BAE SYSTEMS

How effective is your AML auditing?

Executive summary

Has your financial institution recently been through a regulatory audit or thematic review where weaknesses were identified with your audit processes? This is now an increasingly common scenario for Chief Anti-Money Laundering Officers (CAMLO), Bank Secrecy Act Officers (BSA Officers), or other similar positions in financial institutions; and where processes are found to be weak, regulatory commentary and ongoing remedial actions can be sure to follow. As the Anti-Money Laundering (AML) and Counter Terrorist Finance (CTF) regulatory environment experiences ever stricter scrutiny, your AML and CTF audit model and governance procedures will become subject to greater audit and regulatory interest.

On August 11, 2014, the Financial Crimes Enforcement Network (FinCEN) published an advisory (FIN-2014-A007) which re-iterated the prior warnings from the director that FinCEN "...will employ all of the tools at our disposal and hold accountable those institutions and individuals who recklessly allow our financial institutions to be vulnerable to terrorist financing, money laundering, proliferation finance, and other illicit financial activity. Indeed, financial institutions should heed this advisory as a warning shot that FinCEN and other federal regulators will be taking more aggressive and frequent enforcement actions against institutions and their leadership in those situations where weak compliance programs lead to illicit activity."

It is therefore more critical than ever that your financial institution has a strong, comprehensive AML audit process to measure and govern your AML program's compliance with applicable AML and BSA laws and regulations. In this paper we will explore how the framework of a comprehensive AML audit model can support you in preparing for your next AML program audit.

It is more critical than ever that your financial institution has a strong, comprehensive Anti-Money Laundering (AML) audit process

The AML program

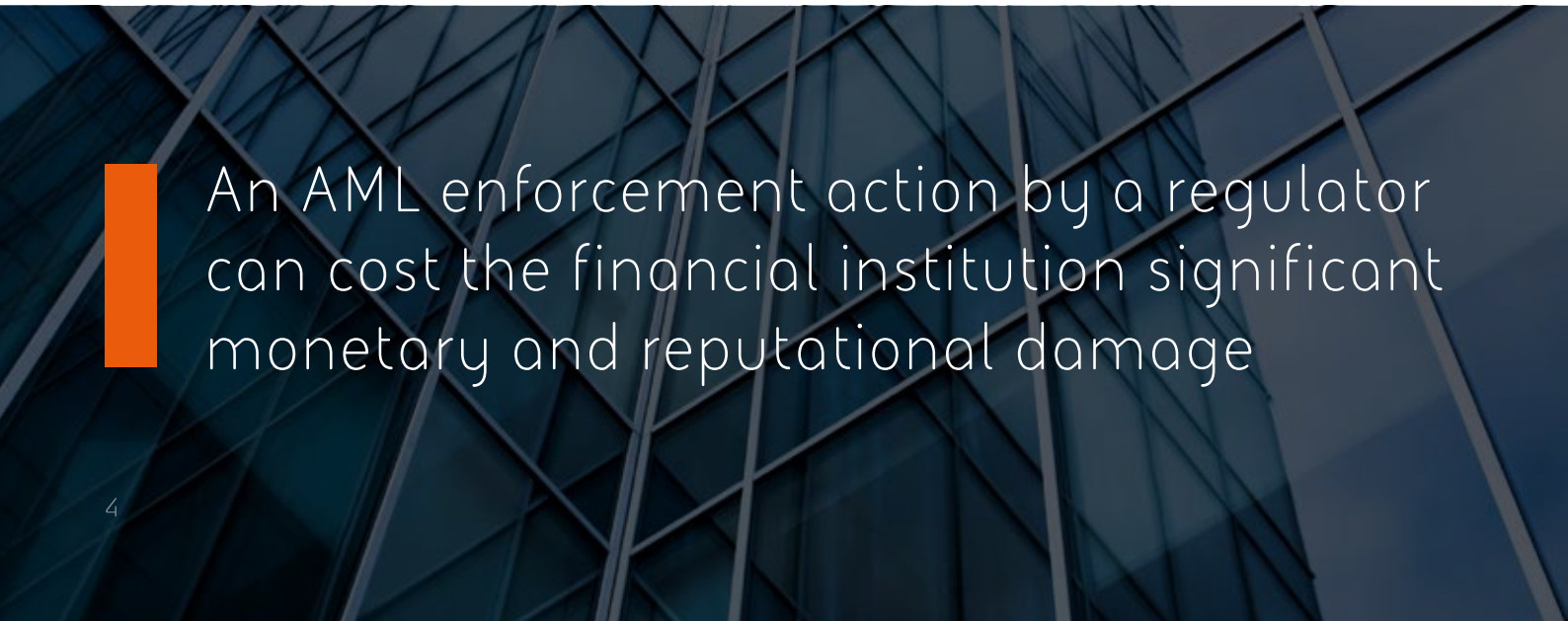
The Financial Action Task Force (FATF) Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) methodology recommendations state: "...financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with procedures". The AML/BSA Examination Manual states, "Review of the bank's written policies, procedures, and processes is a first step in determining the overall adequacy of the BSA/AML compliance program."

