compliance assist

Step 7: Document Everything

Purpose and Importance

The final step is to document the entire testing and tuning process and its outcomes. Comprehensive documentation is critical for demonstrating compliance and for future reference. Regulators (and internal auditors) will scrutinise how you arrived at your results and ensure there's an audit trail for every decision and change. The EBA guidelines emphasise that test results should be "thoroughly documented, justifiable under supervisory scrutiny and integrated into the compliance framework". Similarly, it's no longer enough to say your system works, you must prove it with evidence and formal methodology. This step involves compiling your test plan, data, results, analysis, changes and final outcomes into an organised set of documents. Good documentation serves a dual role: (1) It satisfies regulatory requirements and provides transparency and (2) it preserves institutional knowledge so that next year (or whenever the next test) the team can build on what was learned rather than starting from scratch. Essentially, by the end of this step, anyone should be able to review the documentation and verify what was done, why it was done, what was found, and how issues were addressed, without having to rely on individual memories.

Key Activities and Decisions

In documenting the process:

- **Consolidate test artifacts:** Gather all pieces from previous steps:
    - Test Plan document (objectives, scope, stakeholder approvals).
    - Test Dataset details (the list of test cases and expected results).
    - Test Execution records (the raw output, alert screenshots/exports, logs).
    - Analysis report (findings, metrics, root causes).
    - Change Log and Tuning actions (what was changed and why).
    - Re-test results demonstrating improvements (could be part of analysis or separate).
    - Any email approvals or meeting minutes relevant to decisions or sign-offs.

Ensure you have both digital copies and possibly printed copies (depending on your record-keeping policies) of these items. Organise them, for example in a dedicated folder structure (e.g. "Sanctions Testing 2026" with subfolders for each step's docs).

- **Prepare the final report (summary)**: Write a narrative summary that encapsulates the whole project. This can be a formal report or slide deck that you would present to senior management and regulators if needed. Structure it like:
    - **Introduction and Background**: Why the test was conducted (e.g. regulatory expectations, part of annual validation program).
    - **Scope and Objectives**: What was tested and what the goals were.
    - **Methodology**: How you carried it out (data used, approach, any independent elements).

- **Results**: What you found (initial performance, issues identified, possibly a concise table of them, final performance after tuning).
- **Actions Taken**: The tuning performed to address issues.
- **Conclusion**: Final state of the system (e.g. "After remediation, the system caught 100% of test sanctions and false positives were reduced to X%. The system is now in compliance with EBA/FCA expectations.").
- **Next Steps**: Plans for future (like regular re-testing schedule, any remaining improvements to do later).

Keep the main body high-level and factual, with references to appendices for detail. This report should tell the story clearly to someone non-technical as well.

- **Attach or reference detailed appendices**: Include the supporting documentation as appendices or separate attached documents so the main report isn't too cluttered. Appendices can be:
  - The full list of test cases with expected vs actual outcomes (could be a big table).
  - Detailed analysis tables or logs.
  - The change log of configuration adjustments.
  - Copies of approvals from management.

Label and organise these for easy navigation (e.g. "Appendix A: Test Cases and Outcomes", "Appendix B: Change Log").

- **Ensure auditability**: Check that for every significant step or decision, there is documentation to support it:
  - For instance, if you say "we found 5 misses," ensure the evidence (screenshots or logs) of those misses is included.
  - If you say "threshold lowered from 80 to 70," ensure the change log and perhaps a screenshot of the new setting is available.
  - If management approved the plan, include that approval (email or signed document).

The idea is that an auditor could replicate and validate your findings from the documentation alone. They might not re-run tests, but they should see enough proof that if they did, they'd get the same results.

- **Integrate into compliance program**: Make sure the outcomes are recorded in any relevant risk management documents. For example:
  - Update your AML/Financial Crime Risk Assessment document to mention that sanctions screening effectiveness was tested on X date and summarise results.
  - If you maintain a model validation or system performance register, log this exercise and its conclusion there.
  - If there's a section in your policies or procedures about sanctions screening, update it to reflect any changes (e.g. new thresholds, new processes for regular testing).

- Put a reminder in the compliance monitoring calendar for the next test cycle (e.g. "repeat this test in 12 months").

This shows regulators you're not doing this ad-hoc, it's part of a structured program.

