



Veriphy AML Compliance Checklist

VERIPHY 
A Davies Company

AML compliance is vital for your business because it ensures you meet legal obligations

Protect your reputation and prevent financial crime. By systematically verifying identities, screening for risks, and maintaining robust policies, you reduce exposure to regulatory penalties and build trust with clients and partners. It's a proactive way to safeguard your operations and demonstrate your commitment to ethical business practices.



Stay compliant with AML regulations and Veriphy's best practices by following this six-point checklist:



Identity Verification

Use electronic methods to verify customer identity

Digital tools such as AML ID verification, sanctions and PEP screening, [biometric checks](#) with facial recognition and document validation streamline onboarding and review processes while reducing the risk of fraud.

Ensure compliance with the AML Regulations and JMLSG guidance

Recent guidance mandates enhanced due diligence, especially for high-risk customers, and requires firms to adopt electronic identification and risk-based approaches to prevent money laundering and terrorist financing.



PEP (Politically Exposed Persons) Screening

Screen all clients for PEP status

Identifying [Politically Exposed Persons \(PEPs\)](#) helps assess the risk of potential involvement in corruption or financial crime due to their public roles.

Apply Enhanced Due Diligence (EDD) for PEPs and high-risk individuals

EDD involves deeper scrutiny, such as verifying the source of funds and ongoing monitoring, to mitigate the higher risks associated with these clients.

Document and justify risk-based decisions

Keeping clear records of why certain clients are classified as high or low risk supports transparency and helps demonstrate compliance during audits or regulatory reviews.



Sanctions and Watchlist Screening

Screen all clients for sanctions status

Sanctioned individuals or entities pose a significant risk, as dealing with them may result in serious penalties.

Monitor for changes in status

Monitoring for changes in sanctions status means you are protected 24/7 against unexpected alterations. Volatile global conditions mean that the sanctions regime is constantly changing.



Staff Training

Provide mandatory AML training for all employees

Regular training ensures all staff understand anti-money laundering (AML) laws, internal policies, and their responsibilities in preventing financial crime.

Ensure staff can identify and report suspicious activity

Employees should be equipped to recognise red flags such as unusual transactions or customer behaviour and know how to escalate concerns appropriately.

Keep records of training completion

Maintaining up-to-date training logs helps demonstrate compliance during audits and ensures all employees remain informed and certified.



Written AML Policy

Risk assessments

Identify and evaluate potential money laundering risks associated with customers, products, and services to apply appropriate controls.

Monitoring controls

Implement systems to detect suspicious transactions or patterns of behaviour that may indicate financial crime.

Reporting protocols

Establish clear procedures for escalating and reporting suspicious activity to the appropriate authorities, such as the NCA.

Roles and responsibilities (e.g. MLRO, Nominated Officer)

Define who is responsible for AML compliance, including appointing a Nominated Officer to oversee reporting and ensure adherence to regulations.

Update regularly to reflect regulatory changes

Review and revise the AML policy frequently to stay aligned with evolving laws, guidance, and industry best practices.





Ongoing Monitoring and Review

Continuously monitor client relationships

Ongoing monitoring helps detect changes in customer behaviour or transactions that may indicate increased risk or suspicious activity.

Reassess risk levels and update due diligence as needed

Clients' risk profiles should be reviewed periodically or when new information arises, ensuring **due diligence measures** remain appropriate.

Perform regular audits of AML procedures

Internal audits help identify gaps in compliance, assess the effectiveness of controls, and ensure **AML policies** are being properly followed.



Optional Enhancements with Veriphy

Biometric AML checks (facial recognition, liveness detection)

These technologies verify a person's identity by comparing facial features and detecting real-time presence, helping prevent impersonation and identity fraud.

Batch screening for client lists

This process allows organisations to screen large volumes of customer data at once against sanctions, PEP (Politically Exposed Persons), and watchlists to ensure compliance.

Adverse media and credit screening

Monitoring negative news and credit history helps identify potential risks associated with clients, such as involvement in financial crime or insolvency.

Online AML training modules

E-learning platforms provide flexible, trackable **AML training** that ensures employees stay up to date with regulatory requirements and best practices.

Here to help

Want to find out more about AML compliance?

By following this checklist, you can ensure your business meets regulatory requirements, mitigates risk, and maintains a strong reputation for integrity and compliance.



Get in touch for a free consultation with our experts



Richard Devine

Solutions Consultant

✉ richard.devine@davies-group.com
in Richard Devine



Adam Watts

Client Growth Manager

✉ adam.watts@davies-group.com
in Adam Watts