



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Completing the Disclosure Review Document

A Technical and Legal Guide

The Disclosure Review Document cannot be completed from a lawyer's desk. Section 1 demands a discipline about issues and Models; Section 2 demands facts that only the client's people and your forensic and eDiscovery specialists hold: where the data lives, how much of it there is, what the searches will really return, what technology will be used and what it will cost. This guide sets out, field by field, what to learn from whom before the drafting starts, so the DRD is completed from evidence rather than imagination.

© Estimated reading time: 30 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, supports solicitors through the DRD cycle on live timetables: identification and early assessment run inside the 42-day clock, Section 2 completed from measured volumes and tested terms with hit reports ready for exchange, and examiners available where irretrievable data, damaged devices or authenticity questions must be described accurately. This guide is the practice's field manual for the document itself.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ISO 27001-ALIGNED SECURITY

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

PD 57AD / DRD EXPERIENCE

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: an exam you sit jointly
- 03 Anatomy of the DRD
- 04 What to learn from the client
- 05 What to learn from your eDiscovery specialist
- 06 What to learn from your forensic examiner
- 07 Field by field: who supplies which answer
- 08 Drafting Section 1 well
- 09 Joint completion and negotiation
- 10 The timetable, mapped to the learning
- 11 Worked example: a Section 2 built from evidence
- 12 Common mistakes and technical limitations
- 13 Questions to ask · Suggested wording
- 14 Checklist and red flags · When to involve a digital forensic expert
- 15 Frequently asked questions
- 16 Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE POINT: THE DRD IS COMPLETED FROM THREE SOURCES OF KNOWLEDGE, NONE OF THEM THE DRAFTING LAWYER

The Disclosure Review Document under PD 57AD has two halves. Section 1 (the List of Issues for Disclosure and the Models proposed against each) is legal work, but disciplined legal work: short, neutral, document-focused issues, not the trial agenda. Section 2 is a technical questionnaire about the client's data and your intended methods: where documents are held, by whom, in what volumes, what will be searched and how, what technology (including TAR) will be used, what cannot be retrieved, and what it will all cost. None of those answers originates with the lawyer. They are learned: from the client (systems, custodians, channels, retention, prior handling), from the eDiscovery specialist (measured volumes, tested terms, analytics capability, cost scenarios) and from the forensic examiner (deleted and irretrievable data, device and chat feasibility, encrypted and damaged sources). The lawyer's craft is to commission that learning early enough, on the 42-day clock, that the DRD is drafted from evidence, because every figure and description in it is a representation the certificate will eventually stand behind.

- **The imaginary Section 2 is the regime's most common quiet failure.** Volumes guessed, "TAR under consideration" as a placeholder, sources described from optimism: each becomes a completeness argument, a budget overrun or a certificate problem later. §7's field-by-field table exists to make imagination unnecessary.
- **Three interviews, three deliverables.** The client conversation (the 50-question first meeting and its follow-ups) yields the data map; the specialist engagement yields the assessment report and tested terms; the examiner consult yields the irretrievable-data and feasibility statements. The DRD is those three deliverables, transcribed.
- **Section 1 has its own discipline.** The *McParland* principles (issues needing contemporaneous documents, stated briefly and neutrally; Models chosen per issue; Model C requests precise) are covered in §8, with the drafting habits that keep the list short and the court onside.
- **The document is jointly completed, and the joint process is scored.** Exchange, iterate with data, narrow, and file one document with genuine disputes crisply identified: §9 covers the mechanics, and the cooperation record it generates is itself protective.
- **This guide integrates the series.** The learning it commissions is the machinery of the companion guides: the first meeting, sources, custodians, assessment, search design and the PD 57AD overview each go deeper on their piece.

The problem in plain English: an exam you sit jointly

The DRD looks like a form, and forms invite form-filling: precedent text adapted, boxes completed from what the team believes, the technical questions answered with careful vagueness. The regime is built to punish exactly that. The document is exchanged with an opponent who may have measured its own estate; it is read by a judge who has seen a hundred of them and knows what evidence-based entries look like; its figures feed the costs budget the court will hold you to; and its descriptions of sources, searches and irretrievable data are the skeleton of the disclosure certificate someone will personally sign.

