Module 4: The Risk-based Approach to AML/CTF

Learning objectives

The purpose of this module is:

- to establish the principles and purposes of a risk-based approach to AML/CTF
- to describe risk identification
- to examine methodologies for a risk-based approach to AML/CTF
- to describe the conduct of a risk assessment and offer a checklist
- to examine the design of a risk-based approach.

1. What is risk?

Risk is the effect of uncertainty on objectives. Effect can be seen as a something that might be positive or negative – it is a deviation from the expected.

This definition uses the concept of uncertainty. Uncertainty refers to a state of affairs whereby there is a deficiency of information or understanding or knowledge of an event, or its likelihood or its consequence. When applied to AML/CTF, the risk is that a reporting entity may reasonably face that the fact its provision of designated services might (whether inadvertently or otherwise) involve or facilitate money laundering or the financing of terrorism. An alternative definition of risk is: the chance of something happening that will have an impact on objectives. For example, using the ML/TF risk definition: If a business has an objective to provide designated services to customers for lawful purposes, then ML/TF risk is the chance that customers may use those designated services for money laundering or the financing of terrorism.

Objectives in the context of AML/CTF could be seen as:

- strategic positioning of the quality of the organisation’s AML/CTF programme
- the financial costs of running AML/CTF activities;
- the operational effort involved in accepting new customers;
- the reputation of the reporting entity.

In simple terms risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

Risk is often examined by looking at the likelihood of an event occurring and the consequences if that event occurred. One of the difficult things in ML/TF risk is assessing consequences. The consequences in Malaysia of a customer being involved in money laundering for a reporting entity have not been serious unless the reporting entity has been a willing participant. There has been no incidence of major reputation or regulatory damage to a Malaysian business when it has been involved in suspicious or prohibited transactions, despite this having occurred in a number of instances.
2. What is risk-based regulation?
Increasingly, the current global trend in financial sector regulation is towards the use of a risk-based regulatory approach. Risk-based regulation aims to identify and manage potential risks, or the activities or environment that may result in these risks occurring. The responsibility for identifying, mitigating and managing these risks under a risk-based regulatory regime falls to the regulated entity rather than the regulator. The role of the regulator is to provide the framework within which the regulated sector or entities construct and implement their risk strategies and programmes. The regulator provides the parameters through setting rules and guidelines and providing information to assist in the identification and mitigation processes, and is then responsible for monitoring the development and implementation of those risk strategies by individual reporting entities and enforcing the law and associated regulations and rules.

The rise in the use of risk-based regulatory approaches is partially in response to the limitations of more prescriptive regulatory approaches, which are predominantly compliance and reporting focused and do not necessarily identify and manage risks. The increased preference for risk-based approaches also partially reflects the increased use and sophistication of risk management tools more widely in business, especially in the financial sector, and the increasingly supported view that the reporting entity is in the best position to manage their risks, as they know their own business better than the regulator.

Risk-based regulation can take a number of forms, ranging from the application of selected risk management tools to an overall regulatory approach.

Risk-based regulation has been criticised following the ‘Global Financial Crisis’ (GFC) because many financial firms were regarded as having grossly ignored their risk management responsibilities. The future of risk-based regulation post-GFC has not yet been fully resolved.

3. Key issues for a risk-based regulatory approach
A working definition of the risk based approach is an approach which “identifies ML/TF risks so that a reporting entity can aim its controls at them”.

There are a number of key elements to a risk-based approach that a reporting entity needs to be aware of when constructing its own tailored risk-based AML/CTF.

- One of the advantages of a risk-based approach is that it should overcome the difficulty that compliance activities do not always translate into effective risk management. In other words, a reporting entity may be fully compliant with the regulations, but if those regulations do not accurately reflect the risk of potential money laundering or terrorism financing activities then these compliance efforts will be ineffective in detecting and preventing actual money laundering and terrorism financing activities.

- A risk-based approach allows a reporting entity to develop a tailored AML/CTF risk management strategy and programme that specifically reflects that reporting entity’s operations, environment, customers, products and technology.

- A risk-based approach is less prescriptive and more responsive to changes in risks, which is particularly important when managing the risks of money laundering and terrorism financing activities, which are characteristically highly adaptable. This requires an AML/CTF programme to be sensitive to changes in risk and the environment.

- A risk-based approach relies on correctly identifying how the potential risk of money laundering and terrorism financing to the specific operations of the reporting entity. This is a fundamental consideration when constructing and maintaining an ML/TF risk strategy.
In order for a reporting entity to correctly identify and manage the risks of money laundering, it will not only need to develop and maintain an understanding not just of how these activities occur, but also an understanding of the relationship between money laundering and the underlying criminal activities that generate the funds, including the illicit drug trade, organised crime, tax evasion and fraud, and the relationship between terrorism financing and terrorist activities.

There is a danger, when developing a risk assessment and risk management strategy that silos of risks will be constructed. For instance, the management of risks posed by certain classes of customers might be undertaken without reference to country or product risk, or even without reference to how money laundering and terrorism financing activity operates. In reality, one type of risk is also affected by others, and affects those other risks in turn. This overlooks a fundamental characteristic of risk – risk is relational not linear. In other words, the risk of money laundering activity will translate to the reporting entity across combinations of the key elements of the business (customers, products, channels, countries) and with varying degrees of impact and levels of risk.

4. Interpretation of the risk-based approach
There are varying interpretations of the risk-based approach:

- The FATF released a guidance paper in 2007 which described the risk-based approach as one which encouraged reporting entities to use the risk-based approach to focus on their higher ML/TF risks;\(^{42}\)
- The risk-based approach creates an obligation to identify, mitigate and manage ML/TF risks according to the nature, size and complexity of a business;
- The current FATF view – focusing on identifying, assessing, managing and mitigating risks which can be translated as meaning that reporting entities need to identify their specific ML/TF risks so that they can target them.\(^{43}\)

5. Keys to a successful risk-based approach
In its 2007 Guidance on the Risk-Based approach to combating money laundering and terrorist financing, the FATF identified the following elements as necessary to success at the national level.

- Financial institutions and regulators should have access to reliable and actionable information about the threats.
- There must be emphasis on cooperative arrangements among the policy makers, law enforcement, regulators and the private sector.
- Authorities should publicly recognise that the risk-based approach will not eradicate all elements of risk.
- Authorities have a responsibility to establish an atmosphere in which financial institutions need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Regulators’ supervisory staff must be well trained in the risk-based approach, both as applied by supervisors and by financial institutions.
- National requirements and supervision should be consistent between similar industries.

---

42. The FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing published June 2007. By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, so that all financial institutions, customers, products, etc. receive equal attention, or that resources are targeted, but on the basis of factors other than the risk assessed. This can inadvertently lead to a ‘tick box’ approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing.

