compliance assist

Step 1: Review Current Setup

Purpose and Importance

Begin by establishing a clear understanding of your current sanctions screening setup. This baseline review ensures the team knows how the system works today and uncovers any immediate gaps. Regulators expect firms to thoroughly understand their own tools – the FCA found some firms *"lacked understanding of how their sanctions screening tools were calibrated and when lists were updated,"* leaving them unsure if they were screening correctly. Similarly, the EBA's guidelines require at least annual reviews of screening systems to assess effectiveness, reliability and performance transparency. A comprehensive review sets the stage for meaningful testing and demonstrates to regulators that you have control and oversight of your sanctions controls.

Key Activities & Decisions

- **Inventory systems and scope:** List all systems or modules that perform name screening. Include customer onboarding screening, transaction/payment screening, trade finance screening, any process that filters names against sanctions lists. Note system versions and whether they're in-house tools or vendor products.
- **Document sanctions lists and update processes:** Identify which sanctions lists are used (e.g. UK Sanctions list, EU consolidated list, OFAC SDN, UN list, etc.). Document how each list is obtained and updated. For example, is there an automatic daily feed, or a manual download? Who is responsible for updates and how quickly do updates occur after a new designation? The FCA expects firms to have SLAs for list updates to avoid gaps.
- **Capture current matching logic/settings:** Record how the system matches names. What matching algorithm is in use (exact, fuzzy, phonetic, etc.)? What are the similarity thresholds or scoring cut-offs? Are there specific rules (e.g. ignore common words like "Ltd.", or require full date-of-birth match for common names)? Note whether the system uses different settings for individual vs. entity names. Essentially, document the configuration that determines when an alert is generated.
- **Map roles and responsibilities:** Identify ownership and governance. Who "owns" the screening system (typically the Compliance or Financial Crime team in partnership with IT)? Who can change the settings? Is there a committee or approval process for changes? Also note who monitors daily alerts and clears them, while not directly about the system, it's important context for later steps (e.g. if certain tweaks might overwhelm analysts).
- **Review policies, procedures and past audits:** Gather any internal procedures on sanctions screening (for example, a procedure document for alert handling or a section in the AML policy on sanctions). If internal audit or regulators have reviewed your sanctions controls before, note their findings or recommendations. These often highlight areas needing attention (e.g. "lack of documentation on system configuration" might have been noted previously).
- **Assess known issues or pain points:** Speak with users and stakeholders. Are there complaints about too many false positives on certain names? Any known instances of false negatives (near-misses where a sanction wasn't initially flagged)? Backlogs in alert handling? Documenting these will help focus your testing on high-risk aspects. For example, if analysts say "We often get alerts for common names that are not matches," that hints at a possible tuning issue to examine.

compliance assist

Practical Tips amd Examples

- **Engage IT early**: An IT representative or system administrator can provide valuable input (and documentation) on system configuration and data flows. For instance, they can extract configuration files or settings screens for you and confirm how the system interfaces with list sources.
- **Regulatory alignment**: Cross-check your findings with regulatory expectations. The FCA's 2023 review highlighted that firms should be able to "show the controls they have in place to measure the effectiveness of their sanctions system's thresholds and parameters". Ensure your review captures any control mechanisms like automated reports or metrics the system produces (e.g. does it produce a monthly false positive rate?).
- **Check for undocumented tweaks**: Often, over time, small tweaks or exceptions are applied to the system (like an "exclude list" of certain names or a custom rule). These can be forgotten. Look for any such customisations. An example might be a rule to not alert on "Johnson, John" because it was producing too many hits, note these, as they may need revisiting.
- **Use a standardised checklist**: Creating a checklist for this step (which this guide essentially is) ensures you consistently capture the necessary information. If multiple people are involved, assign sections (one person gathers list info, another documents matching logic, etc.).

Common Pitfalls

- **Relying on memory or assumptions**: Don't assume you know how the system is set up, verify it. People sometimes say "Oh, I think we update the list daily" without checking, that's dangerous if wrong. Always get actual data or system information where possible.
- **Overlooking ancillary systems**: Remember to include any secondary or edge systems. For example, if a separate screening tool is used just for high-risk customer enhanced due diligence, it should be reviewed too. Regulators will consider all sanctions screening processes in scope.
- **Not involving business units**: If certain departments (like Wealth Management or Trade Finance) have their own screening processes or variations in settings, include them in the review. Global firms sometimes discover that different regions or products use different tools or settings.
- **Ignoring governance gaps**: If you find there isn't a clear owner or no formal change control, don't shrug it off. Note it as a gap, governance issues are a common regulatory criticism. You might set a goal to formalise that in future.
- **Failing to record "as-is" in writing**: Ensure the outcome of this step is written down, e.g. a short "Sanctions Screening Current State Summary" document. It will be used in a later step to show auditors and it's invaluable for new team members or if you do a model validation. If it's only in people's heads, that knowledge can be lost.

compliance assist

Checklist – Review Current Setup

- [ ] **Systems identified:** All sanctions name-screening systems or modules in use are listed (including any regional or business-specific tools).
- [ ] **Sanctions lists and sources documented**: Each sanctions list used by the system is noted, along with how and how often it's updated, and by whom.
- [ ] **Matching logic and parameters captured**: The current configuration of matching algorithms, threshold scores and any special rules are recorded (with source documentation or screenshots if possible).
- [ ] **Roles and governance mapped**: Document who owns the system, who can make configuration changes and what the change approval process is. Note any committees or senior management oversight of sanctions screening.
- [ ] **Relevant policies/procedures gathered**: Any internal documentation relating to sanctions screening (compliance policies, operating procedures, previous audit reports) has been collected for reference.
- [ ] **Known issues and gaps noted**: Existing problems (high false positive rates, any false negatives, resource backlogs, etc.) and any obvious compliance gaps (e.g. no SLA on list updates, no documentation of settings) are listed as areas to address.
- [ ] **Baseline report produced**: A summary of the current state (covering points above) is written and saved, providing a baseline for planning and future audits.