compliance assist

Step 2: Define Testing Objectives

Purpose and Importance

Define exactly what you want to achieve with this testing initiative. Clear objectives ensure the testing efforts are focused, measurable and aligned with both regulatory expectations and your institution's risk tolerance. Regulators in the UK and EU are looking for both effectiveness (are you catching what you should?) and efficiency (are you minimising noise) in your screening systems. For example, the FCA observed that firms with well-calibrated systems could *demonstrate* their tools were appropriate for their risk level and had metrics to measure performance. By setting specific goals (e.g. "No critical sanctions hits are missed" or "Reduce false positives by 20%"), you create targets to test against and later demonstrate improvement. Objectives also help gain management buy-in and allocate resources by articulating why this testing matters (e.g. to comply with new EBA guidelines or to address a previous audit finding). In short, this step turns a broad mandate ("test the system") into concrete success criteria, answering: *What will a successful testing outcome look like?*

Key Activities and Decisions

- **Articulate success criteria**: Decide on a handful of key goals. Good objectives are SMART – Specific, Measurable, Achievable, Relevant, Time-bound. For instance: "Identify and remediate any configuration issues causing the system to miss true matches (zero false negatives in test results)" is specific and measurable. Another might be "Improve the true positive to false positive alert ratio from 1:5 to at least 1:3" (making it measurable and tied to efficiency). List out these criteria clearly and set target dates.
- **Align with risk appetite**: Ensure objectives reflect your firm's tolerance for sanctions risk. If you have a zero-tolerance policy for sanctions misses (which most do, due to strict liability), then an objective about eliminating false negatives is critical. If your firm has been struggling with alert volumes, an objective on optimising alert quality (reducing trivial alerts) might be included, within the bounds of not increasing risk. Essentially, tailor goals to what matters most given your business and risk profile.
- **Reflect regulatory requirements**: Map objectives to any regulatory commitments or guidance. For example, the EBA guidelines require demonstrating "reliability and integrity of alert generation", you might interpret that as an objective to test that all required data fields (name, DOB, etc.) are being screened properly and consistently. The FCA expects screening tools to be "appropriate for the sanctions risks [the firm] is exposed to", an objective could be to validate calibration for specific risk areas (e.g. if you have many clients from a sanctioned region, ensure the system handles those names well). If you have any specific regulatory findings (e.g. an examiner previously said "reduce false positives"), include an objective to satisfy that.
- **Define scope boundaries**: Clarify what is included or excluded in this testing round. Are you testing just the name-matching algorithm or the end-to-end process from data entry to alert handling? Will you cover all business units or focus on one first (e.g. retail banking clients now, corporate payments later)? Set boundaries like "we will test individual customer screening, not transaction screening, in this phase" or "we focus on the main screening engine and will not assess the case management workflow." This ensures the team stays on track and can manage workload. You can always expand scope in future iterations.
- **Determine test type and frequency (if applicable)**: Decide if this is a one-time catch-up test or part of a regular program. Given EBA's guidelines for annual reviews, you might establish that "this is our 2026 annual validation of the sanctions screening system." If you plan multiple rounds (initial test, then re-test after

tuning), outline that: e.g. "Objective: By the end of Q1, complete initial testing and implement fixes. By Q2, demonstrate improved metrics in a second test run." Time-bound aspects like this help create urgency and structure.

- **Secure stakeholder input**: Before finalising objectives, discuss them with key stakeholders, e.g. the MLRO (Money Laundering Reporting Officer), Head of Compliance or IT system owner. They might have additional goals or constraints. Importantly, getting their agreement now means you have support later, especially if objectives tie into their interests (like satisfying a regulatory expectation or reducing workload in their team). For instance, Operations might strongly support an objective to cut false positives by X%, as it directly eases analyst burden.
- **Document the test plan**: Write down the objectives and scope in a "test plan" document or charter. Include also the team members involved, timeline, and governance (who will receive results, who approves changes, etc.). This doesn't have to be lengthy, but formalising it helps communication and will be part of your audit trail. It can start with a simple statement: "The objective of this exercise is to validate and improve the effectiveness of [Your Company]'s sanctions name screening system. Specifically, the goals are: 1)… 2)… . Scope: … . Out of scope: … ."