43. See Malaysia Standard AML/CTF Guidelines, s4.2: Sectoral Guidelines for Banking and Financial Institutions, s3.1.
6. **Ownership of ML/TF risk**

Reporting entities differ on who they allocate ownership of ML/TF risk to. The following have a role:

- the governing board, as the ultimate owners of all risks on behalf of the proprietors;
- the chief executive officer, as the person with operational responsibility for the reporting entity;
- heads of business units or streams who receive bonuses for the amount of revenue their area earns, because revenue earned must be balanced against risk assumed.

The following is an extract from the Joint Money Laundering Steering Group (JMLSG) *Guidance for the UK industry Part 1* (see page 34):

A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm’s philosophy, and as such reflected in its procedures and controls. There needs to be a clear communication of policies and procedures across the firm, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Many organisations place ML/TF risk with the compliance function. Management of ML/TF risk is more of an operational risk than a compliance risk, but those that generate returns on the taking of risks should be accountable for the assumption of risk. In ML/TF terms this translates to the quality of:

- customers accepted
- transactions performed
- channels used
- agents and intermediaries used
- countries involved.

7. **The three main categories of risk-based controls**

Controls usually address customer acceptance, ongoing customer due diligence (including monitoring) but are usually silent on product controls. Product controls are also capable of being designed and used as risk-based AML/CTF controls. A fuller list of controls is given in section 24.3 of this module.

There do not appear to be any controls outside these three broad categories. All actions that a reporting entity might take to mitigate ML/TF risk fall within these three categories. ‘Channel’ falls within product controls since it is the product that is supplied through a channel; it can also fit within ‘customer acceptance’ since customers are always derived through a specific channel. Country risk falls within all three controls.

International examples of **risk-based customer acceptance controls** in action:

- All customers with identification documents from higher ML/TF risk countries are required to produce proof of their right to reside in a jurisdiction.
- All customers investing above a certain amount in a managed investment scheme should be required to provide information about source of funds and source of wealth within the first three months of the relationship.
- All customers establishing an on-line relationship with an Foreign Exchange (FX) dealer should be required to provide the account details of their Australian bank accounts and may only remit funds to the FX dealer using that account.

44. Each example is a choice that might be made by a reporting entity about how to manage ML/TF risk. None of the examples are mandatory.
All customers accepted prior to a certain date, e.g. December 2007, should have their information upgraded to current standards by, say, December 2013.

Examples of **risk-based monitoring controls** in action:45

- A reporting entity which has experienced a high level of suspicious activity reports at a particular branch may give more attention to monitoring alerts involving that branch.
- All customers could be attached to a profile based on their occupation and estimated income, and monitoring rules would look for discrepancies between income and transaction volumes and value.
- Businesses that are not cash-intensive are monitored for unusual cash activity.

Examples of **risk-based product controls** in action:46

- Some managed investment schemes will not make third-party payments on redemption of units.
- Application for property financing usually involves providing information about the applicant’s source of wealth and source of funds in order to establish the credit worthiness.
- International telegraphic transfers above a certain amount may require supporting documentation.
- Some reporting entities will not accept cash or will not accept cash above a certain amount.
- Access to safe-deposit boxes may require fingerprint scanning which acts as a form of identification as well as authentication.

8. **Nature, size and complexity of the reporting entity**

Risk-based controls cannot be designed without reference to the nature, size and complexity of the reporting entity’s business. All AML/CTF programmes should document information about:

- Revenue flows by designated service
- Transactions numbers and typical amounts or ranges of amounts
- Numbers of customers
- Demographics of customers (type, business sector etc)
- Risks which are specific to certain business units or designated services
- Numbers of employees and roles
- Offices in the country
- Degree of dependency on technology
- Customer acceptance channel
- Fulfilment channels
- Complexity
- Geographical diversity
- Overseas market targets
- Use of intermediaries, agents and outsourcing
- Size relative to peers.47

9. **Designing risk-based controls**

A control system should be designed with reference to the nature, size and complexity of each reporting entity’s business. It is important to understand that not everything is risk based. The risk-based elements affect:

---

45. Each example is a choice that might be made by a reporting entity about how to manage ML/TF risk. None of the examples are mandatory.
46. Each example is a choice that might be made by a reporting entity about how to manage ML/TF risk. None of the examples are mandatory.
47. See paragraph 3.21 of the FATF Guidance on the risk-based approach.
customer acceptance procedures
ongoing customer due diligence and monitoring
enhanced customer due diligence
employee due diligence
role-based training (customised training according to business lines)
assurance.

Reporting entities should manage their ML/TF risk assessment within the context of their existing operational risk frameworks. While identification and management of ML/TF risk has unique requirements, the methodologies used should be consistent with the overall operational risk framework already in use in the reporting entity.

International experience to date suggests that implementing an AML/CTF framework using a risk-based approach is not straightforward.

10. **Control mapping**
A common and wide spread fault of AML/CTF programmes is that AML/CTF controls are not connected (mapped) to the ML/TF risk assessments. The reasons for this may be:

- there is no requirement to make this express connection; or
- people do not understand the risk-based approach; or
- a combination of those two reasons.

It is difficult to see how an AML/CTF programme can operate effectively unless the selected controls are mapped back to the ML/TF risks that have been identified. In this way:

- gaps in controls can be seen;
- controls can be fine-tuned to different risks;
- controls can follow changes in the business;
- changes to controls can be applied to all aspects of the affected operations; and
- management can see the extent of the programme's coverage.

11. **Risk indicators**
The sum of the ML/TF risk assessment and the risk-based approach is a set of risk indicators. These risk indicators tell a reporting entity whether or not an identified ML/TF risk is or is not present. Examples:

- A reporting entity has decided in its ML/TF risk assessment that customers with overseas addresses are higher ML/TF risk. Overseas addresses are therefore a risk indicator. The customer acceptance procedure (a control) collects addresses and where an address is an overseas address then that customer has a characteristic of higher ML/TF risk. The reporting entity may then require further information from the customer such as their source of funds and why they are conducting a financial relationship outside of their own country and perhaps require a higher standard of verification of identity. It may also subject the customer to a higher standard of monitoring during the life of the account.

- A reporting entity may decide in its ML/TF risk assessment that funds being sent to or received from countries it regards as offshore financial centres are higher ML/TF risk transactions. Offshore financial centres remitting or receiving funds from the reporting entity are risk indicators. The transaction process collects details of the country where the funds are being sent to or coming from; and where a country is an offshore financial centre then the transaction has a characteristic of higher ML/TF risk. The transaction and the customer may be investigated, including seeking further details of the purpose of the transaction and the source of funds.
A reporting entity may decide in its ML/TF risk assessment that structuring of cash deposits is higher ML/TF risk. Multiple cash transactions between 30,000 – 40,000 RM daily over a short period is a risk indicator, and should be monitored as such.