- **Store documentation accessibly**: Follow your organisation's record-keeping protocol for compliance documents. Typically, maintain these records for a number of years (sanctions compliance docs usually for at least 5 years, often longer given look-back requirements, but check local rules). Ensure the documentation is accessible to those who need it (e.g. if the MLRO or auditors want to see it). A secure SharePoint or shared drive folder with proper permissions often works.
- **Prepare a management summary or presentation**: Often, it's useful to present the findings to senior management or the board (maybe in a risk committee meeting). Use the final report or a summarised version to do this. Get their acknowledgement recorded in minutes. This step might be required by internal governance (senior management oversight) and is evidence that the firm's leadership is aware of the system's effectiveness.
- **Plan communications with regulators (if applicable)**: If your regulator is aware of this testing (e.g. you promised to do it in a response letter or they are actively inquiring), you may prepare a summary to share with them. Usually, you wouldn't send full internal docs initially, but maybe a letter that "We conducted a comprehensive validation of our sanctions screening on [date]. Key results: [etc]. Detailed documentation is available on request." If a specific finding had to be reported (e.g. you discovered a significant gap that you are obligated to report and then fix), ensure you've done that as well in a timely manner.
- **Include lessons learned and recommendations**: Document if there are any broader lessons or future enhancements. For example, "During testing we realised that having a testing environment with up-to-date data is crucial, recommend investing in better test environment data refresh." or "We plan to incorporate automated testing routines quarterly to catch issues sooner." Capturing these ensures continuous improvement. It can also be an appendix or a section in the report.
- **Get a final sign-off**: It can be good practice to have a final sign-off on the testing outcome, perhaps by the Head of Compliance or even the MLRO, stating that they are satisfied with the effectiveness of the sanctions screening system following this exercise. This could be a short memo or sign a line on the report. It's an extra layer of demonstrated oversight.

Practical Tips and Examples:

- **Use clear versioning**: Mark the final documents with version numbers and dates. E.g. "Sanctions Screening Test Report – Final – v1.0 – Jan 2026". If revisions are made later, update accordingly. This avoids confusion which draft is final.
- **Executive summary**: Provide a one page executive summary at the very front of the documentation pack highlighting key findings and affirming that issues were resolved. Executives and regulators love concise summaries.
- **Highlight compliance**: In your documentation, explicitly mention compliance with whatever regs: e.g. "This exercise fulfils the requirement in EBA Guidelines EBA/GL/2024/14 for annual screening system

testing. It also addresses points raised in the FCA's sanctions review, specifically improving calibration oversight and documentation."

- **Cross-reference evidence**: When writing the report, cite where details can be found. For instance, "(See Appendix B for full list of test cases and outcomes)" whenever you state a result. This helps show you have backing for statements.
- **Be honest**: Document both strengths and remaining weaknesses. If there is something that's not perfect but acceptable (e.g. "False positive rate is 5%, which is an improvement from 20% and considered acceptable given our customer profile"), state it along with reasoning. Transparency is better than trying to hide a minor imperfection, regulators appreciate candour and rationale.
- **Keep context with data**: If you have stored raw output files, consider adding a readme explaining what they are, so that someone looking at the folder later understands, for example, "alerts_export_17Jan26.csv" corresponds to initial test run results.
- **Backup the documentation**: In addition to primary storage, consider a backup copy (especially of critical evidence files) in line with your firm's data backup practices. If these are needed years later (e.g. in an inspection or if something goes wrong and you need to show due diligence), you don't want them lost due to a drive failure or personnel change.
- **Example documentation package**: Imagine a PDF combining: Title page, Exec summary, Main report, Appendices (test case table, metrics graph, change log, sign-off sheet). Alongside, you have a folder with raw data like "TestDataUsed.xlsx," "AlertsBefore.csv," "AlertsAfter.csv," and "ChangeLog.txt." Someone reviewing can match the summary claims to those files if needed.
- **Continuous monitoring link**: Note in documentation how ongoing monitoring will catch any drift. For instance, "We will produce monthly metrics on sanctions screening alerts (hit rates, etc.) to ensure the system continues to perform as expected, which will be reviewed by the Financial Crime Compliance Committee." This shows that it's not a one-and-done, but part of an ongoing control process.

Common Pitfalls:

- **Documenting in a rush or superficially**: Sometimes teams, after the intensive testing, produce scant documentation because they're drained or assume it's obvious. This is a mistake. Regulators may only see your documents, not the hard work behind them. Spend the time to make them clear and comprehensive.
- **Not preserving key evidence**: If you saw critical failures and fixed them, make sure you have evidence of the before and after. For example, you might be asked, "How do you know those issues are resolved?" If you didn't save the initial error screenshots (because you fixed it and moved on), you lose a bit of story. Keep those "before fix" and "after fix" pieces in the record.
- **Lack of sign-offs**: If your process required approvals, but you don't save proof of those, an auditor might flag that governance wasn't followed. Make sure all approvals (plan, changes, final acceptance) are documented, even if just an email thread printed to PDF.

- **Disorganised files**: If documents are scattered in personal folders or not labelled, people may not find them. Use a logical structure and perhaps an index document listing all items. Consider if someone new had to find everything, make it easy for them.
- **Forgetting integration**: Not updating policy docs or compliance registers to mention this test is a missed opportunity to embed the activity. Also, if an issue revealed a need for policy change (say, screening process needed an update), ensure that change is made and documented.
- **Not scheduling follow-up**: Ensure that documentation includes the plan for the next test or any outstanding tasks (like "Vendor will deliver patch in 2 months. Will test patch on receipt"). If you skip this, it might be forgotten. Regulators might ask, "when will you test again?". You should have an answer documented ("next annual test scheduled for Jan 2027").
- **Failure to distribute/share findings**: If results aren't communicated to relevant parties (e.g. those in charge of related areas), then the exercise loses some value. For instance, if you found data quality issues, the data governance team should be informed to prevent recurrence. Make sure your documentation (or a tailored subset) reaches those who can act on any broader recommendations.
- **Destroying or altering records**: This should go without saying, but maintain the original records of the test outcomes and changes. Do not be tempted to "clean up" things like removing evidence of initial misses out of fear it looks bad. It's far better to show, "We found this problem and fixed it" than to pretend it never happened. Regulators understand systems need tuning, a cover-up is much worse than an initial imperfection.

compliance assist

Checklist – Document Everything:

- [ ] **Comprehensive summary report written**: A final report or documentation package exists summarising the entire testing process, findings, actions, and final status. It provides context, methodology, results, and conclusions in a clear narrative.

- [ ] **Test plan and scope archived**: The original plan (objectives/scope) and any approvals for conducting the test are included in the documentation set.

- [ ] **Test cases and data saved**: The full list of test names, expected outcomes, and actual outcomes (from before and after tuning) is documented and filed (e.g. in an appendix or a spreadsheet).

- [ ] **Analysis and results evidence stored**: Detailed analysis documents, logs, screenshots of alerts and performance metrics are preserved, demonstrating how conclusions were reached. This includes evidence of issues found and evidence of their resolution.

- [ ] **Change log and approvals included**: The log of all configuration changes made during tuning, along with records of who approved them, is part of the documentation. Any relevant approval emails or meeting notes are saved.

- [ ] **Management sign-off documented**: Final acceptance or acknowledgment from a responsible executive (e.g. Head of Compliance/MLRO) that the system has been tested and tuned to their satisfaction is recorded (via signed memo or email).

- [ ] **Integration into policy/records**: Relevant policies, procedures or risk assessment documents are updated to reflect this testing (including date and summary of outcome). The fact that a sanctions screening test was done and its outcome is noted in compliance program records.

- [ ] **Next test or monitoring scheduled**: Documentation notes when the next testing cycle or review will occur (per regulatory expectation or internal policy) and any conditions that would trigger an earlier review (e.g. major system change, new regs).

- [ ] **Documentation accessible and backed up**: All documents and files are stored in the designated compliance repository with appropriate access for future reference. Backup copies are secured according to data retention policies.

- [ ] **Optional – External communication prepared**: If required, a summary of results has been prepared for regulators, external auditors or at least internal docs are in a state ready to support such communication if needed.

- [ ] **Lessons learned noted**: Any recommendations for process improvements (e.g. better test data management, system enhancements, training needs) gleaned from this exercise are documented and assigned for follow-up so that the testing process and system governance continue to improve.