Practical Tips and Examples

- **Balance objectives**: Include at least one objective for effectiveness (no misses) and one for efficiency (manageable alerts), since regulators care about both. For example: "Ensure 100% detection of listed entities (effectiveness) while maintaining a false positive rate below X% for common customer names (efficiency)."
- **Use previous incidents**: If your organisation had any sanctions near-misses or breaches, use those as guidance. E.g. if last year an internal review found a sanctioned entity went undetected due to a name variant, a natural objective is "test and eliminate any weaknesses in detecting name variants of sanctioned entities."
- **Keep it realistic**: While "zero false positives" is ideal, it may not be realistically achievable without enormous cost. It's okay for objectives to aim for improvement rather than perfection (aside from false negatives, where zero really is the aim). You might state "reduce false positives by 30%" instead of "eliminate false positives entirely," acknowledging a practical balance.
- **Example objectives set**: Consider a scenario: A fintech company sets these objectives, (1) Coverage: Verify the system is screening against all required sanctions lists (UK, EU, US) and catching all sample designated names. (2) Accuracy: Fine-tune so that at least 90% of alerts correspond to actual sanctions or true close matches (improve precision). (3) Audit readiness: Document the system's performance and tuning such that we meet EBA's 2025 guideline requirements. These cover compliance and performance and the third explicitly addresses documentation, which can be an objective too.
- **Prioritise high-impact scenarios**: If your resources are limited, you might prioritise objectives. For example, "focus on EU/UK list names because that's our obligation; de-prioritise OFAC-only names in this test." It could be part of scope definition. Just be sure you're still covering what regulators expect for your jurisdiction.
- **Get management sign-off**: Have the objectives approved by the project sponsor or relevant manager via email or meeting. A quick email like: "As discussed, our testing will aim to achieve X, Y, Z by [date]. Please

confirm you're aligned with these goals." Their approval will be useful to point to if priorities are questioned later and demonstrates top-level support.

Common Pitfalls

- **Objectives too vague or broad**: Avoid non-specific goals like "make the system better" or "ensure compliance." These can't be measured. Without clear targets, you won't know when you're done or if you succeeded. This can also make it hard to report results (management will ask "did it work?" and you'll struggle to quantify).
- **Overloading objectives**: Don't set a laundry list of 10+ objectives, that can be unmanageable. Focus on a core set (perhaps 3–5 key objectives). Too many objectives can dilute effort and confuse the team on what's most important.
- **Ignoring regulatory must-haves**: Make sure you haven't omitted something regulators consider fundamental. For example, if the FCA specifically called out an issue in your last examination (e.g. lack of management information on sanctions screening effectiveness), ensure your objectives include something that addresses that (like establishing baseline metrics as part of this test).
- **Setting conflicting objectives**: Be mindful that pushing one metric may worsen another. If you set "zero false negatives" and "50% reduction in alerts," note the potential conflict, you might achieve the latter by raising thresholds but that could conflict with the former. Acknowledge trade-offs and decide which has priority (almost always, effectiveness over efficiency for sanctions).
- **Not communicating objectives to the team**: Everyone involved in the testing (analysts, IT, etc.) should know what the goals are. If, for instance, IT thinks the goal is just to test upgrade readiness, they might not capture metrics needed for false positive analysis. Clear objectives guide everyone's actions.
- **Omitting documentation as an objective**: Since regulators (especially EBA) emphasise documentation, one objective can be to produce a thorough report or to improve auditability of the system. Ignoring that could lead to doing the work but failing to impress regulators due to poor evidence.

compliance assist

Checklist – Review Current Setup

- ☐ **Objectives clearly documented**: A written test plan or charter lists the specific goals of the testing exercise in clear terms.
- ☐ **Effectiveness covered**: There's an objective addressing detection of sanctioned parties (e.g. no missed hits on test data, coverage of all required lists).
- ☐ **Efficiency covered**: There's an objective addressing false positives or alert quality (e.g. reduce noise, improve precision of alerts).
- ☐ **Scope defined**: The scope of testing is explicitly stated (systems, data sets, and scenarios included and any exclusions).
- ☐ **Regulatory alignment**: Objectives take into account relevant regulatory guidelines or findings (e.g. annual EBA review requirements, FCA expectations on calibration).
- ☐ **Risk-based focus**: Objectives reflect the institution's risk profile (targeting the most relevant risks, such as particular geographic name variants if applicable).
- ☐ **Measurable targets**: Each objective has a success metric or criteria (percentage improvement, threshold to achieve, etc.), where feasible.
- ☐ **Timeline set**: If applicable, a timeframe for achieving objectives or completing the testing cycle is defined (especially for iterative test-and-tune processes).
- ☐ **Stakeholder buy-in**: Key stakeholders (e.g. Head of Compliance, MLRO, system owner) have reviewed and agreed to the objectives and scope.
- ☐ **Resources committed**: It's verified that the necessary people, data access, and environment will be available to meet these objectives (ensuring goals are attainable with given resources).
- ☐ **Plan for reporting results**: Criteria for how success will be reported (and to whom) are noted, laying the groundwork for documentation and management reporting.