The better mental model: the DRD is an exam sat jointly by three parties on your side. The client sits the paper on its own systems and people. The eDiscovery specialist sits the paper on volumes, methods and costs. The forensic examiner sits the paper on what no longer exists and what special sources will yield. The lawyer sets the questions (from the issues), invigilates the timetable, and writes up the answers in the court's language. A lawyer who tries to sit all three papers alone fails all four roles at once, and the failure surfaces at the worst possible moments: the CMC, the budget hearing, the certificate, the completeness challenge.

§ 0 3 · THE DOCUMENT

Anatomy of the DRD

- **Section 1: Issues for Disclosure and Models.** The List of Issues for Disclosure (drafted first by the claimant, engaged with by the defendant), each party's proposed Model (A to E) per issue with brief reasons, and, where Model C is proposed, the specific requests themselves. This is where the scope argument happens; everything else implements it.
- **Section 2: data and method.** In substance, a structured questionnaire covering: where and in what form relevant documents are held (systems, devices, accounts, hard copy), the custodians and the date ranges, the volumes involved, how the party proposes to search (terms, and the intended use of analytics, sampling and technology-assisted review), documents that are no longer in existence or not reasonably accessible (with reasons), proposals on production format and structure, and estimates of the costs of the proposals in play. It is completed in a granularity proportionate to the case, and it is where the technical learning of §§4 to 6 lands.
- **The Less Complex Claims variant** shortens the form substantially while keeping the logic; the learning burden shrinks with it, but does not disappear: even the short form asks where the data is and how it will be searched.
- **Status and updating:** the DRD is a working, jointly completed document, filed for the CMC and capable of revision as the case develops; treat it as versioned, like the strategy document it summarises, and diarise the updates that pleading amendments or staged tranches will require.

FOR THE PRACTITIONER

Download the current forms at the start of every matter rather than reusing last year's: the DRD and its guidance notes have been amended since the regime was made permanent, and opponents notice stale boilerplate. The forms' own guidance repeats a theme this guide shares: the document is meant to be short, cooperative and factual, not a second round of pleadings.

What to learn from the client

The client conversation (run as the structured 50-question meeting in our companion guide, with written questionnaires behind it) supplies the factual half of Section 2. Before drafting, the file should contain client-sourced answers on:

- **Systems and tenancies:** the platforms (mail, chat, drives, business systems), who administers them (including the MSP), licence tiers and what they mean for holds, logs and export; migrations and decommissioned systems over the relevant period, and where their data went.
- **Custodians and identities:** who actually did the relevant work (participation, not rank), their aliases and addresses across domain changes, delegation arrangements, leavers and the state of their accounts and devices, and the shared mailboxes and channels that individual custodians will not cover.
- **Channels, honestly:** the chat and messaging reality (Teams, WhatsApp, Signal), personal-device and personal-account use for work, and any disappearing-message settings, because Section 2's source descriptions are tested against the opponent's copies of exactly these communications.
- **Date anchors:** the events behind each pleaded issue, per issue, so ranges are proposed from the chronology rather than the calendar.
- **Retention, deletion and backups:** the live timer settings, the backup regime and rotation, what has already auto-deleted and when, and any post-dispute changes to any of it: the raw material for the irretrievable-data entries and for honest preservation statements.
- **Prior handling:** anything already collected, exported, reviewed or tidied, by whom and with what tools, because Section 2's descriptions must fit the facts an examination would find.
- **Third-party holdings:** MSPs, hosts, processors, former providers and counterparties holding the client's documents, for the control-and-sources entries and the preservation narrative.

The discipline: every client answer that will appear in the DRD is confirmed in writing (the numbered meeting note, the questionnaire returns), because "the client told us" needs a document behind it when the entry is later probed.

What to learn from your eDiscovery specialist

The specialist converts the client's facts into the measured numbers Section 2 actually asks for, through the early-assessment machinery of this series. Commission, and receive before drafting:

