

Document Dump Triage Checklist

The first 30 minutes after receiving public records

Preserve before reviewing

- ☐ Save the received package exactly as delivered.
- ☐ Keep original filenames and do not annotate the original files.
- ☐ Record the delivery channel, sender, received date/time, and original location.
- ☐ Generate a SHA-256 manifest before conversion, OCR, splitting, or renaming.

Inventory the production

- ☐ Count files, pages where practical, total bytes, and file types.
- ☐ Identify unreadable, encrypted, empty, corrupt, or duplicate files.
- ☐ Check whether attachments mentioned in emails are actually present.
- ☐ Check numbering sequences, date spans, and obvious production gaps.

Create the review map

- ☐ Assign each source a stable ID before taking substantive notes.
- ☐ Record exact page, line, row, timestamp, or file references for findings.
- ☐ Separate events, financial entries, claims, contradictions, and missing proof.
- ☐ Reconcile every total before describing a discrepancy.

Close the first-pass readback

- ☐ Write down what was received, what failed, what remains unknown, and the next proof step.
- ☐ Store the manifest and readback outside the untouched originals folder.
- ☐ Verify that working copies can be traced back to an original source and hash.

Do not call a record “missing” merely because it is not in the first folder you checked. Record the locations searched, naming variants, and whether a cloud or case-management copy still needs review.

Methodology checklist only. This is not legal advice and does not establish authenticity, admissibility, completeness, or wrongdoing.