THOMSON REUTERS
PRACTICAL LAW™

Using a Virtual Data Room for an M&A Transaction

by Ashley Melidosian, iDeals Solutions Group, with Practical Law Corporate & Securities, with special thanks to Alexander Arbour

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-025-3524**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Practice Note highlighting key items for corporate counsel to consider when using a virtual data room (VDR). Topics covered include common VDR features and timing considerations and acquiring, setting up, populating and maintaining, and closing a VDR in a merger or acquisition transaction (M&A transaction).

Setting up a virtual data room (VDR), also called deal room or project room, and managing a transaction is a multifaceted task, involving sensitive data, multiple parties, and varying levels of access. However, following the steps outlined in this Note provides a solid foundation for corporate counsel to host a VDR for a merger or acquisition transaction (M&A transaction). In particular, breaking down the process into discrete tasks is a quick way to ensure that counsel is not forgetting anything crucial and that all applicable responsibilities have been delegated appropriately.

VDR Use in M&A Transactions

Usually, a VDR is a cloud-based document repository for storing and sharing sensitive information between businesses. For information on cloud computing and related legal and commercial considerations, see Practice Note, Cloud Computing: Understanding the Business and Legal Issues.

In an M&A transaction, VDRs are primarily used to facilitate the M&A due diligence review process (see Practice Notes, Due Diligence for Public Mergers and Acquisitions and Due Diligence of Private Mergers and Acquisitions).

Corporate attorneys are often tasked with hosting or advising a client on hosting a VDR during an M&A transaction. Although VDRs vary by provider and plan, the general process for hosting a VDR tends to be universal.

VDR Features

Specific VDR features depend on the provider and scope, size, and industry of the M&A transaction. All VDRs generally allow counsel to perform the following tasks:

- Upload and store the client's sensitive documents (see Populating the VDR With Files and Folders).
- Invite authorized users to the data room (see Inviting Parties to the VDR).
- Track user activity in the data room to determine level of interest (see Using a VDR Report).
- Restrict access to certain folders and files based on the user's authorization level.
- Control which users can view, print, or download specific data.
- Prevent users in the data room from seeing other parties.
- Watermark files for security purposes and to prevent duplication (see Customizing the VDR's Watermarks).

Most VDRs also include the following standard features:

- A customizable clickwrap agreement form of nondisclosure agreement (see Setting Up a Clickwrap NDA in a VDR).
- The ability to brand the VDR room (see Branding the VDR).
- A built-in question and answer or messaging platform to securely store and share questions and answers inside the data room.
- The ability to redact and update files.
- The ability to allow users to download files but later lose access to those files (for example, after the M&A transaction closes).

Speak to a senior team member or the client to determine if additional features may be helpful for the specific M&A transaction.

VDR Implementation Groundwork and Timeline

Before starting an M&A transaction, consider whether internal preparation of the client's folders and files is required. Depending on the workflow, counsel can handle this process in a VDR, either during the staging process or using a dedicated preparation folder (see Creating Folder Structure and Delegation of Uploads). The specific workflow depends on counsel's preference and the available features of the VDR.

Even if the VDR is fully populated and configured for the M&A transaction, it is not advisable to invite outside users (for example, potential buyers and their representatives) to the data room until completion of at least the following:

- Confirm with the client that it is ready to proceed to the due diligence stage of the M&A transaction.
- If the M&A transaction is an auction (the sale of a business where the seller seeks competing bids), send a teaser to invited bidders and wait until potential buyers have returned indications of interest based on the teaser. A teaser is a marketing document that gives a brief description of the business or target company that is for sale, often without identifying it, and highlights a few facts that make it an attractive acquisition. For additional information on seller considerations in auctions, see Practice Note, Auctions From the Seller's Perspective.
- Confirm receipt of a signed confidentiality or nondisclosure agreement (NDA) from all interested buyers (for an example, see Standard Document, Confidentiality Agreement: Mergers and Acquisitions).

After completion of these steps, access to the VDR may be granted to outside users, including potential buyers and their representatives.

Considerations for Acquiring a VDR

Traditionally the seller in an M&A transaction hosts the VDR. However, in some cases a buyer may already have a VDR subscription and may opt to facilitate the process by hosting the data room.

If the client does not already have access to a VDR, counsel may be asked to recommend one. Once counsel understands the requirements of the specific M&A transaction, counsel may recommend a VDR to the client or purchase a subscription directly and bill the client after.