- **Measured volumes:** per-custodian and per-source sizes and item counts (in-place platform reports at minimum, indexed seed data where the case warrants), with expansion allowances stated, so the volume entries are ranges with bases rather than guesses.
- **Duplication and overlap:** measured dedupe rates and cross-custodian hash overlap, which turn custodian negotiations into arithmetic and justify preserve-only proposals for marginal names.
- **Tested terms with hit reports:** every term proposed in the DRD run against real data first, with hit counts (documents and families, unique hits) and sampled relevance, exchange-ready, because the regime's search entries are negotiating positions and untested positions lose.
- **Analytics and TAR capability, specifically:** what the platform will actually do (threading, near-duplicates, clustering, continuous active learning), how validation runs (sampling, elusion, richness tracking) and what documentation the court would see, so the TAR entry is a described method rather than a genuflection.
- **Processing and exception realities:** what file types the population contains, the forecast exception load (encrypted, corrupt, no-text), and what the platform cannot index, feeding the honest limits every search description needs.
- **Production capability:** supported formats, load files, family handling, native production for spreadsheets, redaction workflow, so format proposals are made once, early, and kept.
- **Cost scenarios:** the price of each live proposal (yours and the opponent's) through collection, processing, hosting and review, on the measured numbers, aligned with the Precedent H disclosure phase so the DRD and the budget tell one story.

§ 0 6 · SOURCE THREE

What to learn from your forensic examiner

Certain Section 2 entries can only be made honestly on forensic advice, because they describe what no longer exists, what cannot easily be reached, or what special sources will yield:

- **Documents no longer in existence:** what was auto-deleted and when (from retention settings and platform behaviour), what recovery is realistically possible (recycle stores, unallocated space, backups, cloud sync residue) and at what cost, so the "no longer exists" entries are accurate in both directions: neither writing off the recoverable nor promising the gone.
- **Not reasonably accessible sources:** the true cost and feasibility of legacy tapes, damaged media, obsolete formats and encrypted stores, with figures, because accessibility exclusions survive only when evidenced.
- **Device and chat feasibility:** what extraction level each handset and app will support, what disappearing messages have already taken, and what a targeted, privacy-protective personal-device protocol can deliver, before the DRD promises (or concedes) anything about mobile sources.
- **Integrity and authenticity concerns:** where prior handling, suspected deletion or contested documents mean an entry should be framed carefully and an examination may be needed, including whether any issue is heading toward CPR Part 35 territory that the DRD should anticipate rather than collide with.
- **Preservation adequacy:** a short forensic review of what the day-one steps actually captured (were the holds effective, do the logs still exist, is the leaver's device intact), so the preservation statements describe verified reality.

WHY THIS CONSULT IS CHEAP INSURANCE

Irretrievable-data entries are the DRD's most litigated lines: opponents test them, courts remember them, and certificates inherit them. An hour of examiner time per problematic source, before drafting, is the difference between "deleted and unrecoverable" written accurately and the same words written hopefully, discovered to be wrong by the other side's expert.

§ 0 7 · THE MAP

Field by field: who supplies which answer

DRD TERRITORY	WHO SUPPLIES IT	THE EVIDENCE BEHIND THE ENTRY
Issues for Disclosure; Models per issue; Model C requests	Lawyer (with counsel)	Pleadings, the issue-source matrix, and the measured costs of each Model alternative
Sources: systems, devices, accounts, hard copy	Client + specialist	Data map from interviews, questionnaires and cross-checks; tenancy reports
Custodians and date ranges	Client + specialist	Tiered custodian list with rationales; footprint counts; per-issue anchors checked against timelines
Volumes	Specialist	Assessment report: measured sizes and counts, expansion allowances, stated tolerances
Search proposals: terms, ranges, scope	Specialist + lawyer	Tested terms with hit reports and sampled relevance; the search protocol
Analytics and TAR	Specialist	Named methods, validation plan, specimen documentation
Documents no longer in existence / not reasonably accessible	Examiner + client	Retention settings and deletion history; recovery feasibility and cost statements
Preservation narrative	Client + examiner	Hold register, suspension confirmations, notices, the written confirmation, verified
Production format proposals	Specialist	Platform capability; the draft production specification
Cost estimates	Specialist + lawyer	Scenario models on measured numbers, reconciled to Precedent H

The habit the table enforces: no entry is drafted before its evidence exists on the file, and every entry can be answered, if probed, by producing a document rather than a recollection.

