d'afficher metadata avant contenu lourd, pas de dépendance à la vidéo.

## 10. Checklist avant ouverture

- NDA exécuté.
- Buyer/adviser group validé.
- Information owner nommé.
- Folder ACL reviewed.
- Downloads policy reviewed.
- Expiry set.
- Watermark/redaction where needed.
- Q&R ready.
- Audit log active.
- Revocation test passed.
- AI access constrained to current permissions.

## 11. Stop conditions

Pas d'ouverture si : lien public ; NDA manquant ; propriétaire du VDR non identifié ; données personnelles massives non minimisées ; malware non traité ; document T2 exposé à un groupe non autorisé ; révocation non testée.

## 12. Mapping DealPME

P11 produit la preuve NDA ; P12 gouverne le VDR. Le vendeur définit le périmètre ; l'accès reste révocable ; DealLens ne doit jamais connaître plus que l'utilisateur courant.

## 13. Classification pratique de l'information

| Classe            | Exemple                                    | Traitement par défaut                    |
|-------------------|--------------------------------------------|------------------------------------------|
| T0 / public-safe  | secteur, zone large, ordre de grandeur     | peut être exposé selon règles produit    |
| T1 / anonymisé    | finance anonymisée, profil plus riche      | contreparties selon gate                 |
| T2 / confidentiel | identité, prix, termes, VDR                | NDA + qualification + permission         |
| Restricted        | secrets, données personnelles, concurrence | redaction / clean team / accès nominatif |

La classification ne doit pas être déduite seulement du dossier. Elle doit être portée par metadata et contrôlée côté serveur.

## 14. Folder architecture de référence

1. Corporate & ownership
2. Financial information
3. Tax
4. Commercial / customers
5. Material contracts
6. People / management
7. Assets / operations
8. Technology / cybersecurity
9. Permits / compliance / litigation
10. Transaction documents

Chaque dossier doit avoir un owner et un statut de complétude. Les sous-dossiers sont créés uniquement lorsque le volume le justifie.

## 15. Document quality controls

Avant publication d'un document : vérifier lisibilité, version, signature lorsque pertinente, date/source, absence de malware, statut de redaction, tier d'accès, propriétaire, supersession et lien avec la demande de diligence.

Un fichier intitulé `final_v7_new.pdf` n'est pas une preuve gouvernée. Le nom visible peut rester lisible, mais le système doit conserver un ID stable et l'historique des versions.

## 16. Permission Lens

Pour chaque accès sensible, l'utilisateur doit pouvoir comprendre : **pourquoi l'accès est accordé, à quelles pièces, jusqu'à quand, avec quelle politique de téléchargement et quelle personne l'a autorisé**. Un refus réglementaire doit être distingué d'un simple manque de permission.

## 17. Q&R operating model

Définir SLA interne, responsabilité de réponse, reviewer et règle de publication. Une réponse destinée à un groupe d'acquéreurs ne doit pas être automatiquement visible à tous les autres groupes. Les réponses qui modifient une information matérielle doivent provoquer la mise à jour de la source ou une note explicite.

## 18. Contrôle des versions

Une nouvelle version d'un document doit : recevoir un nouveau numéro/version ; garder le lien vers la version remplacée ; préserver l'audit des consultations antérieures ; notifier les utilisateurs autorisés si le changement est matériel ; mettre à jour les analyses/IA futures.

## 19. Plan de révocation

Tester au minimum : utilisateur individuel, groupe, expert temporaire, URL déjà ouverte, document remplacé, session active, compte suspendu, fin de NDA/mandat, expiration automatique et retrait d'un fichier. L'équipe doit connaître le délai cible de propagation et savoir où consulter la preuve.

## 20. Incident playbook

En cas d'accès indu ou fuite suspectée : suspendre l'accès concerné, préserver les logs, notifier sécurité/conformité, qualifier les données touchées, appliquer le plan juridique/notification applicable, corriger la permission, documenter les actions et vérifier que les couches IA/index ne continuent pas à exposer la source.

## 21. Checklist de clôture du VDR

- accès externes expirés/révoqués selon politique ;
- Q&R exportée et archivée ;
- documents de closing identifiés ;
- versions finales figées ;
- logs conservés selon politique ;
- données personnelles traitées selon obligations ;
- obligations post-closing assignées ;
- accès des experts terminés ;
- preuve de clôture du data room documentée.

# Outil de travail — Document Index

Imprimez ou complétez ce tableau pendant le processus. Les champs vides sont intentionnels : ils doivent être renseignés à partir de preuves ou de décisions propres au dossier.

## Ligne 1

|                  |    |
|------------------|----|
| document_id      |    |
| title            |    |
| domain           |    |
| owner            |    |
| source_date      |    |
| version          |    |
| evidence_status  |    |
| tier             | T2 |
| download_allowed | NO |
| access_group     |    |
| expiry           |    |
| supersedes       |    |

# Outil de travail — Qa Register

Imprimez ou complétez ce tableau pendant le processus. Les champs vides sont intentionnels : ils doivent être renseignés à partir de preuves ou de décisions propres au dossier.

## Ligne 1

|               |      |
|---------------|------|
| question_id   |      |
| document_id   |      |
| domain        |      |
| question      |      |
| asked_by      |      |
| asked_date    |      |
| priority      |      |
| answer        |      |
| answer_source |      |
| owner         |      |
| status        | OPEN |

# Sources, méthodologie et limites

Les sources ci-dessous soutiennent les règles, méthodes ou éléments de contexte utilisés dans ce playbook. Elles ne transforment pas le document en avis juridique, fiscal, financier, de valorisation ou d'investissement.

---

## **ISO/IEC 27001:2022 - Information security management systems**

Éditeur: ISO · Niveau: Tier 3/standard

Utilisation: Information security principles, including confidentiality, integrity and availability.

<https://www.iso.org/standard/27001>

---

## **Virtual data rooms for M&A: software, security and AI-powered deal platforms**

Éditeur: Datasite · Niveau: Tier 4

Utilisation: First-party description of VDR security, permissions and auditability in M&A.

<https://www.datasite.com/en/resources/insights/virtual-data-rooms-for-m-and-a>

---

## **DealPME governed product baseline - Core Build Pack and P04-P25 process reference**

Éditeur: DealPME · Niveau: Governed internal source

Utilisation: Product rules for RPS, T0/T1/T2, buyer qualification, NDA, VDR, LOI, diligence and human decision ownership.

Source interne gouvernée / Governed internal source