Although comparing VDR providers is not within the scope of this Note, counsel can use reputable software review platforms, such as G2.com, to obtain detailed comparisons.

Some general items to discuss with the client as a starting point, include:

- Whether the client or firm already has a preferred provider.
- Whether there are budgetary or timeline restrictions.
- Which federal, state, and industry regulations and other standards may affect the level of security required to protect the information that is uploaded to the VDR. For example, consider if the information:
  - includes protected health information the use and disclosure of which must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (see Practice Notes, HIPAA Privacy Rule and HIPAA Security Rule: Overview and Administrative Safeguards); or
  - needs to be service organization controls (SOC) compliant (for example, a SOC 2 audit report is a report prepared by an auditor under the American Institute of Certified Public Accountants (AICPA) standards regarding a service organization's controls related to security, availability, processing integrity, confidentiality, or privacy (see AICPA, SOC 2 – SOC for Service Organizations: Trust Services Criteria; see also Practice Note, Accounting, Auditing and Financial Reporting in the US: Governing Authorities: AICPA)).

  For information on other potentially applicable regulations and standards, see Practice Note, Cloud Computing: Understanding the Business and Legal Issues: US Regulations and Standards.
- Whether there is a specific jurisdiction where servers for the client's data must or cannot be located (sometimes referred to as "data sovereignty"). Depending on the subject matter of the stored information and the jurisdiction of the VDR servers, the client may be subject to additional disclosure or other requirements (see Practice Note, Cloud Computing: Understanding the Business and Legal Issues: Jurisdictional Concerns).
- Determining how many administrators (individuals given the ability to invite and grant data room access to others) and guest users are anticipated to need access to the room.
- Approximately how many pages of storage or units of data the project is likely to require.
- How much ongoing help and support is needed from the VDR provider.

When counsel has a better understanding of what the M&A transaction requires, counsel can share these requirements with the shortlist of VDR providers being considered. Once counsel has confirmed that a provider can fit the M&A transaction's needs, schedule demonstrations and obtain price quotes.

General Setup of a VDR

After counsel agrees on a VDR provider and obtains access to their VDR platform, counsel can begin to set up a data room for the specific M&A transaction. There are several initial steps counsel can take to customize the VDR. Below are some recommended first steps.

Most of the steps outlined below are simple and may require no additional instruction to implement. However, to minimize delays when using a new VDR provider, it may be useful to communicate with the VDR provider to request assistance during this set up stage.

Adding Administrators

It is a best practice to assign administrative rights to at least two separate individuals at the firm managing the M&A transaction. This should include the primary lawyer responsible for the M&A transaction and at least one other team member (for example, a partner, associate, or paralegal working on the M&A transaction). The administrators should be necessary to the deal or already be bound by an NDA, if an NDA isn't already programmed automatically in the data room (see Setting Up a Clickwrap NDA in a VDR).

Assigning at least two administrators allows multiple individuals to invite users to the data room, make changes in the room, and reassign user permissions in case the other administrator is unavailable. M&A transactions with only one administrator may experience delays.

Individuals that may be granted administrative rights, include individuals that are:

- A trusted member of the firm that counsel has confidence in to make sound decisions in counsel's absence and who knows when to involve counsel.
- Actively engaged in the M&A transaction.
- Knowledgeable of how to or willing to learn how to use a VDR.
- Authorized to see all privileged information inside the VDR or, if not, the individual should understand and be willing to be bound to any necessary NDAs or general disclosure restrictions.
- Authorized to view all incoming correspondence from the client and from outside parties concerning the deal.
- Knowledgeable about which levels of access to provide new invited users of the data room based on their role in the M&A transaction.

Once counsel assigns administrative rights to another team member, it is helpful to clarify what counsel expects from them and in which circumstances they should take action in the data room. This step ensures a clear and efficient workflow during the M&A transaction.

Setting Up a Clickwrap NDA in a VDR

At this stage, it is likely that counsel has already distributed and received manually signed NDAs from all potential buyers needing initial access to the data room (for an example, see Standard Document, Confidentiality Agreement: Mergers and Acquisitions). However, including a copy of the existing NDA or a customizable clickwrap agreement form of NDA in the VDR is fairly common. Most VDR platforms offer this feature and it can usually be configured to appear the first time a new user logs into the data room (requiring the user to accept its terms before viewing any additional information in the data room).