Drafting Section I well

- **Issues for Disclosure are not the trial issues.** The *McParland* test: only the key disputed issues the court will need contemporaneous documents to decide. Most cases yield four to eight; a list of twenty is a pleading in disguise and will be said so.
- **Draft neutrally and briefly.** "Whether the works were completed by [date]" not "The Defendant's failure, in breach, to complete". Neutral wording is agreed faster, and wording fights are the classic DRD cost sink the courts have criticised.
- **Choose Models per issue, with the measured cost of each.** No default; a deliberate mix (A or B where documents will not decide the issue, C where requests can be precise, D where they will) is itself persuasive. Attach the numbers: a Model proposal with its forecast population and cost reads as engagement; one without reads as reflex.
- **Model C is a drafting discipline.** Particular documents or narrow classes, date-bounded and issue-tied ("the test reports for batches 41 to 47 issued between March and June 2025"), not themes ("all documents relating to quality"). Respond to the opponent's requests the same way: agree the precise, offer reformulations of the vague, resist the fishing with reasons.
- **Keep the known-adverse duty in view.** Model A and B proposals are palatable exactly because known adverse documents are disclosable regardless; saying so in the reasons defuses the standard objection.

Joint completion and negotiation

- **Run the exchange on the front foot:** serve the draft issues on time, volunteer your Section 2 information rather than being chased for it, and ask for the opponent's equivalents by return: volumes, custodian counts, tested terms, the basis of their entries.
- **Iterate with data.** Exchange hit reports; counter wide terms with sampled relevance figures and reformulations; answer custodian inflation with footprint and overlap tables; offer structure (preserve-only tiers, staged tranches behind defined triggers, clawback protocols) visibly.
- **Converge on one document.** The court expects a single, jointly completed DRD, not duelling versions: incorporate agreed positions as they land, and isolate the genuinely disputed entries into crisp, numbered disagreements with each side's evidence attached, ready for a Disclosure Guidance Hearing or the CMC to resolve in minutes.
- **Mind the tone and keep the record.** DRD correspondence is conduct evidence: cooperative, specific and data-backed letters win costs arguments later, and the file of offers and narrowings is your paragraph 20 shield.
- **Involve the specialists in the negotiation itself.** Joint provider calls on format and TAR, exchanged specimen validation documentation, even a joint hit-report exercise on disputed terms: technical convergence between providers routinely dissolves disputes the lawyers were escalating.

The timetable, mapped to the learning

DEADLINE	LEARNING THAT MUST ALREADY BE DONE
Day 1 (instruction)	Preservation executed and evidenced; the 50-question meeting held; specialist and (where triggered) examiner engaged
Within 28 days of final statement of case (state whether Extended Disclosure likely)	Issues sketched; data map v1; in-place volume reports pulled, enough to know whether and where Extended Disclosure is worth seeking
Within 42 days (claimant serves draft Issues for Disclosure)	Issue-source matrix complete; custodian tiering drafted; assessment under way with first measured volumes
Exchange and negotiation window	Assessment report delivered; terms tested with hit reports; examiner statements on irretrievable and special sources; cost scenarios per live proposal
Filing before the CMC	One joint document; disputes numbered with evidence attached; budget reconciled to the proposed scenario

The uncomfortable arithmetic: the 42-day clock is the assessment clock. A specialist instructed in week five cannot measure what the draft due in week six describes, which is why the strategy guide in this series puts provider engagement in week one, and why "we will firm up Section 2 later" is a plan to draft it from imagination.

Worked example: a Section 2 built from evidence

THE ENTRIES, AND WHAT STOOD BEHIND THEM

In a £7m distribution dispute, the defendant's Section 2 stated: sources (M365 tenancy, one legacy on-premises archive, a Teams estate, WhatsApp on four handsets, a Sage system reported via its owner), on the data map from dual-track interviews and an SSO cross-check; custodians (seven: four core, three targeted, with five claimant-proposed names offered preserve-only on footprint counts of under 1,100 issue-period items each and 84 per cent hash overlap); volumes (312 GB collected-equivalent, an estimated 480,000 to 560,000 items post-expansion, measured duplication 41 per cent); search (sixteen tested terms, hit reports exchanged twice, three terms rewritten with proximity operators after sampling; CAL proposed with elusion-sample validation, specimen documentation offered); irretrievable data (a 2023 mailbox purge under a pre-dispute 24-month policy, dated from the retention audit log, with the examiner's statement that backup coverage ended eight months short of the purge window); not reasonably accessible (94 legacy tapes, restore quote £61,000, sampled uniqueness under 2 per cent, parked openly); production (searchable PDF plus natives for spreadsheets, standard load file, families intact); costs (three scenarios priced, the proposed one at £174,000, reconciled to Precedent H).