Having a compliant AML program therefore requires daily operations and procedures to be undertaken in accordance with BSA guidelines. Failing to do so can have undesirable consequences for an institution, including regulatory violations, penalties, monetary fines, and regulator involvement. To avoid such outcomes, regulators require financial institutions to implement a comprehensive AML audit model with the purpose of properly identifying any weaknesses or deficiencies within AML onboarding and operations, and for those measures to stand up to audit, examination or regulatory scrutiny.

Everyone has to audit – what is different for AML?

Auditing is a standard operation performed by all financial institutions in some capacity. It can be performed by internal staff as well as independent third parties, and is typically approached from a financial perspective. AML program compliance, however, requires daily tasks to be completed accurately, timely, and effectively. This makes compliance audits very different from their financial brethren, whose focus is primarily number reconciliations and number crunching. AML audits must identify deficiencies, gaps, and weaknesses that may exist in the content, controls, and operations of the AML program. in this context, content is defined as having a written policy, procedures, training, monitoring, and reporting.

A consequence of ineffective auditing may lead to potential AML violations, such as failing to report suspicious activity or collecting proper customer identification documents. An AML enforcement action by a regulator can cost the financial institution a great deal in terms of monetary and reputational impact.

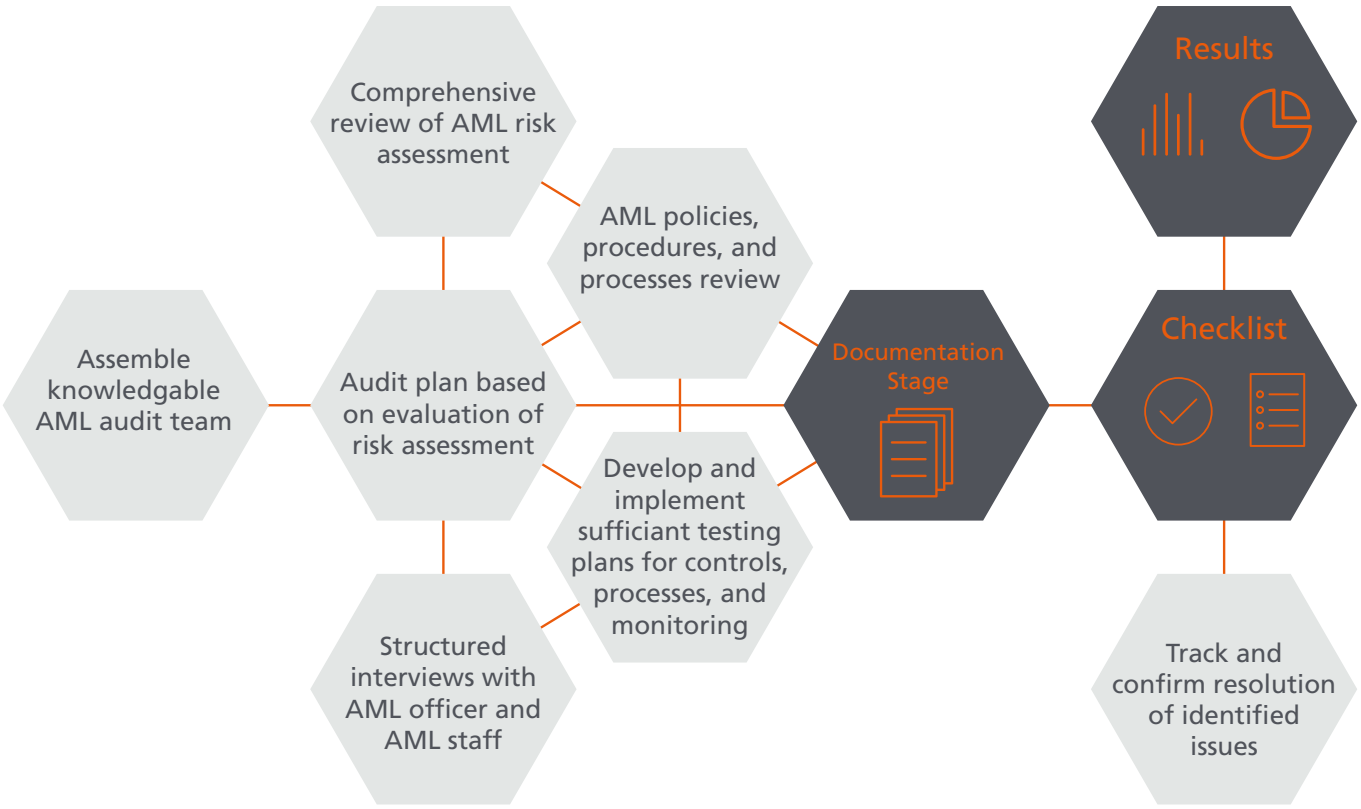


An AML enforcement action by a regulator can cost the financial institution significant monetary and reputational damage

What defines an **effective AML** audit model?

Financial institutions that have consistently demonstrated AML Program compliance with favourable examination reports share similar characteristics in their approach to AML audit governance. The Association of Certified Anti-Money Laundering Specialists (ACAMS) observes in its How Audit Departments Can Develop An Effective AML Program: "Several key components need to be considered when creating a strong AML Audit Program. There is no one right answer as every firm has its own unique obstacles; however, all firms need to consider their governance, execution, and reporting components."

Below is an outline of those, and other commonly identified traits, that have been consistently identified in effective AML audit programs.



For AML audit models that are missing one or more of these components, issues, concerns or violations may not be readily identified. This might include inadequate procedures or monitoring, repeatedly-missed red flags or a failure to report suspicious activity in a timely manner. Strong test plans, therefore, are vital to the creation of a consistent, repeatable AML process.

Preparing for your AML audit

Many financial institutions struggle to build effective audit procedures for AML. Unlike other audits, those that test AML capabilities require analytics and evaluations from a different perspective, and with different methodologies. The alternative perspectives, skills and processes involved place very different pressures and requirements upon AML auditors; their assessment is based on the financial institution's AML program documentation, tasks, processes, monitoring and reporting.

