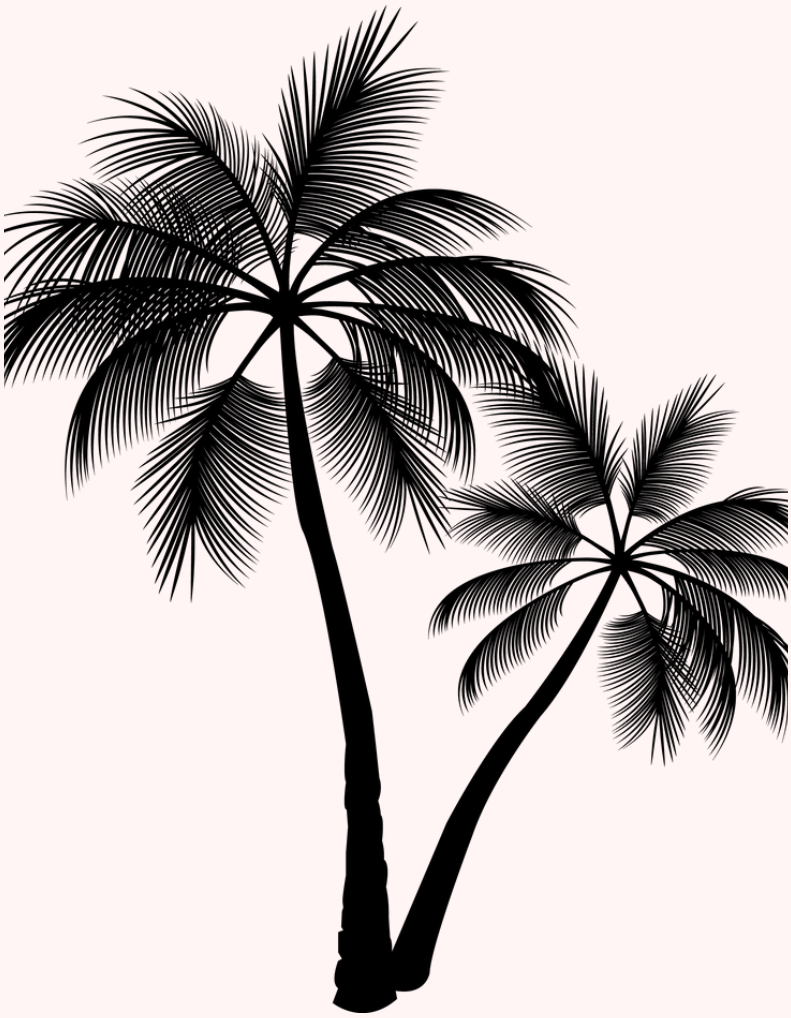
KNOW YOUR EMPLOYEE GUIDANCE

COMPLIANCE COMMISSION



INTRODUCTION

The Compliance Commission is raising awareness of why it is important to know your employees. KYE is a necessary program to determine an employee's background and investigate if they have any history related to money laundering, fraud, deceit or criminal activity.

Weak KYE procedures may lead to penalties, reputation damage, financial losses, and the loss of business opportunities.

Effective KYE procedures are required by the Financial Action Task Force (FATF) that sets the standard for combating money laundering, terrorist and proliferation financing. KYE guidelines are included in the CC Codes of Practice which are enforceable by law.

Understanding you employee can also help to improve productivity and job satisfaction.

WHAT IS KNOW YOUR EMPLOYEE?

KNOW YOUR EMPLOYEE, OFTEN ABBREVIATED AS KYE, IS THE PROCESS BY WHICH BUSINESSES VERIFY THE IDENTITIES AND BACKGROUNDS OF BOTH CURRENT STAFF AND POTENTIAL HIRES. THE OBJECTIVE OF KYE IS TO ENSURE THAT EMPLOYEES ARE WHO THEY SAY THEY ARE AND ARE NOT OVERLY RISKY DUE TO HAVING HISTORIES OF CRIMINAL ACTIVITY.

WHY KYE IS IMPORTANT?

MOST BUSINESSES INVEST IN KNOW YOUR CUSTOMER (KYC), KNOW YOUR BUSINESS (KYB), AND KNOW YOUR TRANSACTION (KYT) PROCESSES TO PROTECT AGAINST THE THREAT OF FINANCIAL CRIME FROM OUTSIDE THE COMPANY. KNOW YOUR EMPLOYEE, OR KYE, IS ABOUT PROTECTING A COMPANY FROM INSIDER THREATS.

