1. Why is it mandatory to align our EWRA with the 2024 NRA, and what happens if we don't?
   The Enterprise-Wide Risk Assessment (EWRA) must reflect the current national risk context. The 2024 NRA identifies new risks (e.g. misuse of VAs, foreign predicate offences, unlicensed actors) and updates sectoral residual risk levels. Failure to align your EWRA means:

   - Your controls may no longer be proportionate to actual risk.
   - Your institution may be rated higher risk by the SCA.
   - You could face findings during inspections or be placed under a Remediation Plan (RMP).

2. How do we identify which typologies from the NRA apply to our business?
   Review the NRA's threat and vulnerability summaries for your sector (e.g., VASPs, brokers, fund managers). For example:

- If you're a VASP, apply the typologies related to:
  - Peer-to-peer transfers
  - Use of privacy coins
  - Unhosted wallets and mixing services
- If you're a broker, consider risks such as:
  - Onboarding offshore SPVs
  - Layering through securities trading
  - Weak UBO documentation in third-party account structures

3. We're a low-risk firm. Do we still need to take action on the NRA findings?

   Yes. FATF and the SCA require proportional application, not exemption. Even low-risk firms must:

- Review the NRA
- Document its relevance (or non-relevance)
- Reassess their EWRA at least once a year

4. How should we reflect country risk updates based on the NRA?

   The NRA identifies countries and regions associated with:

- High TF threat
- High ML threat due to predicate crimes (e.g., fraud, corruption)
- High exposure to unlicensed VASPs

You should update:

- Your geographic risk scoring table
- EDD triggers for clients from high-risk countries
- Transaction monitoring rules to flag flows to/from these areas

5. What documentation is needed to show we've implemented NRA findings?

The SCA expects to see a clear audit trail. You should maintain:

- A summary note showing which NRA risks were reviewed and how they were addressed
- The updated EWRA (clearly date-stamped post-2024 NRA)
- Revised policies and procedures (KYC, monitoring, training)
- Internal memos or board minutes where changes were approved

6. How can we train our staff on the NRA findings?

   You should incorporate NRA content into your AML/CFT training by:

- Creating a summary presentation of the key risks applicable to your institution
- Updating case studies with scenarios from the NRA (e.g., VA layering, nominee misuse)
- Holding a compliance roundtable to discuss how internal policies are changing

7. Do we need to report anything to the SCA after updating our EWRA?

   You are not required to submit the EWRA immediately. However:

- You must retain it for SCA review during inspections or upon request.
- You must reflect the changes in your annual AML Return, especially in the sections related to:
  - Institutional risk
  - High-risk client statistics
  - Controls updated during the year

8. Should we update only our AML/CFT policy, or other documents as well?

   Your AML/CFT policy is central, but other documents must be updated too:

- Onboarding procedures (especially KYC checklists)
- Risk scoring tools
- EDD checklists for PEPs and complex clients
- STR escalation protocols
- Third-party reliance policies (to reflect national vulnerabilities like reliance on unregulated introducers)

9. We are a brokerage firm. How should we apply the NRA's findings related to nominee structures and shell companies?

   As per the NRA, misuse of legal persons is a vulnerability in the UAE. Brokerage firms must:

- Identify if a client is acting on behalf of others, especially if linked to offshore jurisdictions.
- Collect documentary evidence of beneficial ownership and source of wealth.

- Apply EDD when onboarding investment vehicles registered in high-risk jurisdictions or with complex trust layers.

10. We’re a fund manager dealing with GCC clients. Do we need to take action on VA or TF risks even if we don’t hold crypto?

    Yes. While you may not directly handle virtual assets, your investors or underlying clients might. You should:

- Screen for indirect exposure to virtual assets, e.g., investments in blockchain-related instruments.
- Identify if underlying clients use nominee structures that obscure UBOs.
- Update your policies to:
    - Ask targeted onboarding questions
    - Conduct periodic reviews of high-risk clients or asset classes

11. What are practical steps we should take to detect terrorist financing risks mentioned in the NRA?
    According to the NRA, TF risks may be hidden in:

- Charity-linked transactions to high-risk countries
- Use of cash or hawala-like patterns
- Crypto donations with emotional/religious motivations

You should:

- Monitor for structured low-value remittances to high-risk zones.
- Scrutinise customer justifications for recurring crypto outflows.
- Train frontline staff to flag suspicious fundraising or NGO-related activity.

12. Are we expected to conduct a gap analysis between our existing AML programme and the NRA findings?

    Yes, and it’s highly recommended. A gap analysis helps demonstrate that your institution:

- Reviewed each relevant NRA risk
- Mapped controls already in place
- Identified where enhancements are needed (e.g., EDD, CDD triggers, country risk scores)
- Documented progress, including board-level review

13. How should we reflect NRA findings in our product or service risk assessments?

    Each product or service you offer (e.g., VA trading, portfolio management, margin lending) must be re-evaluated in light of NRA-identified vulnerabilities. Consider:

- Which products are more susceptible to anonymity (e.g., crypto withdrawals, offshore trades)?
- Which delivery channels may enable non-face-to-face onboarding?

- Which service features enable high-value, rapid movement of funds?

14. Are there risks from customer profiles that were not previously considered high-risk, but are now flagged in the NRA?

    Yes. The 2024 NRA highlights risks previously under-assessed, including:

- Clients using offshore legal structures with unclear economic rationale
- Individuals sending or receiving crypto assets from unlicensed or non-transparent exchanges
- Cross-border clients linked to countries with weak AML enforcement or public corruption concerns

15. What is the role of senior management or the Board in responding to the NRA findings?

Senior management must:

- Review the impact of the NRA on the business model
- Approve the updated EWRA and risk mitigation plan
- Ensure that changes to policies, controls, and technology are funded and implemented

The Board should be aware of:

- The entity's sectoral risk rating
- How compliance has changed post-NRA
- The inspection/enforcement risk if changes are not made

16. Do we need to update third-party contracts or onboarding forms because of the NRA?

    Yes, especially if:

- You rely on third-party onboarding (e.g., introducers or affiliates)
- You use external technology partners for KYC/monitoring
- Your onboarding forms do not capture indicators now required (e.g., source of VA funds, high-risk geographic ties)

17. How do we evidence that NRA-aligned changes have actually been implemented—not just written in policy

    You should:

- Keep version-controlled policies with highlighted changes and dates
- Maintain staff training logs covering NRA topics
- Document system or process changes (e.g., monitoring thresholds, new risk models)
- Show actual case escalations or decisions influenced by NRA guidance