Enabling this feature not only streamlines things, it also protects the client if additional individuals not a party to a manually signed NDA (for example, representatives of potential buyers, including legal counsel and financial advisors) need access to the data room during the due diligence process. This feature also works as a record keeping device allowing counsel to create a report detailing which individuals submitted clickwrap NDAs and when.

Recommendations for setting up a clickwrap NDA for a data room include:

- Ensuring that the clickwrap NDA is a general agreement that applies to all users of the data room, including the buyer, seller(s), or target company and each of their respective representatives.
- Adding a section to the clickwrap NDA with language that acknowledges that the terms and conditions for the clickwrap agreement apply to all users entering a data room unless otherwise agreed to by the parties. Parties entering into a separately signed NDA with differing terms can still default to that agreement if those terms supersede the clickwrap NDA (see Standard Document, Confidentiality Agreement: Mergers and Acquisitions: Section 13 and Drafting Note, Terms of This Agreement Control).

- In addition to the clickwrap NDA in the data room, create a folder for storing any separately signed NDAs, including any amendments to the NDAs.

While many administrators choose to enable both the clickwrap NDA feature in their VDR and separately collect signed NDAs, some firms or clients use only one method. Counsel should confirm which method its firm recommends and which method the client prefers.

If the data room is maintained by the seller's or target's counsel and contains a copy of the separately signed NDAs for the M&A transaction from all potential buyers, access to these agreements should be restricted to avoid a breach of the seller's or target's confidentiality obligation to other potential buyers as NDAs typically prohibit any party from disclosing information about a potential M&A transaction to others (see Standard Document, Confidentiality Agreement: Mergers and Acquisitions: Section 3 and Drafting Note, Discussions to Remain Confidential: Reciprocal Provision). This process is generally simple and handled by turning "off" or "avoiding enabling" that particular set of folders in the data room for all but authorized users (typically administrators).

Branding the VDR

If the platform supports it, add a logo and customize the colors of the VDR to reflect the firm's or the client's brand.

If counsel has not already named the data room, determine the best project name for the M&A transaction and update it accordingly (this is usually done under "general settings").

Customizing the VDR's Watermarks

Many data rooms come with automated watermarks that reflect a user's name, the M&A transaction's project name, and the time a document was opened. However, it is best to double check these watermark settings and make any changes needed before inviting users to the room.

Deleting Any Content No Longer Needed

Many VDR providers offer training materials for getting started to help set up the data room. Remove or delete these files before going live with the data room, so that only relevant M&A transaction materials are in the room during the M&A transaction process. The deletion of any training materials and other files unrelated to the M&A transaction should be completed before inviting users to the data room.

Compliance With Document Retention Policies

Before the deletion of any data room information, consult the firm's document retention policy (for an example, see Standard Document, Document Retention Policy). Some firms retain a complete copy of all M&A transaction due diligence materials (see Practice Notes, Due Diligence for Public Mergers and Acquisitions: Distribution and Organization of the Materials and Due Diligence for Private Mergers and Acquisitions: Distribution and Organization of Materials).

Populating the VDR With Files and Folders

Now counsel is ready to populate the data room with folders and files. Below are the most common ways to add information to the data room.

Uploading Folders and Files Directly

Uploading the folder and file structure from the user's computer to the data room is the most straightforward and usually the most efficient way to get the data into the new VDR. With this method, counsel or another VDR administrator can directly upload the folder structure counsel has created locally on counsel's computer into the data room.

Factors that make a direct upload more beneficial, include:

- Counsel already has the majority of folders and files required for the M&A transaction and due diligence stored locally.
- The folders and files counsel plans to upload are already in order.
- The folders and files counsel plans to upload are already properly named.

When counsel uploads the data directly, counsel has full control and knows exactly what is and is not going into the data room.

Creating Folder Structure and Delegation of Uploads

When counsel creates folders using an M&A checklist, counsel provides an outline for the data room first and then delegates the task of obtaining the materials responsive to the checklist to one or more other administrators or users with uploading rights.

While this method is usually the most secure, it does not work in all cases. Not all users may be willing to learn how to upload their data to a VDR. If the client is not accustomed to using data rooms, the client may default to the less secure approach of sending the files directly to counsel.

The delegation method may be useful in M&A transactions if:

- Counsel has multiple users (for example, in various departments) responsible for populating and updating some or all of the folders that fall within their department.
- Counsel is working with another VDR administrator, usually a paralegal, preparing the materials for the deal directly. This individual is responsible for organizing the entire room.
- The client has not yet provided counsel with all of the needed materials, but is comfortable with uploading the documents directly to the data room when given access.
- Counsel represents the buyer, but is hosting the data room (see Considerations When the Buyer's Counsel Hosts the VDR).

When using this method to populate the data room, it helps to have a system for reviewing uploaded documents before inviting other users to the data room. Setting up upload notifications for the data room so that counsel can review a document when it is uploaded by another user can help counsel keep track of new data uploads. However, if the data room is to host hundreds of documents, it is helpful to have additional procedures in place. For example, counsel can create a preparation folder in the VDR that only counsel can see. Once counsel has reviewed and approved a document, counsel can move the file out of the preparation folder and into the actual folder that is available to other users in the data room.

Syncing the VDR With a Local Folder

Some VDR platforms allow counsel to sync the contents of the data room with a local folder or vice versa. If this feature is available, it can be used to initially populate the data room and maintain the room during the M&A transaction. If counsel uses this solution for uploading data, it is important that access is restricted on both sides of the sync.

In addition to these main ways of populating the VDR, most platforms allow administrators to update, move, and rename folders and files at any time.

Redacting Documents Inside the VDR

The use of redaction in VDRs is an important tool to ensure that confidential information is protected from unauthorized disclosure. Most platforms allow counsel to:

- Choose between manual redaction or search and redact. Manual redaction involves manually marking an area for redaction, such as a word, line, paragraph, image, or an entire portion of the document. Search and redact allows counsel to find specific words or phrases within a document and redact them automatically.
- Save redaction drafts for collaboration with colleagues by saving redaction drafts before applying them. This feature allows multiple users to work together on the document within the data room, streamlining the redaction process.
- Unredact previous redactions. As the M&A transaction progresses, the target company may agree to reveal some or all of the previously redacted information. Full administrators typically can unredact a file (often with just a click of a button) so that users with access to the applicable information can view it in its entirety.
- Track redaction activity to control the redaction process using the reports section. This feature logs all redaction-related actions.

Inviting Parties to the VDR

After the VDR is populated, counsel is ready to invite outside users (for example, potential buyers and their representatives). The specific technical instructions for inviting guests to a VDR vary from provider to provider. However, the general process is as follows:

- Create a user group or individual entry for the person or team counsel is inviting to the VDR.
- Determine which files and folders the new individual or group is to have access to.
- Set the level of permission for files and folders an individual or group has access to (which folders or files they can view, print, download).
- Add email addresses for the user group or individual and send out invitations.
- After users receive their VDR invitation they can access the contents of the data room available to them. Project administrators can review and define security parameters on the project level, which will be mandatory for all project users, including

administrators. The security parameters can go from a basic 2-step verification to, in some cases, more advanced restrictions based on corporate email domains and/or IP addresses.

- View activity reports of user groups or individuals to see which folders and files are being accessed and by which parties.

When inviting outside users to a data room, it is common for new VDR administrators to have concerns about independent parties (for example, competing bidders in an M&A transaction) remaining confidential when accessing the VDR. Luckily, most VDRs are designed to allow users to enter a VDR privately by default. However, counsel can never be too cautious during this phase, so ensure all administrators have received training for the specific VDR platform.

Considerations When the Buyer's Counsel Hosts the VDR

While hosting a VDR on the buy-side is less common, it does happen. This scenario introduces additional complexity for inviting administrators and users to the data room. Considerations, include whether:

- The main buy-side contact (the client) is to be given administrative access to the room they are hosting during the deal. If so, determine whether the sell-side team is comfortable knowing that counsel can view all their activities and documents in an unrestricted fashion.
- The main buy-side contact (the client) is going to forego administrative access during the M&A transaction.

Possible solutions include:

- Assign an independent legal advisor to manage the data room for the duration of the M&A transaction. In this case, neither sell-side nor buy-side has administrative rights.
- Let the buy-side retain administrative access and agree to share a final report of the documents accessed by the buy-side party at the conclusion of the M&A transaction. This way the sell-side party has full transparency and a record of which files the buy-side viewed should they require this information later.
- Grant administrative rights to key individuals on both the buy-side and sell-side.

In some cases, the sell-side may not have a preference or may agree to user only privileges. In this case, deciding which role to assign the sell-side party is at the discretion of the VDR host.

Maintaining the VDR

A well-maintained data room means that users receive timely responses and that the content is updated and relevant at all times during the M&A transaction. Here are some general tasks associated with ongoing VDR maintenance to discuss with the team, including:

- Determining which individuals are to be responsible for inviting new users and user groups to the VDR and whether these individuals are to be given the necessary rights for inviting outside users to the VDR directly (as administrators of the VDR) or through a request to an administrator (via email for example) handled outside of the data room.
- Defining which individuals are to be responsible for disabling access to the data room for users and groups when their participation in the M&A transaction is no longer relevant.
- Deciding which individuals are to be responsible for answering questions from users in the room. Also determining the process for ensuring that questions are answered in a timely manner.
- Choosing which individuals are responsible for keeping content in the room up-to-date and whether these individuals are to be given upload permissions for the folders they are required to renew.
- If internal staff without administrative rights can upload files to the data room, determining whether a preparation folder is to be created in the VDR where files can be reviewed internally before going live or whether suggestions are to be handled outside of the data room.

Once the internal workflow is established, maintaining the data room is straightforward.

Communicating with Built-In Q&As

Managing communications during M&A transactions can be a daunting task. However, with the help of various filtering and sorting options typically available in the Q&A section of a VDR, counsel can streamline the process and ensure efficient management of collaboration. From hot-filter tabs to sorting options and advanced filtering, there are many tools typically available to make the process easier.

Here are some key points regarding features that are typically available in VDR built-in Q&As:

- Question categories can serve as an additional filtering option and facilitate navigation through the questions, especially when there are many.

- Questions can typically be automatically grouped in filter tabs for quick navigation.
- Sorting options such as unread, last updated, created, status, priority, and question team are typically available.
- Users can typically search for any question thread using keywords and apply advanced filters based on various criteria.
- Counsel can typically reset all applied filters and add or remove specific parameters as needed

During the Q&A set up counsel can select which roles to include in the Q&A workflow depending on the transaction requirements. Typically, VDRs include expert, question submitter, answer coordinators, and answer approver roles.

The available Q&A tabs can vary based on the user's Q&A role as defined by counsel. For example typically:

- If the expert role is enabled without auto-assignment, answer coordinators can manually assign questions to experts of the selected category or answer the questions themselves.
- If the expert role is enabled with auto-assignment, newly created questions are automatically assigned to experts of the selected category, and answer coordinators can also reassign them if needed.
- When using question categories, at least one category should be created if auto-assignment to experts is enabled (categories are optional if auto-assignment to experts is disabled).
- If no expert is assigned to a category, only the answer coordinator can see the questions in that category.
- The question side can change the previously selected category while the question is in draft status, but not after it is submitted to the answer side. However, the answer coordinator can typically change the category at any time.

Using a VDR Report

One of the benefits of a VDR is the ability to track the activities of outside users in the data room. These reports are available for VDR administrators to review, but are not available to invited users.

These reports provide leverage for the administrators of a data room. They show which documents are of interest to counsel's users and which documents and folders are not getting attention.

Some typical reports available in most VDRs include reports showing:

- When users or user groups logged into the room.
- Which folders and documents were viewed and which were not.
- Which documents specific users viewed and when.
- All changes in the data room made by administrators.

These reports can be obtained by logging into a VDR from an administrator's account. Some platforms also allow administrators to automate their reports, so that they arrive in the administrator's inbox automatically. From that point, relevant reports can be shared with the client.

Closing a VDR

When the M&A transaction is complete, counsel is ready to close the data room. Here are some final steps to consider during this phase:

- Deactivate all user groups to prevent them from accessing the data room.
- Create a backup of the data in the data room before closing the data room (see Compliance With Document Retention Policies). Counsel can usually do this by downloading the contents of the data room and saving it locally. However, some VDR providers allow counsel to also order encrypted flash drives of the data.
- Determine whether to delete the data from the VDR before closing it. It may instead be preferable to simply close the room without altering the data so that counsel can open the room again later, if needed (for example, if the parties terminate the M&A transaction before closing and a potential future transaction with another buyer is possible).