11.1 Iterative and dynamic relationship
There is an iterative relationship between the ML/TF risk assessment, ML/TF risk indicators and the risk-based approach. The ML/TF risk indicators are produced as a result of both the ML/TF risk assessment and the operation of controls. Changes in controls may change ML/TF risk indicators. Changes in the ML/TF risk assessment will change ML/TF risk indicators which will change controls.

11.2 Summary
- The relationship between the ML/TF risk assessment, the ML/TF risk indicators and controls is iterative and dynamic.
- There are three controls that can be used to mitigate ML/TF risk – Know Your Customer, Monitoring and Product controls.
- Best practice dictates that a control library linking controls and ML/TF risks is an essential part of an effective AML/CTF programme.

12. Impacts of the risk-based AML/CTF approach
The main impacts of the AML/CTF risk-based approach for a reporting entity will be:
- The reporting entity has the primary responsibility for identifying, mitigating and managing the risk of money laundering and terrorism financing activities occurring.
- The reporting entity will have to construct and apply a tailored risk assessment methodology that reflects the specific operational aspects of the business and translates the risks posed by money laundering and terrorism financing activities to the reporting entity’s business.
- All ML/TF risk assessments are data hungry. The data they need about customers, products, channels and countries often does not exist or is not readily obtainable within a reporting entity, making completion of the assessment problematic. This can corrupt the process of designing an ML/TF risk assessment because there may be a tendency to look only at ML/TF risk that can be quantified or identified.
- A regular review of the ML/TF risk assessment approach, and of the identified risks that inform that risk assessment, needs to be undertaken as part of the overall AML/CTF risk-based approach.

13. Basic concepts of risk assessment
Risk methodology
In order to conduct an ML/TF risk assessment there needs to be a method, an approach to guide the assessment. The methodology is different from the assessment; it is the recipe which produces the assessment. Methodologies should be reviewed regularly. Methodologies should always be documented.

Inherent risk
Is the level of risk before it is treated or mitigated by controls. ML/TF risk assessments look first at inherent risk. After the design and implementation of AML/CTF controls, in combination with other business controls, inherent risk is reduced to residual risk.

Residual risk
Is the level of risk remaining after AML/CTF controls and other business controls have been implemented.
Risk assessment
An ML/TF risk assessment produces the information that a reporting entity can use to construct its risk-based approach. How a reporting entity performs its risk assessment depends on a number of factors, including the nature of its business, the countries in which it has businesses, its customer base, and its general risk assessment processes. The ML/TF risk assessment should be consistent with other operational risk frameworks deployed in the business. ML/TF risk assessments should be repeated regularly, at least annually.

It is not recommended that reporting entities create a separate methodology from other operational risk methodologies to assess ML/TF risk.

Risk-based approach
A risk-based approach is the entirety of all the actions that a reporting entity takes regarding those areas where it is permitted to use risk-based systems and controls to meet its obligations. It is driven by the ML/TF risk assessment. The risk-based approach used by a reporting entity depends on the reporting entity’s risk appetite, among other things.

Risk appetite
Risk appetite describes the approach a reporting entity takes to risk. A risk-based approach does not mean that a reporting entity may approach its AML/CTF obligations with a vigorous appetite for taking risks. It does not mean that risks rated at the lower end of the scale can be ignored. More risk-averse reporting entities are likely to have more and stronger AML/CTF controls than those with greater risk appetites.

The clearest view of the risk-based approach is the view in this course which is aligned with the current views of the FATF; namely, that by knowing its ML/TF risks a business can point its controls squarely at those risks. Controls are not designed in a vacuum but instead are designed with the ML/TF risks they are addressing in mind.

Risk indicators
A risk indicator is something that points to the presence of a risk. For example, the fact that a stored value card might be able to be used anonymously in any automatic teller machine in the world and does not have identification information visible on the card is both an indicator of mobility and of anonymity.

Controls
A control is a process, policy, device, business practice, procedure, tool or other action or device that acts to minimise negative risk or enhance positive opportunities. A reporting entity should be encouraged to use appropriate risk-based controls. When deciding what an appropriate risk-based control is, a reporting entity must have regard to the nature, size and complexity of its business, as well as to its ML/TF risk.

14. The theory of identification of ML/TF risks
A reporting entity should identify, manage and mitigate the risk of potential money laundering and terrorism financing activity that it may reasonably face. A reporting entity should ensure that its AML/CTF risk assessment methodology is consistent with other risk assessment methodologies it uses for other types of risk, and that it is based on its specific business characteristics.

The identification of ML/TF risk involves:

- Identifying the risks of potential money laundering activity and terrorism financing activity based on an understanding of these activities. Decisions will be required regarding how this information will be obtained and used, and how it will be kept up to date.
Module 4: The Risk-based Approach to AML/CTF

- Identifying the vulnerabilities specific to the sector of the financial industry that the reporting entity is involved in, so that these risks can be factored into the ML/TF risk strategy and management programme for the reporting entity.

- Identifying the specific organisational risks that apply to the circumstances and operating environment of the reporting entity. These risks may include the type of business operations the reporting entity is involved in (for example, wholesale banking and funds management), the type of branch network that operates, the technology used, or any overseas operations and types of business relationships with parent companies or related entities. These risks can be factored into the ML/TF risk strategy and management programme for the reporting entity.

This provides the basis on which to develop indicators of potential money laundering activity. It is these indicators that provide the basis of the ML/TF risk assessment methodology.

A reporting entity must decide whether it will:

- encapsulate all risks of potential criminal activity that occur within its business, including customer, employee and third party fraud, tax evasion, identity fraud, and may include activities like insider trading; or

- focus more narrowly on the activities of money laundering and terrorism financing.

If a reporting entity adopts the second approach and focuses on money laundering and terrorism financing, then the risk assessment process must be linked and informed by other, separate risk assessment processes that detect possible criminal activity associated with its business, especially any anti-fraud systems. Fraud and tax evasion are common underlying criminal activities that generate funds to be laundered. If a financial fraud is committed within your business, then the very movement of the funds once the fraud has been perfected is money laundering. Identity fraud is a very strong indicator of other criminal activity, especially terrorism financing and financial fraud leading to money laundering.

An annual review of the identified money laundering and terrorism financing risks is recommended. Money laundering and terrorism financing are highly adaptive criminal activities that take advantage of weak points and changes in opportunities. This means that the risks identified in an ML/TF risk assessment process need to be reviewed regularly to determine if they are still relevant, and new potential risks need to be identified and incorporated into the risk assessment. Part of this review should also be informed by the reporting entity’s experience of potential money laundering and terrorism financing activities over the previous period.

15. Special consideration – combating the financing of terrorism

The process a reporting entity has used for assessing its money laundering risk can be used for assessing terrorism financing risk. The information and data used will be different, however, because the terrorism financing risk assessment involves identifying the key characteristics of terrorism financing (not money laundering), and constructing common methods of terrorism financing (not money laundering) within the sector of the industry in which the reporting entity operates, taking into account the specific characteristics of its business.

This provides the basis on which to develop indicators of potential terrorism financing activity. It is these indicators that provide the basis of the terrorism financing risk assessment methodology.

Identifying the risks associated with terrorism financing activities is much more difficult than for money laundering, as there is less information available and less research has been undertaken. However, this may increase over time. In order to accurately identify
the risks the reporting entity will still need to develop an understanding of terrorism and financing methods, and this understanding will need to be developed as more information and analysis becomes available.

15.1 Wolfsberg’s view on CTF and the risk-based approach
The Wolfsberg Guidance on the risk-based approach specifically chose not to address a risk-based approach for identifying potential risks associated with terrorism financing because it did not believe such a methodology could be effective. The Group sees terrorism funds as indistinguishable from other funds and generally not derived from illegal activity. Instead, the Guidance states that it is for governments to identify those associated with terrorism financing and provide that information to financial institutions in a timely manner.

Reporting entities struggle to distinguish funds being laundered from legitimate funds so there is significant merit in the above views on terrorism financing.

15.2 Higher ML/TF risk is still acceptable business
Just because a customer or transaction is rated as higher ML/TF risk does not mean it should be rejected. It simply means that controls to mitigate the ML/TF risk need to be deployed if the customer is to be accepted or the transaction performed. A function of risk appetite is to define the boundaries of where higher ML/TF risk exceeds the appetite of the reporting entity.48

16. The principles underlying a risk assessment
Reporting entities are not expected to eradicate ML/TF. They are expected to make it harder. If the only fishing net being used is one which can only stop anything bigger than a small whale, then all the other fish will swim through undetected and untrapped. As the fishing net is gradually made of smaller and smaller holes, fewer fish can swim through undetected and untrapped.

A common approach to the risk process is to adopt the following steps.

- Risk identification (to create a comprehensive list of risks).
- Risk analysis (understanding the identified risks).
- Risk evaluation (brings into play the concept of risk appetite and tolerance by looking at which risks need treatment and the priority for treatment).

This process is refined and extended later in this module.

16.1 Existing Operational Risk Methodology
Work with the existing operational risk methodology within the reporting entity is the most appropriate framework to guide qualitative and quantitative measurement of ML/TF risk. Reporting entities should review the requirements of their operational risk methodology and ensure that they incorporate the information requirements of the methodology into the work done on ML/TF risks.

16.2 Understand key terms and setting the scope of the assessment
When preparing to design and conduct an ML/TF risk assessment, an AML/CTF Officer must first understand and/or decide:

- The definition of ML/TF risk in the legislation and regulations;
- The definition of risk in use within their reporting entity;
- The scope of the ML/TF risk assessment – e.g. does it include or exclude all sanctions?

48. See the Wolfsberg Guidance on the risk-based approach.
The definition of customer type – e.g. individuals, sole traders, companies, trusts, partnerships, registered cooperatives, incorporated and unincorporated associations and government entities;

Types of products and services – is the product or service required to be covered by the ML/TF risk assessment?

Legal prohibitions on certain customers under sanctions lists.

16.3 A Multi-dimensional approach to risk
Reporting entities should avoid a silo approach to ML/TF risks. Although risks will be looked at from the separate perspective of customers, products, channels, geography and employees, it is also important that the relationships between these are also assessed.

Higher ML/TF risk customers may use lower ML/TF risk products and vice versa. Good people come from higher ML/TF risk countries and bad people may come from lower ML/TF risk countries. Controls that are built to relieve compliance burdens on lower ML/TF risk products, channels, countries and employees may be abused by higher ML/TF risk customers.

Money launderers and terrorism financiers do not wish to stand out – so they will be mimicking behaviour and attributes of the normal bell curve for a customer, product, transaction, channel or country.

Remember the three-dimensional toy called the Rubik’s cube invented in 1974. It is an excellent way to think about ML/TF risk because it is relational not linear. Once you introduce the concept of relation, it shows that the factors of customers, products, channels, geography and employees all come together either as opportunities for money launderers or terrorism financiers, or conversely, as barriers to their activities.

17. Key characteristics of a ML/TF risk assessment
A reporting entity should be able to demonstrate that its ML/TF risk methodology:

- Deals with money laundering and terrorism financing separately;
- Includes assessment of organisational weaknesses associated with processes and procedures;
- Covers the four factors that should be considered (customer types (including PEPs), types of designated services, delivery channels and foreign jurisdictions with which it deals);
- Deals with the ML/TF risks of employees;
- Has the means to measure and act on changes in the reporting entity’s ML/TF risk internally and externally;
- Covers the types of ML/TF risks that its peers in the industry have covered in their risk assessments, and if it does not, the reporting entity needs to demonstrate that there is good reason why these are not covered;
- Covers risk indicators gathered from suspicious activity reported by the reporting entity in the past. This type of information helps to guide analysis of likelihood and consequence;
- Incorporates feedback received from regulators on the reporting entity’s management of ML/TF risk;
- Incorporates current and emerging trends in money laundering and terrorism financing in Malaysia, and where relevant, overseas. This type of information is also useful in the guidance of likelihood and consequence;
- Is linked to the reporting entity’s change control processes; and
- Is reviewed periodically for efficacy.
A good risk assessment methodology will be one that:

- Sets out clearly how it works;
- Leverages external and internal information;
- Is easily updated; and
- Can be explained and, if appropriate, operated by staff in business units.

17.1 Change management
Changes and additions to employee roles, products, customer groups, businesses, business systems and processes and technological developments need to be considered within the risk assessment methodology. Strong links are required between the risk assessment methodology and the change management processes of the reporting entity.

18. Beyond the risk assessment
It should be noted that a risk assessment of customers, products, delivery channels and country connections does not just mean assessing these groupings and taking no other action. An ML/TF risk assessment must be followed by construction of the reporting entity’s risk-based approach through control design and control mapping.

19. How micro must the ML/TF risk assessment be?
Depending on the nature, size and complexity of an organisation, ML/TF risk assessment may be macro or micro. The essential test will be whether a reporting entity knows what the ML/TF risks are of their customers and the transactions they undertake. Many organisations will assess ML/TF risk at the individual customer level during the acceptance process. This requires systems and possibly, technology. This approach does not covering the risk represented by existing customers, where there might be inadequate data held about their risk indicators.