The claimant's Section 2 answered volumes with "substantial" and terms with "to be agreed". At the CMC the court adopted the defendant's scheme nearly whole, directed the claimant to answer the defendant's information requests within 14 days, and said what it thought in the costs order. Nothing in the defendant's document was clever; every line simply had a document behind it.

Common mistakes and technical limitations

Common mistakes

- **Drafting before learning.** The DRD written in week five and the facts commissioned afterwards to fit it.
- **The imaginary Section 2:** guessed volumes, unnamed methods, "TAR under consideration", sources described from the org chart rather than the estate.
- **Issue-list inflation:** twenty adversarial issues where six neutral ones serve, and the costs of the wording war noticed by the court.
- **Untested terms proposed (or agreed) in the document,** discovering their hit counts after the order that embeds them.
- **Irretrievable-data entries written hopefully:** "deleted and unrecoverable" without an examiner's view, corrected later by the opponent's expert.
- **The DRD and the budget telling different stories,** with the divergence surfacing at the costs hearing.
- **Duelling documents:** two rival DRDs filed instead of one joint document with numbered disputes.
- **Stale forms and boilerplate,** including entries that survive from the precedent matter and describe someone else's estate.
- **No versioning:** the case moves, the DRD does not, and the certificate eventually describes a document two amendments out of date.

Technical limitations

- **Estimates carry tolerances.** Volumes expand in processing, exceptions hide until touched, platform counts differ from processed counts: state ranges with bases, and the DRD inherits honesty instead of hostages.
- **The form flattens complexity.** Chat, structured systems and continuous data do not fit document-count boxes gracefully; describe them in their own units with a stated review-and-production approach rather than forcing false precision.
- **Granularity is proportionate.** A Less Complex Claim does not need seed indexing and scenario models; it needs the short form completed from the level 1 reports and a sensible protocol. Scale the learning to the case, not the anxiety.
- **Joint completion needs a counterparty.** Where the opponent will not engage, perform your half visibly, request theirs in writing, and let the court draw the conclusion the file supports.

§ 13 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client (before drafting)

- Is every system, channel and device we will describe in Section 2 confirmed in writing from the meeting note and questionnaires, or are any entries still recollection?
- What has changed since the first meeting: leavers, migrations, settings, anything already collected or touched?
- Who will review the draft Section 2 for factual accuracy before it is exchanged, and confirm in writing that it matches the estate?

Ask your opponent

- Please provide the information behind your Section 2 entries: measured volumes per custodian and source, and the basis of measurement.
- Have your proposed terms been tested? Please exchange hit reports and sampled relevance before positions are fixed.
- For each "no longer in existence" or "not reasonably accessible" entry: the factual basis, dates, and any expert input behind it.
- Please confirm your proposed production format, TAR approach and validation method, and provide specimen documentation.

Ask your eDiscovery / forensic provider

- Can you deliver the DRD support pack (volumes, custodian counts, tested terms, cost scenarios, format proposal) inside the 42-day clock from a standing start?
- Which Section 2 entries in this draft would you not currently stand behind, and what learning would fix each?
- For every irretrievable or inaccessible source we propose to list: what is your evidenced statement, and would it survive the other side's expert?
- Who attends the CMC or a Disclosure Guidance Hearing if method entries are challenged, and in what capacity?

SUGGESTED WORDING · INSTRUCTION TO A PROVIDER FOR THE DRD SUPPORT PACK

"To support completion of the Disclosure Review Document on the current timetable, you are instructed to deliver by [date]: (1) measured data volumes per custodian and source (in-place reports across the estate; indexed seed for the sources at Schedule 1), with expansion allowances and tolerances stated; (2) per-custodian issue-period item counts and cross-custodian overlap analysis for the candidates at Schedule 2; (3) hit reports and sampled relevance results for the candidate terms at Schedule 3, iterated once with our comments; (4) a statement of proposed analytics and TAR methodology with the validation plan and specimen documentation; (5) evidenced statements on the retrievability, accessibility and recovery cost of the sources at Schedule 4, prepared or reviewed by a forensic examiner; (6) a proposed production specification; and (7) cost scenarios for each disclosure proposal in play, in a form reconcilable to Precedent H. Deliverables should be in a form deployable, as to their tables and statements, in Section 2 and in exchanges with the other side."