FINANCIAL ACTION TASK FORCE (FATF) RECOMMENDATION 18 & 23 REQUIRES:

FINANCIAL INSTITUTIONS AND DNFBPS TO IMPLEMENT PROGRAMS AGAINST ML/TF, WHICH HAVE REGARD TO THE ML/TF RISKS AND THE SIZE OF THE BUSINESS, INCLUDING SCREENING PROCEDURES TO ENSURE HIGH STANDARDS WHEN HIRING EMPLOYEES.

Accordingly, registrants have an obligation to implement an employee due diligence program that protects against money laundering and terrorist financing. These measures should ensure that the risk from internal functions such as their employees are mitigated, and the employee is suitable for the tasks assigned.

Experienced, motivated, honest, and educated employees are critical to the success of your business and the effectiveness of the AML program. Implementing high standards for employee due diligence protects against reputational, legal, and operational risks and helps identify red flags.

Knowing your employee (KYE) covers the relationship with the employee from the recruitment process, ongoing employee relationship and if need be, termination of employment.

The AML regime is risk-based, and more stringent screening procedures are required for employees that function in high-risk roles. When an employee is moving to a new role registrants should determine based on their risk assessments and controls whether the new role requires the employee to update or undertake a rescreening process and the frequency. In particular if their role puts them in a position to facilitate the commission of a ML/TF offence. These procedures must be documented and include disciplinary actions if it is detected that that information provided by an employee is false.

TO SCREEN PROSPECTIVE EMPLOYEES, YOU SHOULD ASK THEM TO PROVIDE THE FOLLOWING INFORMATION TO ASSIST WITH DETERMINING THEIR SUITABILITY.

- Employment history
- Reference checks – character and from previous employers
- Identify and verify identity.
- Police certificate
- Background check by the RBPF or private investigator, as required based on risk assessment.
- For positions that require technical qualifications and/or practicing certificates, such as a lawyer or an accountant, you may confirm the person is a member of the relevant professional association. Assess the skills and knowledge to determine suitability.
- Academic qualifications (checking the authenticity of academic qualifications depending on risk of role and knowledge of the prospective employee)
- Credit check
- Some companies also use a questionnaire requiring the prospective employee to sign a declaration that the information they have provided is true and correct and they consent to background checks. In addition, issue a code of conduct or ethics that outlines the company's employment conditions including conflict of interest, confidentiality policies and sanctions that employees must sign and attest to understanding each year.

HIGHER RISK ROLES - THAT POSE A HIGHER ML/TF, (FOR EXAMPLE, AN EMPLOYEE THAT HAS AUTHORITY TO AUTHORIZE THE INVESTMENT AND RELEASE OF FUNDS, COMMUNICATES DIRECTLY WITH POTENTIAL OR EXISTING CUSTOMERS, POWER TO CHANGE PROCESSES AND ACCESS TO HIGHLY SENSITIVE BUSINESS OR CUSTOMER INFORMATION – REQUIRE ADDITIONAL EDD MEASURES.

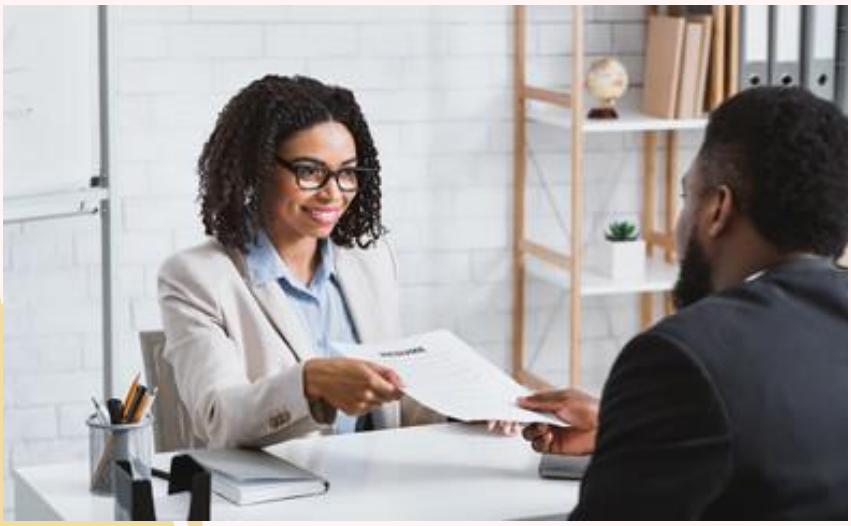
- A sanctions and PEP check (world check, SafetyNet, KYC screening tools
- Adverse media checks
- Additional checks to verify qualifications & experience, education, and professional qualifications.
- Has the employee lived in high-risk countries or abroad for an extended period that may cause further checks.
- Subject to any court or legal action.

EMPLOYEE ACCESS

Employees may have access to sensitive information about the affairs of their employers as well as their policies that must be kept confidential.

Consequently, companies should put in place controls along the lifecycle of employment to ensure confidentiality.