Performing the ML/TF risk assessment at the individual customer or transaction level is best considered as a control since it is implementing the ML/TF risk methodology.

20. Preparing to conduct an ML/TF risk assessment
In order to conduct an ML/TF risk assessment, AML/CTF Officers need to assemble or have engaged the following:

- A list of all products and services supplied by the reporting entity;
- Information about the characteristics of the products and services sufficient to know their vulnerabilities and strengths in the hands of money launderers and terrorism financiers;
- The channels through which the products and services are delivered;
- A list of all customer types that acquire the reporting entity’s products and services;
- The channels by which the reporting entity acquires customers and services;
- What agents and intermediaries the reporting entity uses to deliver products and services and/or acquire customers;
- What products and services and customers involve overseas countries;
- The different roles of employees and the AML/CTF functions they perform, e.g. customer acceptance, fulfilment, monitoring, etc.
- The business owners of customers, products and services and channels, as they are the true owners of ML/TF risk including its risk assessment;
- The reporting entity’s operational risk methodology.

21. Illustration of a risk assessment methodology
As shown, the process is a series of simple steps. Each step has two aspects: one to cover money laundering, and the other to cover terrorism financing.
21.1 Step 1 – Predicate crime and ML/TF method

21.1.1 Identifying the inherent risks of money laundering in a reporting entity’s business

This requires you to understand:

- How money laundering works. You need to understand the three stages of money laundering – placement, layering and integration.
- The underlying crimes that generate the funds to be laundered (sometimes these crimes are called the predicate crimes). The major groupings of these criminal activities are the illicit drug trade, organised crime activities, fraud, tax evasion, computer crime and identity crime.
- The relationship between the underlying crimes and money laundering activities. Different criminal activities and different kinds of criminals tend to favour different methods of money laundering. Often the laundering method selected reflects existing criminal structures or practices. For instance, organised crime money is often laundered through legitimate business fronts because these already exist to enable other organised crime activities.
- What the different forms of money laundering would look like to your business. If organised crime money uses legitimate business fronts then your risk indicators will involve factors associated with private companies in cash or high-volume businesses.
- What experience your reporting entity has had in recent times of possible money laundering. You can obtain this information from analysing suspicious activity reports filed over chosen periods and analysing transactional data using rules which aim to detect unusual activity. Unusual and suspicious activity detected from this type of data can then be reviewed to identify the defining characteristics of transactions, customer, channels and countries potentially involved in money laundering.

21.1.2 Identifying the inherent risks of terrorism financing in a reporting entity’s business

This is more difficult and requires you to understand terrorist activities in general and how these activities are structured. For instance, the al Qaeda-style approach to terrorism uses small cells with minimal communication between the cells, whereas other terrorist operations, such as the IRA in the past, have a more organisational and hierarchical structure. By understanding the main structures of the terrorist groups and their key activities, a better understanding can be developed of their need for finance, the ways funds are moved, and preferred financing options. Reporting entities are also expected to consider sanctions lists when addressing ML/TF risk.
The process of constructing risk indicators can be completed by applying actual and potential methods of terrorism financing to the possible use of financial products, services and delivery channels provided by a reporting entity. This requires you to understand:

- The methods used for terrorism financing, including the use of charities and legitimate businesses. Terrorism financing may also be financed through criminal activities such as drugs and arms trading, although the use of criminal proceeds tends to be more location specific.
- What experience your reporting entity has had in recent times of possible terrorism financing. Any activity you detect in this area, even though it is in the past, should be reported to law enforcement immediately and you may need to seek legal advice regarding the position of your reporting entity. The detection method would need to use the characteristics that are said to indicate terrorism financing. It must be understood that these characteristics are not helpful because they generally look like normal transactional behaviour. Anything that is detected is then reviewed to identify the defining characteristics of customers potentially involved in terrorism financing.

21.1.3 How Step 1 is best achieved
Performing this step through engagement with business owners of products, customers and channels. Explain ML/TF to them and then invite them to identify how they would use the reporting entity’s products and services to launder money and finance terrorism. Your briefing to initiate their process should provide them with some examples of ML/TF. In this process it is important to stay focused on inherent risk, rather than dismiss risks because controls are in place to prevent them from happening. Those controls will form part of the risk-based approach and it is important not to overlook the ML/TF risk they address. There are at least two approaches:

- A top down approach of using available research and by evaluating the known methods presented in publicly available case studies and typologies (see the resources already suggested); and
- A bottom up approach of either using the knowledge of businesses within your reporting entity about methods they know of, and/or to develop likely methods.

21.2 Step 2 – Identity risk indicators
21.2.1 Risk Indicators for Money Laundering
In this step you identify the risk indicators that your reporting entity should be looking for, as potential signs of money laundering derived from your understanding of money laundering and common money laundering methods. These risk indicators are what you will use to detect the presence of money laundering risk through your reporting entity’s AML/CTF programme.

The process of constructing risk indicators involves the work from step 1 and identifying what signs you would look for as indicators of ML/TF risk.

21.2.2 Risk Indicators for terrorism financing
In this step you identify the risk indicators that your reporting entity should be looking for as potential signs of terrorism financing derived from your understanding of terrorist activities and common terrorism financing methods. These risk indicators are what you will use to detect terrorism financing through your reporting entity’s AML/CTF programme.

The process of constructing risk indicators involves the work from step 1 and identifying what signs you would look for as indicators of ML/TF risk.
21.2.3 How to complete Step 2

Wholesale banking, retail banking, funds management, broking, derivatives trading, insurance and other financial activities will all experience different money laundering and terrorism financing risks and have different indicators of these risks, as the financial activities undertaken, products offered, customer types and service delivery methods differ between different sectors and between different reporting entities.

Information and research sources for Steps 1 and 2

Steps 1 and 2 call for information, some of which reporting entities are unlikely to possess and will find difficult to obtain. There are a number of books that provide a good overview of money laundering and terrorism financing. These have been listed at the end of this module in the ‘References’ section.

FATF, Egmont and the associated regional groups provide a large amount of information regarding money laundering and, to a lesser extent, terrorism financing. The websites also include some case studies (they are called ‘typologies’ on these websites). Although these case studies are generic they do provide a good general understanding of the most commonly known methods of money laundering (at the time of writing terrorist case studies were not available on these sites, but are to be included in the future).

The Financial Information Units in various countries (particularly the UK and the US) provide some additional information, along with some law enforcement sites such as Interpol.

A number of online journals are also available.

Press reports on cases or alleged cases of money laundering and terrorism financing are useful to identify trends. Press reports also provide some information about current trends in the underlying criminal activities. However, press reports about crime are sometimes highly distorted and present the criminal activity in a stereotyped format.

Discussion with regulators and industry peers regarding AML/CTF programmes, risks and money laundering and terrorism financing methods is invaluable.

The disadvantages of some of the information sources given here are that they are not organised in a way that would make them useful to reporting entities and they are not published in a timely manner, even though they are dealing with highly adaptive (and thus constantly changing) behaviour. The need for more current real-time information about the crimes that are behind the activity of money laundering and about patterns of money laundering is critical.

Expected output from Steps 1 and 2

When you have completed these steps you will have

- a list of criminal types and their likely money laundering methods and associated risk indicators;
- a list of types of organisations and persons that finance terrorism and their likely approaches to terrorism financing and the associated risk indicators.

21.3 Step 3 – Focusing the list of risk indicators

21.3.1 Exclusions and inclusions

This step involves excluding irrelevant risks and adding other risks using scenarios and risks that are identified through changes both within and external to the reporting entity. This gives focus to the risk assessment. A brief explanation of each of the elements is set out below.
21.3.2 Excluding irrelevant risks
Some of the risks identified by Steps 1 and 2 might not be relevant to your reporting entity because of the nature of its business or where it is located. Once it excludes these, a reporting entity can focus on the ML/TF risks that it might reasonably face.

21.3.3 Adding scenarios
Step 3 is one place in which to introduce scenarios that, although not substantiated by available typologies, appear reasonable to include in the ML/TF risk assessment. Scenarios should be obtained from business owners, customer-facing staff and product owners within the reporting entity.

21.3.4 Adding changes to ML/TF Risk
A key characteristic of any ML/TF risk assessment methodology must be its capability to handle changes in risk. Detection of a change might occur through other processes external to the risk assessment methodology or be part of its functionality. All such changes must be able to be managed within the methodology once they are detected. They cannot remain unaddressed until the next periodic review of the risk assessment methodology.

21.3.5 Incorporating feedback from law enforcement
Where law enforcement has provided feedback to the reporting entity about its management of ML/TF risk this can be incorporated into the ML/TF risk assessment methodology in this step.

21.4 Step 4 – Additional sector and organisational risks
In this step the following inputs are added to refine the risks being assessed.

- **Specific sector vulnerability** derived from the methods of laundering money and terrorism financing identified in Steps 1 and 2;
- **Operational risks** associated both with the structure and organisational aspects that are specific to the business, and to the risk profile of the reporting entity itself;
- Risks directly linked to the potential for non-compliance by a reporting entity with its own AML/CTF procedures.

21.4.1 Sector vulnerabilities
Sector, in this context, refers to specific segments of the financial services industry in Malaysia. Examples of sector vulnerabilities are:

- Retail banking is more conducive to the placement of cash for money laundering and for minor credit card or identity fraud.
- Retail banking is more likely to be used to launder funds from the illicit drug trade, as this money tends to be collected in small amounts through multiple deposits into personal accounts with a significant regular transfer to a third-party account.
- Wholesale banking is more conducive to organised crime derived funds; as laundering tends to be undertaken utilising legitimate business fronts, trade finance and derivatives transactions.
- Funds management is conducive to layering, as the flow of funds in and out of managed funds is considerable; it tends to involve larger amounts; and often involves the transfer of money to and from overseas.

21.4.2 Operational risks specific to a reporting entity
These include internal weaknesses (e.g. inaccurate customer databases), risks associated with the locations of specific businesses, risks associated with specific classes of customers, a history of poor relationships with the regulators. They can be separated into the structural aspects of risk and organisational aspects.
Module 4: The Risk-based Approach to AML/CTF

**Structural operational risks**
Operational risks that are structural in nature would include:

- Having an overseas parent company;
- Having an overseas parent company domiciled in a high-bank privacy country, a tax haven, or high-risk country;
- The group structure and the types of business included, such as having a retail banking operation or funds management in the group; or
- Subsidiaries in high-risk countries or countries with less stringent AML/CTF regulations and oversight. In such cases, the application of global AML/CTF requirements may be less stringent than what is required in Malaysia.

These structural aspects represent different operational risks and translate into different vulnerabilities to potential money laundering and terrorism financing activity for a reporting entity. For instance:

- Overseas parent companies, and in particular parent companies either domiciled in high-risk countries or with significant exposures to high-risk countries, are more likely to be targeted for money laundering activity with a flow through to other parts of the business, such as the Malaysian operations that could be used to facilitate moving funds elsewhere in Asia, as fund transfers within a financial group are likely to attract less scrutiny.
- Customer relationships within related organisations or the parent company where funds would be transferred within the reporting entity to subsidiaries in other countries. For instance, the parent company may have a large client exposure to the Middle East, where some of these funds are transferred to Malaysia or invested in Malaysia through a managed fund as part of an international allocation.
- Offshore subsidiaries would enable customers to move money to and from overseas or through currency transactions or derivatives.

**Organisational operational risks**
Organisational aspects of operational risk reflect the business model, customer segments, processes, technology and third-party relationships an organisation has in order to undertake its business. For instance, operational risks that are organisational in nature would include:

- Poor processes or technology;
- Business models with heavy reliance on and use of the Internet for banking and other transactions. These delivery channels are more appealing for laundering and terrorism financing as this method does not require face-to-face contact; transactions are completed quickly and can be difficult to trace;
- Large numbers of accounts and customers who do business involving high-risk countries;
- Business concentrations in trade, international business or derivatives, which are exposed to a higher risk of having money launderers and terrorist financiers as both customers and counterparties. Financial activities associated with trade, international business and derivatives generally involve international fund transfers but also provide easy cover for illegitimate activities;
- A significant number of charity accounts with overseas links and relationships, which tend to be used for moving terrorist-related funds;
- A large number of wholesale managed funds that are not superannuation funds. These funds are more conducive to laundering due to the larger amounts involved; or
- Third-party processing performed by organisations that have been criticised by regulators for the quality of their AML/CTF practices.
Risk of non-compliance with AML/CTF procedures
A reporting entity should have a reasonable understanding of its weaknesses when complying with its own procedures. Some business units might have a greater propensity for such breaches than others. Some classes of employees may have a reputation for these kinds of breaches. These risks need to be added into the risk assessment methodology. There are three phases that organisations typically move through when institutionalising a culture of compliance. These phases are:

- Making a commitment to comply.
- Securing compliance know-how.
- Making compliance a business practice.

21.5 Step 5 – categorising risk indicators
The risks gathered from Steps 1 to 4 need to be placed into categories that permit the reporting entity to assess the level of risk posed by each. Like risks should be placed into the same category. Reporting entities might find it sensible to also organise these risks by business units or lines of operation, depending on their business structure. Examples of such categories will include:

- Customers (including politically exposed persons)
- Products and services
- Delivery channels
- Countries
- Businesses overseas
- Staff
- Business processes
- Business systems (including technology).

Most importantly, this categorisation provides for easy mapping of controls to the different risks.

21.6 Step 6 – Quantifying risk
21.6.1 Purpose of quantification
A reporting entity needs to measure the level of risk it faces. Quantification will depend on the category and the nature of the risk. The operational risk methodology that is in use within the reporting entity is the most appropriate framework to guide qualitative and quantitative measurement of ML/TF risk. The work done in Steps 1–5 provides the information base that most generic operational risk methodologies need.

It is beyond the scope of this diploma to provide a complete operational risk framework for reporting entities that do not have one in place.

The process of quantification assists reporting entities to consider the nature, size and complexity of their businesses (including permanent establishments overseas) in the context of the ML/TF risks they have identified.

Reporting entities can gather data about risk factors as evidenced in their existing customer base, if they have such data, which will then allow them to refine their risk-based approach accordingly.

The objective of this step is to develop a quantitative understanding of the relationship between the risk indicators identified and the operations of the reporting entity. Where an item in a risk category records a significant number of occurrences then this risk probably needs a higher risk ranking, score or profile.
Quantification can involve ranking or rating/scoring, or profiling. Regardless of the way a reporting entity ranks, scores or profiles risk, its approach is informed and based on the relevant identified money laundering and terrorism financing indicators generated from previous steps. Ranking, rating/scoring and profiling are explained below.

21.6.2 Ranking
A risk ranking approach is the simplest method because it uses relative rankings. It is the most appropriate for simpler business structures and operations that have generated easily identifiable money laundering and terrorism financing indicators. A ranking approach involves categorising business characteristics such as customers, products, countries, delivery channels, ownership structures and counterparties as high, medium or low risk. Reporting entities might even choose just two categories, higher risk and lower risk.

21.6.3 Rating or scoring
A risk rating or scoring approach involves weighting the money laundering and terrorism financing indicators in terms of the likelihood of those money laundering and terrorism financing risks occurring and the vulnerability to them of the business operations. The weighting is mathematical and the total scores provide a number that is used to measure matters of likelihood and severity.

21.6.4 Profiling
Risk profiling involves constructing customer, product and transaction profiles based on complex risk indicators with multiple relational characteristics. Risk profiling requires advanced data capabilities and is an approach that is most suited to more complex business operations. Risk profiling is also used in monitoring customers and transactions.

21.6.5 What does quantification deliver?
At the end of Step 6, a reporting entity will have an enterprise-wide ML/TF risk profile that represents the sum of all the risk profiles prepared in the business, usually at a business unit level. This ML/TF risk profile represents how money laundering and terrorism financing activities are expected to occur through the reporting entity and highlights those areas of operations, products, technology or customer groups that are conducive to money laundering or terrorism financing activities.

This risk profile should be presented to the board and should be reviewed regularly.

22. Outcomes of the risk assessment methodology
By the end of Step 6, a reporting entity should have:

- An understanding of both predicate crimes and the crimes of money laundering and terrorism financing;
- A comprehensive list of the risk indicators of money laundering and terrorism financing activities that it reasonably faces;
- A quantification of the extent that the risk indicators are prevalent in its business;
- An ML/TF risk profile for its business units and for the enterprise as a whole which has been presented to the Board;
- A process for managing change in ML/TF risks;
- Feedback processes to other activities within the reporting entity which impact on identification, mitigation and management of ML/TF risk;
- Strong links between the risk assessment methodology, the risk-based approach and the change management processes in use in the reporting entity; and
- A review schedule for the risk assessment methodology and the risk-based approach.
23. Summary – a checklist for a good ML/TF risk assessment methodology

<table>
<thead>
<tr>
<th>Does the ML/TF risk assessment methodology in your organisation:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deal separately with money laundering and terrorism financing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have money laundering and terrorism financing risk indicators that reflect the activities of those crimes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include the risk that your staff might not comply with the AML/CTF legislation or the AML/CTF rules or its own AML/CTF Programme?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incorporate the broad sector and the specific organisational risk profile of the reporting entity?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate issues such as customer types (including PEPs), types of designated services, delivery channels and foreign jurisdictions with which the reporting entity deals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have the means to measure and act on changes in the reporting entity’s ML/TF risk assessment internally and externally?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cover the types of ML/TF risks that your peers in the industry have covered in their risk assessments, and if it does not, do you have a good reason why?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cover risk indicators gathered from suspicious activity reported by your reporting entity in the past?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incorporate current and emerging trends in money laundering and terrorism financing in Malaysia, and where relevant, overseas?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undergo periodic review for efficacy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have all the data you need to complete a risk assessment using the ML/TF risk methodology that has been designed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your ML/TF risk assessment follow the operational risk assessment methodology in use within your reporting entity?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has your current ML/TF risk assessment methodology been approved by the Board?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you allocated responsibilities for constructing, implementing and reviewing the ML/TF risk assessment methodology, and have you recorded these in your governance map?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have those roles that need to be trained in the use of your ML/TF risk assessment methodology been trained in its use?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

24. Designing the risk-based approach: implementary controls

24.1 Categories from Step 5

In Step 5 of the risk assessment methodology, risk indicators were placed in categories that were used Step 6 to quantify the ML/TF risk faced by a reporting entity. These same categories come into use in planning the risk-based approach because they are a logical way of organising risk indicators and matching them with appropriate controls.

The question which arises for each risk indicator is: How will you find it in your organisation interactions with its customers? For example:

- If you have decided that all overseas customers are higher ML/TF risk, how will you find these customers?
- If transactions with certain countries or persons are prohibited because it is not economic to analyse them against domestic or international sanctions, how will you detect them?
If you have decided that occupation or type of business activity is information you will use to identify higher-risk occupations and business activity, how will you get this information?

All risk indicators need to be tracked by a control otherwise the reporting entity will be unaware their presence. If a risk indicator cannot be tracked by a control for current operational reasons, then that gap needs to be recorded and eventually closed. This is a tricky area of ML/TF risk assessments because it is seems just as easy to drop the risk and the risk indicator than have the gap. This is a tactical and weak approach to ML/TF risk assessment.

24.2 Organise Controls into a control library
A control is a process, policy, device, business practice, procedure, tool or other action or device that acts to minimise negative risk or enhance positive opportunities. For each risk indicator, a current control is needed to identify, mitigate and manage that risk indicator. Begin by creating a control library, which is a list of the all the controls in operation within the enterprise. Add to that list all the controls that are desirable, even if they are not currently in use. Place the controls into useful categories. One control will manage many risk indicators for example, the customer acceptance procedure is a control that should be addressing many ML/TF risk indicators associated with information about customers.

24.3 Examples of categories and contents
Some examples of control categories and their contents are:

- KYC controls
- Scanning against sanctions lists
- Scanning customer names against lists of PEPS
- Customer identification procedures
- Conduct of research on beneficial ownership
- Use of an ML/TF country risk matrix
- Use of an industry risk matrix
- Correspondent banking due diligence
- Ongoing customer due diligence
- Regular customer review
- Monitoring procedures
- Workflows following trigger events
- Weighting processes for prioritising alerts generated by transaction monitoring processes
- Special due diligence for trade finance transactions
- Record-keeping (controls are needed to ensure that a reporting entity meets its mandatory obligations under the AML/CTF legislation and regulation, as well as risk-based obligations)
- Regular sampling activities to validate the reliability of records creation and retention
- Standard suspicions transaction reporting to law enforcement
- Using of mystery shopping programmes to test the quality of procedures about tipping-off
- AML/CTF Programme
- Providing role-based training to meet the AML/CTF needs of each role
- Refreshing AML/CTF training on a role-based cycle
- Using an AML/CTF calendar to manage review cycles and date-driven activities
- The categories and controls used vary between reporting entities. However, knowing what controls your peers use is important information in guiding your choice of appropriate controls.
24.4 Assess the appropriateness of Controls
Identified controls need to be reviewed for their appropriateness on a regular basis. If the control is weak or ineffective, or rarely used correctly, then it is not an appropriate control. If a control is so complex that staff do not understand it, then it is not an appropriate control. Controls that rely on data need to be kept current; for example, country ML/TF risk requires current information about the countries it refers to in order to be effective.

24.4.1 Identify the places where no control exists
If there is no control in existence then this needs to be treated as a gap that requires remediation. Do not delete the risk indicator from the ML/TF risk assessment.

24.5 Deciding what is an appropriate control
Reporting entities must determine what an appropriate control is. This decision should take into account the nature, size and complexity of its business, as well as its ML/TF risk. Reporting entities should also consider other factors, such as the cost and efficacy of the control. If a control is low in cost, then reporting entities would have difficulty in defending a failure to have such a control. An important determinant of what is appropriate will be the existing operational risk methodology in use within the reporting entity. This methodology is the framework that should be used to guide qualitative and quantitative analysis of ML/TF risk in order to determine appropriate controls.

Screening for names on sanctions lists is a good example of whether a control is appropriate or not.

24.6 Peer comparisons
Knowing what controls are considered to be appropriate by peers is important information, which can be used to guide decisions by a reporting entity on what is an appropriate control. The best way that a reporting entity can acquire this information is through building effective relationships with peer organisations, concentrating only on AML/CTF. This reduces the risk of regulatory creep, where the regulator sees a control in one organisation and then tries to require all similar reporting entities to apply that control, even if it is not appropriate for them.

24.7 Measuring the effectiveness of controls
Reporting entities should measure the effectiveness of their controls in order to be able to prepare such reports. It is also good practice to monitor the effectiveness of controls by using a variety of means, such as:

- Using checking mechanisms to verify the quality of completion of key steps, such as account opening;
- Sampling completed workflows which are triggered by events, such as filing of suspicious activity reports, to validate that they are completed and completed correctly;
- Sampling key decision-making processes;
- Verifying steps such as records retention.

24.7.1 Using a Compliance or Requirements Plan
Reporting entities should maintain a complete register or plan of the ways they measure the effectiveness of controls. This register or plan forms part of the management process of ML/TF risk because it provides the reporting entity with the ability to organise and control its AML/CTF actions. It also stands as the complete record of the reporting entity's risk-based approach. Reporting entities can be required by regulators to demonstrate their risk-based approach during routine reviews (as well as reviews occasioned by money laundering or terrorism financing events). Without such a register or plan, a reporting entity may struggle to satisfy regulatory expectations. There
will be an overlap between a control library and a requirements plan although they are not the same thing.

25. **Additional review activities**
Reporting entities should include regular review of key aspects of their ML/TF risk assessment and risk-based approaches. These review activities will differ in the length of their review cycle according to the elements under review. Some review activities will be triggered by events such as the filing of suspicious activity reports. These additional review activities are by their nature a risk-based approach, and thus form part of the risk-based approach.

26. **Deliverables from the risk-based approach**
At the end of designing its risk-based approach, a reporting entity should have:

- A control library;
- One or more controls covering the 'identify, mitigate and manage' guidelines allocated to each risk indicator;
- A plan of work to upgrade current controls that are deemed inappropriate (if any);
- A plan of work to implement new controls to close gaps (if any);
- A register or requirements plan listing all the controls and the ways that the reporting entity intends to test their effectiveness;
- A documented review cycle for key elements of the ML/TF risk assessment process and the risk-based approach; and
- Arrangements in place for Internal Audit to perform its regular review.

26. **Documentation**
Reporting entities should have an appropriate documented record of procedures, without which a reporting entity will find it difficult to demonstrate to the regulator that it has a risk-based approach.
**Tasks**

1. Establish five objectives of the business you work in which may be impacted by ML/TF risks including regulatory risks.
2. List the circumstances which would lead to your reporting entity experiencing a significant impact from being involved in a money laundering event.
3. a) Using the structure and content of your ML/TF risk assessment, design a Control Library and a Compliance or Requirements Plan that complements the ML/TF risk assessment.
   
   b) Prepare a briefing note for Internal Audit describing these documents and why they are relevant to the AML/CTF programme of your organisation.
   
   c) Identify the reports that could be provided to the Board about AML/CTF from these documents and what these reports will mean to the Board in terms of their approval and oversight function.
4. Read the FATF Guidance on the Risk-Based Approach 2007 and summarise its main recommendations.
5. Carry out an ML/TF risk assessment on a business with which you are familiar. Indicate the key characteristics of the assessment.
Self assessment questions

1. Define risk in the context of AML/CTF.
2. What is meant by a risk-based approach to AML/CTF?
3. Who is responsible within a reporting entity for implementing a risk-based approach to AML/CTF?
4. What is a risk-based control?
5. In building a risk-based control system, name six areas of the business likely to be impacted by the risk-based approach.
6. Give three examples of risk-based controls.
7. What are risk indicators? Give two examples.
8. What do you understand by the term 'risk appetite'?
9. Outline the six steps of risk assessment methodology.
### Module outcomes

By the end of this module you should:

- understand the principles and purpose behind the risk-based approach, apply guidance, including the FATF Guidance, on the risk-based approach.
- explain the relationship between an ML/TF risk assessment and the key controls of know your customer, monitoring and product functionality.
- understand the main ways to measure effective controls and the importance of mapping controls to risks.