SUGGESTED WORDING · SECTION 2 VOLUME AND SEARCH ENTRIES (STYLE TO ADAPT)

"Volumes: the sources identified hold approximately [n] GB, estimated at [range] documents after processing (measured cross-custodian duplication [x] per cent; figures from an early data assessment completed [date], tables annexed). Searches: the [party] proposes the search terms at Appendix [x], each tested against the assessed data; hit reports (documents and families, unique hits per term) were exchanged on [dates] and sampled relevance results are annexed. Review will be prioritised by continuous active learning, validated by a random sample of the unreviewed population of not fewer than [n] documents, with the residual rate and stopping decision recorded. Items that cannot be searched by these means (encrypted, corrupt or image-only items) will be logged and resolved or reviewed separately, and the description of the search in any certificate will reflect that log."

§ 1 4 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The DRD completion checklist

- ☐ Current forms downloaded; LCC applicability checked
- ☐ Client learning complete and in writing: systems, custodians, channels, anchors, retention, prior handling, third parties
- ☐ Specialist pack delivered: measured volumes, overlap, tested terms with hit reports, TAR method and validation plan, format proposal, cost scenarios
- ☐ Examiner statements on every irretrievable, inaccessible or special source proposed for Section 2
- ☐ Section 1: issues short, neutral, document-focused; Models per issue with measured reasons; Model C requests precise
- ☐ Every Section 2 entry traceable to a document on the file; client factual sign-off in writing
- ☐ DRD and Precedent H reconciled on the same scenario
- ☐ Exchange run with data; offers and narrowings recorded; one joint document; disputes numbered with evidence
- ☐ Versioning and update triggers diarised

Red flags

- Any entry beginning life in the draft before its evidence exists on the file.
- "Substantial", "to be agreed" or "under consideration" doing the work of a number or a method.
- An irretrievable-data line no examiner has seen.
- Terms in the document that have never met a hit report, on either side.
- An opponent's Section 2 that answers information requests with adjectives.
- The budget and the DRD priced from different scenarios.
- Precedent text describing systems your client does not have.

When to involve a digital forensic expert

For the DRD specifically: whenever Section 2 will assert that documents no longer exist, cannot be recovered or are not reasonably accessible (the entry should be evidenced by an examiner before it is exchanged); whenever mobile, chat, encrypted or damaged sources must be described with feasibility and cost; whenever prior handling or suspected deletion means the preservation narrative needs verification; and whenever an entry is heading toward a dispute that will need CPR Part 35 evidence, so the expert who will defend the position helps frame it. The wider triage discipline is in *eDisclosure or Digital Forensics?* and the surrounding workflow in *How to Build a Defensible eDisclosure Strategy*.

§ 15 · COMMON QUESTIONS

Frequently asked questions

Who actually completes the DRD?

The lawyer drafts and owns it, but its content is learned: the client supplies the facts about systems, people and retention (confirmed in writing), the eDiscovery specialist supplies the measured volumes, tested terms, methods and costs, and the forensic examiner supplies the statements about deleted, irretrievable and special sources. The document is then completed jointly with the other side into one filed version. A DRD completed by any one of those actors alone is deficient in a way opponents can usually detect.

How much detail does Section 2 really need?

Proportionate detail, but evidenced detail: ranges with bases rather than false precision or empty adjectives. A heavy Commercial Court matter warrants an assessment report behind every number; a Less Complex Claim warrants the short form completed from platform reports and a sensible protocol. What no case warrants is an entry nobody could stand behind if asked "how do you know?"

What if we genuinely do not know a figure yet?

Say what is known, state the measurement in progress and the date it will land, and update: "in-place reports indicate [range]; an indexed assessment of the core sources completes on [date] and figures will be exchanged then" is a compliant, credible entry. What is not compliant is a guess dressed as a fact, or a blank held open indefinitely while the timetable runs.

The other side's Section 2 is vague. What do we do?

Request the underlying information in writing (volumes and bases, tested terms, the facts behind irretrievable entries), propose exchange of hit reports, and if vagueness persists put the correspondence before the court: at a Disclosure Guidance Hearing or the CMC, a party with evidence facing a party with adjectives usually gets both its scheme and its costs. The worked example in §11 is the standard shape.

Can the DRD be changed after the CMC?

Yes: it is a working document, and the regime provides for varying disclosure orders as the case develops. Changes are made openly (versioned, reasoned, promptly proposed), typically where pleadings amend, staged tranches trigger, or new sources surface. What damages parties is not change but silent divergence: an exercise that drifted from the filed document without anyone updating it.