Trust between an employer and its personnel is based on initial screening during recruitment (often followed by initial trialing via probation) and years of the employee relationship.



EMPLOYEE LIFE CYCLE STAGES

ONGOING EMPLOYEE RELATIONSHIP

- Exposure to organization policies and procedures through a combination of training and awareness to encourage and enforce compliance.

THE RECRUITMENT PROCESS

- Interview

- Background verification

- Communicating confidentiality obligations and the importance of new employees having a clear understanding of their information security obligations and sanctions.

TERMINATION OF EMPLOYEE

- Financial institutions should have human resources policies and processes related to termination of engagement that protect sensitive information and ensure confidentiality of information is maintained beyond employment

THE RECRUITMENT PROCESS

- INTERVIEW

Must underscore the importance of information security, confidentiality, and importance of not taking actions to cause reputational or legal or operation risks to the firm. Assessing the integrity of the person. Guard against hiring dishonest staff.

- BACKGROUND VERIFICATION

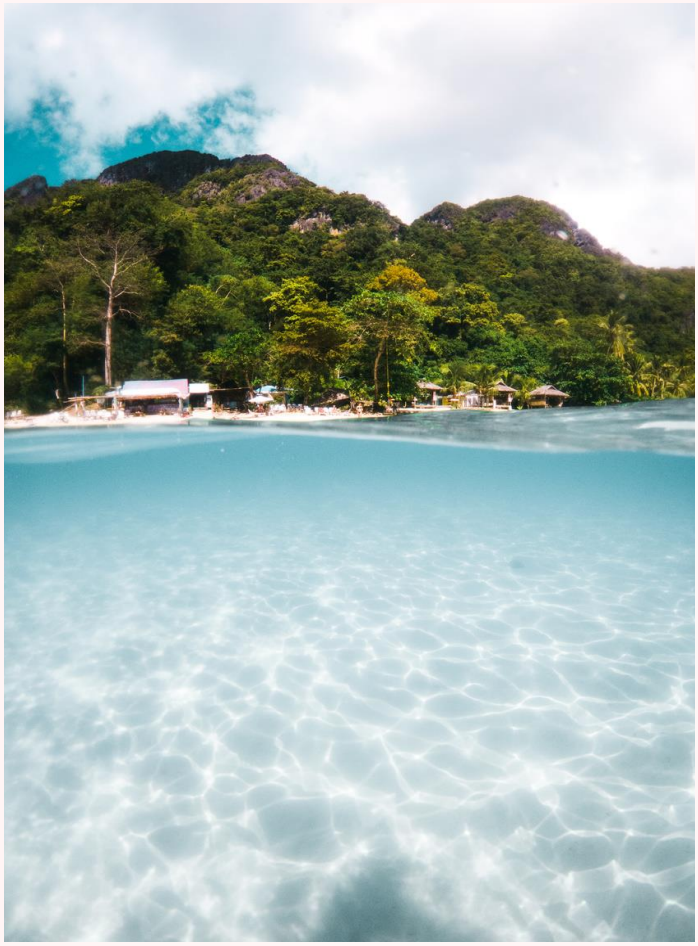
Proportional to the confidentiality and access to sensitive data and perceived risks of the role - this may involve security vetting by the police dept, which is a more intense suitability check to get a good understanding of an individual's background and character - common with regulators or government jobs. Vetting should be time-bound and refreshing when there is a significant change in the personnel's role, or they move to a more sensitive position.

Some organizations use private firms to conduct suitability & character checks to weed out toxic personalities and persons associated with criminals.

In small countries like The Bahamas the saying is "we know who the criminals are".

•COMMUNICATING CONFIDENTIALITY OBLIGATIONS AND THE IMPORTANCE OF NEW EMPLOYEES HAVING A CLEAR UNDERSTANDING OF THEIR INFORMATION SECURITY OBLIGATIONS

This may include signing and acknowledging understanding of the company codes of conduct including confidential provisions that include penalties/sanctions for disclosure of company information and ethics training.



ONGOING EMPLOYEE RELATIONSHIP

During employment, the personnel should receive regular exposure to the organization policies and procedures in practice, through a combination of training and awareness to encourage and enforce compliance.

TERMINATION OF EMPLOYMENT

DNFBP's should have human resources policies and processes relating to the termination of engagement that protect sensitive information and ensure that the confidentiality of the information is maintained beyond employment.

The most effective KYE programme should be complemented by a sound on-going training programme which includes staff awareness. Employees should be aware of penalties and sanctions that apply in case of confidentiality breaches or bad behavior.

The CC expect registrants & or licenses to meet the FATF standards and maintain screening procedures to ensure high standards when hiring employees.

Source: CC KYE Presentation, Austrac, OECD Confidentiality in Information Security