For an AML auditor to effectively perform these assessments, it will require the department being examined to show evidence, methodologies and process documents that support to their daily operations. But what is initially provided may not be adequate or comprehensive enough to facilitate an effective audit for a number of reasons - not all of which have any bearing on the capabilities of the team or function itself. This could be a result of the AML department not having a full understanding of what is being requested, inexperienced auditors who are not adequately trained on AML rules and regulations, or simply that the AML audit plan is not adequately scoped by the AML auditor.

Therefore, the information provided by the AML department prior to commencement of the audit, coupled with a clear understanding of roles and responsibilities, is essential to achieving a productive and successful audit.

1. AML auditor roles and responsibilities consist of:

    a) Providing a list of specific documentation that will be needed to start the audit to the AML department being audited;

    b) Outlining the audit plan and approach; and

    c) Drafting and presenting the audit results and findings

2. AML department roles and responsibilities.

The AML department will gather the requested documentation, and will obtain clarification from the AML auditor where requests are unclear or require further definition. The initial documentation can provide the auditor with the AML program's framework and structure, which can assist the auditor in identifying potential areas that may require additional focus, documentation, and review.

Unlike other audits, AML audits require analytics and evaluations from a different perspective with different audit methodologies

Overcoming your AML audit challenges

The path to overcoming your AML audit challenges and achieving an effective AML audit model may require your auditor to reassess their audit approach. At a minimum the following steps should be considered:

1

Obtain prior to audit kick-off - Initial Documentation

- Comprehensive enterprise AML risk assessment
- Methods of risk assessment (determining high risk customers, PEPs, MSBs, etc.)
- Written policies and procedures
- Training materials
- AML Solution generated audit reports.

2

Planning - AML audit approach

- Clearly defined AML audit strategies
- Properly scoped and documented audit plan specific to AML
- Comprehensive risk-based testing plans.

3

End of day - Results and Findings

- Detailed report of findings to board and senior management
- Follow-up plans to confirm any issues or concerns have been properly addressed and/or resolved

Overcoming these challenges requires an AML auditor to reassess their audit approach

Ensuring future **effectiveness**

In general, the effectiveness of any audit program is measured by its ability to fulfill its objectives through its own established processes and procedures. AML audits can only be as effective as the results they produce, and those results are based on the audit operations themselves. In ensuring that AML audits are effective, it takes more than just gathering the materials themselves. It requires that your AML department has implemented a strong program and solution tools, as well as requiring additional steps to be taken by the auditor that often get overlooked. As a result, pertinent information regarding procedures, solutions, and personnel ability may not get sufficient attention or missed all together.

Effective AML auditors ensure they have undertaken the following activities:

- Clearly define the audit goals and objectives. AML audits can be conducted as part of routine procedures, or conducted for a specific purpose in mind.

- Assign an auditor knowledgeable in AML laws, regulations, and expectations. Auditors who are not knowledgeable or lack AML experience can potentially miss gaps or weakness in an AML program. AML audits need to incorporate, at a minimum, transaction monitoring and how it applies to AML and suspicious activity monitoring.

- Prepare a request list of all documents and potential supporting documentation needed to perform a comprehensive audit. This list must be presented to the AML department in advance, and its staff must have sufficient time to collate the requested items. Often, auditors misjudge how much time it will take for the AML team to obtain this information, and as a result, the AML department rushes and inadequately gathers the items. Don't skimp on documentation. Be sure your work papers and other supporting documents back up your audit plan including mapping the AML/BSA risk profile to the audit program and maintaining sufficient evidence of testing and results. Additional support is warranted for higher-risk observations.

- Prepare a list of interview questions in advance for personnel, including specific questions for the AML Officer. AML auditors have to have an overall understanding of the AML department's program, procedures, operations, and daily activities. This information may not be easily accessible within the written program.

- Obtain audit reports from the AML department's solution program in advance. Effective auditing also relies on the AML department's ability to adequately and efficiently produce its own audit reports. The AML department must have a solution in place capable of producing various AML audit reports that provide adequate and comprehensive supporting documentation for its AML efforts.

- Ensure detailed reviews are conducted of the AML audit reports produced by their implemented solution. Because of the detailed information they provide, effective AML audit reports can help ensure that effective AML audits are being performed. The reports generated by the AML solution should be quantified, have appropriate terminology, unfamiliar terms defined, report and/or link findings to customers, transactions, or entities, and have images or diagrams for result presentation.

- Make sure your sample sizes are sufficient and representative. Higher risk issues like Money Services Businesses or privately owned ATMs (Automated Teller Machines) should be more closely examined than lower risk activities. Are you looking at enough accounts? The right accounts? Are you focused on the correct time periods for testing?

Transparency is key

A successful; audit - and a successful AML operation - comes down to transparency. The easier it is for regulators to understand how you have defined, documented, controlled and audited your risks, the more comfortable they will be with your AML audit effort and results. It is vital to assess your AML audit program through a regulator's eyes, and ensure that your audit plan and documentation of work performed will withstand the scrutiny it will surely receive.

In Germany, for example, BaFin, the financial regulatory authority, has for many years required organisations to provide annual risk assessments audit reviews as part of its risk analysis or "Gefährdungsanalyse". Maintaining a transparent view of risk and managing this over time with a clear audit is key.

In summary, effective AML audit programs should provide insight and support the financial institution's goals and business strategies, and not be defined by the number of findings or exceptions it identifies. Tie your audit plan to your risk profile. Just as your internal controls should reflect your unique geographic, product and customer risks, so too must your AML audit plan. Long-term effectiveness is defined by the AML audit's ability to do so. The value added to a financial organisation as a result of an effective AML audit can be priceless.

Stay compliant with BAE Systems

BAE Systems work with global banks, insurers and governments to provide intelligence and solutions to combat fraud and financial crime. We aim to protect your organisation, your customers and your reputation. Our range of solutions can help identify, combat and prevent financial threats, as well as reducing risk, loss or penalties and ensuring your institution is fully compliant with regulatory obligations.

To find out more about BAE Systems and how our AML solutions can help you, visit us at http://www.baesystems.com/aml

BAE Systems works with global banks, insurers and governments to combat fraud and financial crime

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

BAE Systems
Level 26, North Tower
459 Collins Street
Melbourne, Victoria
Australia
Tel: +03 8623 4300
General Enquires +61 1300 027 001
Sales Enquires +61 3 8623 4400

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
Tel: +61 (2) 9240 4600
General Enquires +61 1300 027 001
Sales Enquires +61 3 8623 4400

BAE Systems
1 Raffles Place #23-03, Tower 1
Singapore 048616
Singapore
General Enquires: +65 6499 5000
Sales Enquiries: +65 6714 2100

BAE Systems
Level 29 Menara Binjai,
2 Jalan Binjai,
Kuala Lumpur, 50450
Malaysia
General enquires +603 2191 3000
Sales Enquires +60 3 2191 3400

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST CESG Certified Service Cyber Incident Response CPNI Centre for the Protection of National Infrastructure