Does the DRD bind us at the certificate stage?

Practically, yes: the certificate describes the search actually performed, and the DRD (as ordered and as varied) is the benchmark it is read against. This is the deep reason for completing it from evidence: entries you measured, you can perform and certify; entries you imagined, you must either quietly miss (a certificate problem) or expensively honour (a budget problem).

§ 1 6 · REFERENCE

Glossary

Assessment report

The early-data-assessment deliverable whose tables populate Section 2's volume and method entries.

DRD

The Disclosure Review Document: Section 1 (Issues for Disclosure and Models) and Section 2 (data, methods, costs), completed jointly.

DRD support pack

The commissioned bundle of measured volumes, tested terms, method statements, feasibility statements and cost scenarios behind the draft.

Hit report

Per-term counts (documents, families, unique hits) against a real population; the currency of search negotiation.

Irretrievable-data statement

The evidenced (examiner-reviewed) entry that documents no longer exist or cannot reasonably be recovered, with basis and cost.

Issues for Disclosure

The key disputed issues needing contemporaneous documents to decide; deliberately fewer than the trial issues.

LCC

Less Complex Claims: the simplified PD 57AD track with a shortened DRD.

Model C request

A precise request for particular documents or a narrow class, date-bounded and issue-tied.

Preserve-only proposal

Offering marginal custodians or sources as preserved but not collected, evidenced by footprint and overlap data.

Scenario model

The forecast population and cost of a given custodian, range and term combination; the pricing behind Model proposals.

Section 2 sign-off

The client's written confirmation that the factual entries match the estate before exchange.

Validation plan

The stated sampling and stopping methodology behind a TAR entry.

Sources and authoritative references

The completion discipline in this guide draws on materials published by our e-discovery practice and laboratory, referenced here as sources:

- e-discovery.uk, EDRM Phase 01 · Identification and Phase 04 · Processing (the data map behind the source entries; terms iterated against samples with hit reports; exception reporting): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/processing
- e-discovery.uk, the practice's method statement ("Bring us in early. Defensibility is built, not retrofitted") and Knowledge Centre notes including "Writing search terms that survive negotiation": e-discovery.uk · e-discovery.uk/knowledge
- cflab.uk, digital forensics services (deleted-data recovery feasibility, damaged and encrypted sources, and the CPR Part 35 reporting behind irretrievable-data statements): cflab.uk/digital-forensics-services
- cflab.uk, mobile phone forensics (extraction feasibility for the device and chat entries): cflab.uk/mobile-phone-forensics · guides for lawyers: cflab.uk/guides
- Practice Direction 57AD, with the Disclosure Review Document forms and guidance notes: justice.gov.uk, PD 57AD
- *McParland & Partners Ltd v Whitehead* [2020] EWHC 298 (Ch): bailii.org · *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch): bailii.org
- CPR Part 3 (costs management and Precedent H): justice.gov.uk, Part 3 · CPR Part 35 (experts): justice.gov.uk, Part 35

- CPR Part 31 and PD 31B (the regime outside the B&PCs, and the Electronic Documents Questionnaire as the analogue exercise): [justice.gov.uk](https://www.justice.gov.uk), [PD 31B](#)
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about completing the Disclosure Review Document in the United Kingdom as at August 2026. The worked example is a fictional illustration and all figures are illustrative. The Practice Direction and its forms are amended from time to time; always check the current text. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The DRD support pack in this guide is a standing product of our e-discovery practice (**e-discovery.uk**): measured volumes and custodian analytics from in-place reporting and indexed seeds, tested search terms with exchange-ready hit reports, named analytics and TAR methodology with specimen validation documentation, a production specification, and cost scenarios reconciled to Precedent H, delivered inside the 42-day clock from a standing start where preservation allows. The laboratory side supplies what the honest entries need: evidenced statements on deleted, irretrievable, encrypted and damaged sources, mobile and chat extraction feasibility, and verification of the preservation narrative, with examiners who defend those statements under CPR Part 35 / CrimPR Part 19 if challenged. We routinely join provider-to-provider calls that dissolve format and TAR disputes before the CMC. Conflicts checks, confidential scoping discussions and fixed-fee DRD packages are routine.



INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@cflab.uk

E-DISCOVERY

e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace