



PLAYBOOK

The SME Virtual Data Room Playbook

Build a controlled, auditable and revocable data room for due diligence.

LANGUAGE

EN

STATUS

RELEASE CANDIDATE

EVIDENCE CUTOFF

24 September 2026

REFERENCE

P03

The SME Virtual Data Room Playbook

Outcome

Build a VDR that enables diligence **without turning confidentiality into operational chaos**.

The target state is a workspace where every document has an owner, version, access tier and traceable usage history.

1. Workflow

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

Gate	Question	Output
V0	What information exists?	T0/T1/T2 classification
V1	Is the file ready?	index + owners + versions
V2	Can this counterparty access?	NDA + qualification + permission
V3	Is scope proportionate?	ACL + expiry + download policy
V4	Is diligence traceable?	Q&A + logs + issues
V5	Can access close cleanly?	revoke + evidence pack

2. Structure folders around diligence questions

A useful architecture may cover corporate, finance, tax, commercial, contracts, people, assets/operations, technology/cyber, permits/compliance and transaction documents.

Do not create 100 empty folders. Structure should reflect the real complexity of the file.

3. Minimum document index

Each row: document_id, title, domain, owner, source_date, version, evidence_status, tier, download_allowed, access_group, expiry, supersedes.

4. Permissions

Use deny by default.

Typical groups: seller core team, buyer core team, buyer advisers, scoped expert, clean team, compliance. A technical administrator does not receive business-document read access by default.

5. Security

ISO/IEC 27001 provides a management framework for confidentiality, integrity and availability. For VDR operations, consider encryption in transit/at rest, MFA/SSO where available, ACLs, logs, backup, resilience, malware protection and download control.

Never claim a certification the platform has not actually obtained.

6. Q&A

Each question should carry ID, linked document, domain, author, date, priority, answer, answer source, status and owner.

Convert it into an issue when the response reveals a material risk or contradiction.

7. Revocation

Test revocation before the deal opens. Propagation should cover active sessions, short-lived URLs, controllable downloads, search indexes, expert access and permission-aware AI.

8. Clean Team

Use only where information genuinely requires a separated perimeter. The protocol should specify members, data, purpose, duration and reporting format.

9. Low bandwidth

Use optimised PDFs, progressive viewing, pagination/resume, metadata before heavy content and no dependence on video.

10. Pre-opening checklist

- NDA executed.
- Buyer/adviser group approved.
- Information owner named.
- Folder ACL reviewed.
- Download policy reviewed.
- Expiry set.
- Watermark/redaction where needed.
- Q&A ready.
- Audit log active.
- Revocation test passed.
- AI constrained to current user permissions.

11. Stop conditions

Do not open where there is a public link, missing NDA, no VDR owner, unminimised bulk personal data, unresolved malware, T2 content visible to an unauthorised group, or untested revocation.

12. DealPME mapping

P11 creates NDA evidence; P12 governs VDR access. The seller defines scope, access remains revocable and DealLens must never know more than the current user.

13. Practical information classification

Class	Example	Default treatment
T0 / public-safe	sector, broad region, size band	may be exposed under product rules
T1 / anonymized	anonymized financial profile	gated counterparties
T2 / confidential	identity, price, terms, VDR	NDA + qualification + permission
Restricted	secrets, personal/competition-sensitive data	redaction / clean team / named access

Classification should not live only in folder names. It should be metadata-driven and enforced server-side.

14. Reference folder architecture

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

Each folder has an owner and completeness state. Subfolders are created only where complexity requires them.

15. Document quality controls

Before publication check readability, version, signature where relevant, date/source, malware status, redaction status, access tier, owner, supersession and link to the diligence request.

A file called `final_v7_new.pdf` is not governed evidence. The visible name can remain readable, but the system should maintain a stable ID and version history.

16. Permission Lens

For every sensitive grant the user should understand **why access exists, which documents it covers, when it expires, download policy and who authorized it**. A regulatory block must be distinguishable from ordinary permission denial.

17. Q&A operating model

Define internal SLA, answer owner, reviewer and publication rule. An answer to one bidder group must not automatically become visible to another. If an answer changes material information, update the source or add an explicit correction note.

18. Version control

A new version should receive a version number, link to the superseded file, preserve prior access audit, notify permitted users if material, and update future AI/search analysis.

19. Revocation plan

Test individual user, group, temporary expert, already-open URL, replaced document, active session, suspended account, end of NDA/mandate, automatic expiry and file withdrawal. The team should know the target propagation time and where the evidence is recorded.

20. Incident playbook

On suspected unauthorized access: suspend affected access, preserve logs, notify security/compliance, classify affected data, apply applicable legal/notification process, correct the permission, document actions and verify AI/index layers no longer expose the source.

21. VDR close-out checklist

- external access expired/revoked under policy;
- Q&A exported and archived;
- closing documents identified;
- final versions frozen;
- logs retained under policy;
- personal data handled under applicable obligations;
- post-close obligations assigned;
- expert access closed;
- data-room closure evidence recorded.

Working tool — Document Index

Print or complete this table during the process. Blank fields are intentional and should be completed using deal-specific evidence or decisions.

Row 1

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

Working tool — Qa Register

Print or complete this table during the process. Blank fields are intentional and should be completed using deal-specific evidence or decisions.

Row 1

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

Sources, methodology and limitations

The sources below support the rules, methods or context used in this playbook. They do not turn the document into transaction-specific legal, tax, financing, valuation or investment advice.

ISO/IEC 27001:2022 - Information security management systems

Publisher: ISO · Tier: Tier 3/standard

Use: 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

Publisher: Datasite · Tier: Tier 4

Use: 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

Publisher: DealPME · Tier: Governed internal source

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

Source interne gouvernée / Governed internal source