Narrowing the quality criteria for anti-money laundering commercial-off-the-shelf (COTS) software products under the Bank Secrecy Act

CAMS-Audit Advanced Certification White Paper

Emil Ivanov

Contents

Table of Figures

Table of Tables

Executive summary

The Anti-Money Laundering (AML) regulatory acts such as Bank Secrecy Act[1], Foreign Assets Control Regulations[2], Financial Record Keeping and Reporting of Currency and Foreign Transactions regulations[3], and the USA PATRIOT Act[4] provide guidance to organizations for developing and maintaining systems of internal controls that are flexible to changes in the business and operating environments. Due to the constant proliferation of criminal and terrorist activities throughout the world, financial institutions should adapt their AML-related business processes and tools to address these risks.

Emerging technologies, together with the expansion of the Internet's cyber banking commerce, transforms the money laundering processes to make it significantly easier for launderers to hide its origins, insert dirty money into the financial sector stream, wash it through authentic businesses, and then integrate it back into the economy. As a response, organizations should expand the features for traditional AML tools and add capabilities, such as tracking IP addresses with timestamps, cyber-event data, and virtual-wallet information - to follow criminals, identify victims, and trace illicit funds.

The software tools used through various stages of the AML are aimed to attain effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations. Because of the swift growth in the software technologies and the necessity for businesses to adapt to money laundering typologies, the use of independent audits are the way AML software integrate into internal control environment and is of high interest to the financial institution, information systems community, auditors, and regulators.

Introduction

Any software, moreover complex systems such as AML, is never built overnight. Software building takes planning, interaction with financial institutions, and testing to arrive at even an initial version of the application. Developers' quality assurance (QA) software, if implemented, should follow comprehensive standards to ensure that the application satisfies the requirements. Once the software products are delivered to the market, the internal QA function completes its purpose, leaving it up to the customers to assess and evaluate the attributes of the software. When the business purchases Commercial off-the-shelf (COTS) products, they acquire a "black box" of functionalities: functionalities which satisfy certain requirements in theory. Consequently, the burden of discovering defects not identified or fully addressed during the development process and assessing the fitness of the software for real-world cases falls on the buyer. This "transfer" of responsibilities in such a high risk and compliance-driven environment, like the AML environment, represents a high, inherited risk for the financial institution.

Therefore, a common quality model and evaluative criteria for COTS will serve as an interrelated term and joined criteria among the 'lines of defense', empowering each AML each

[1] Bank Secrecy Act - 31 USC 5311 - 5330
[2] Foreign Assets Control Regulations (OFAC) 12 CFR 500
[3] Financial Record Keeping and Reporting of Currency and Foreign Transactions - 31 CFR 1010.310
[4] United States. (2001). The USA PATRIOT Act: Preserving life and liberty: uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism. Washington, D.C.: U.S. Dept. of Justice

function – Internal Audit, Risk Management & Compliance and Controls Testing & Monitoring Solutions - into a strategic asset to drive business performance.

As an examining and supervising financial institutions body, The Federal Deposit Insurance Corporation (FDIC) issued direction (FIL-121-2004) for the bankers "on performing proper due diligence when selecting a software package or service provider, including ensuring that the software package is compliant with applicable laws"[5]. In addition, the FDIC directs the banks to exercise "due diligence" and develop programs to assess the quality and the effectiveness of the COTS software. However, "quality" and "effectiveness" are very general terms for measurement and must be narrowed and defined specifically in the context of their use in the AML market.

I used scholar search engines – Google search, Science Direct, Ebsco, Emerald Fulltext and Management Reviews, IEEE Computer Society Digital Library -- to research industry standards for software quality models. These scientific sources are utilized to also explore and examine AML software vendors and the availability of data related to their criteria for software quality criteria and compliance metrics.

Before exploring and contextualizing prevailing industry quality models with respect to AML software, a basis for software measures are introduced. According to (IEEE 24765:2017(E)) commercial-off-the-shelf (COTS) is "software defined by a market-driven need, commercially available, and whose fitness for use has been demonstrated by a broad spectrum of commercial users" (p.59). A quality model is a "set of characteristics and of relationships between them, which provides a framework for specifying quality requirements and evaluating quality". Furthermore, a quality requirement is "a requirement that software attribute be present in software to satisfy a contract, standard, specification, or other formally imposed document" (p.289)[6].

In this paper, the criteria for evaluating COTS software through more acceptable criteria in the applicable domain of AML are narrowed. The approach is comprised of the following steps:

1. Perform research and choose a software quality model as the basis.
2. Identify common characteristics of the applications in the domain of AML. Those quality attributes are identified for the COTS applications by researching the AML market and vendors offerings. In addition to that I performed research on the compliance requirements for software. Then, by comparing these quality characteristics with quality factors of our model I discuss and propose applicable level quality criteria related.
3. Suggesting specific activities for auditing and evaluation criteria to ensure that there is an adequate number of systems designed to ensure that business quality objectives are met. Elaborating and discuss the testing of the controls during the overall AML audit activities
4. Assigning ranking to the quality factors and criteria.

[5] USA, Federal Deposit Insurance Corporation. (FIL-121-2004). Computer Software Due Diligence Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance. Retrieved January 13, 2018, from https://www.fdic.gov/news/news/financial/2004/fil12104.html#body

[6] ISO/IEC/IEEE 24765:2017(E) - ISO/IEC/IEEE International Standard - Systems and software engineering-Vocabulary

Software quality models

The subject of software metrics for quality and effectiveness has been under research and subject to many industry standards from the early days of software engineering. The questions about the ways to measure an abstract object such as, "software", and more precisely help to develop software better and faster to help acquirers fully utilize its business value are very important for quality evaluation. Furthermore, the research is centered on the quality and effectiveness of the COTS as a final, ready-to-be-used product rather than on the software development lifecycle.

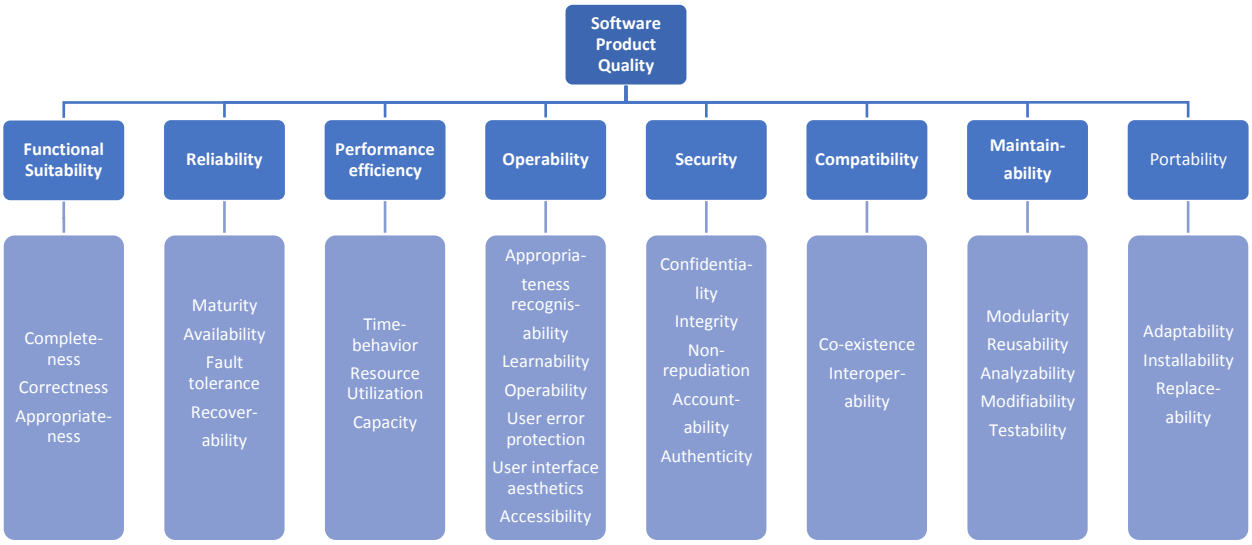

Figure 1 - Software product quality model as depicted in ISO/IEC 25010

Thapar SS & Singh P & Rani S. (2012)[7] provide a comprehensive overview of the evolution of the software quality models. They compare about 24 software quality models in existence during 1970 and 2011. Most software quality models (QMs) can be assigned to one of two strategies for modeling the quality; specifically, a basic model and tailored one. The former usually stipulates a strict set of quality characteristics or metrics, whereas the latter uses methods to guide the experts in the development of customized metrics.

The International Organization for Standardization (ISO) released a reworked software product quality model standard in 2011: ISO/IEC 25010[8]. That model is heavily influenced by its predecessor, ISO 9126[9], and adds several parts of the older quality models developed by the Organization. The ISO/IEC 25010 has eight product quality characteristics depicted in **Error! Reference source not found.**.

[7] Thapar SS & Singh P & Rani S. (2012). "Challenges to the Development of Standard Software Quality Model," International Journal of Computer Applications (0975 – 8887) Volume 49– No.10, pp 1-7.
[8] ISO/IEC 25010:2011 - Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models
[9] ISO/IEC 9126:1991 Software Engineering -- Product quality

Those are further divided into 31 sub-characteristics. These sub-characteristics are evidenced externally when the software is used as part of a complex computer software system, and are the result of internal software attributes.

There are essentially two approaches that can be followed to ensure software product quality: an approach which focuses on characteristics intrinsic to the product, and one which evaluates the quality of the end product. Internal quality characteristics can be features such as system properties, while external ones are usually denoted to the system properties that can be evaluated by the user or independent parties (internal/external auditors, subject matter experts) during its execution. These properties are distinguished, recognized, and analyzed by users when the system is in operation and undergoing maintenance, e.g. it is measured in terms of the results of using the system rather than the properties of the system itself.

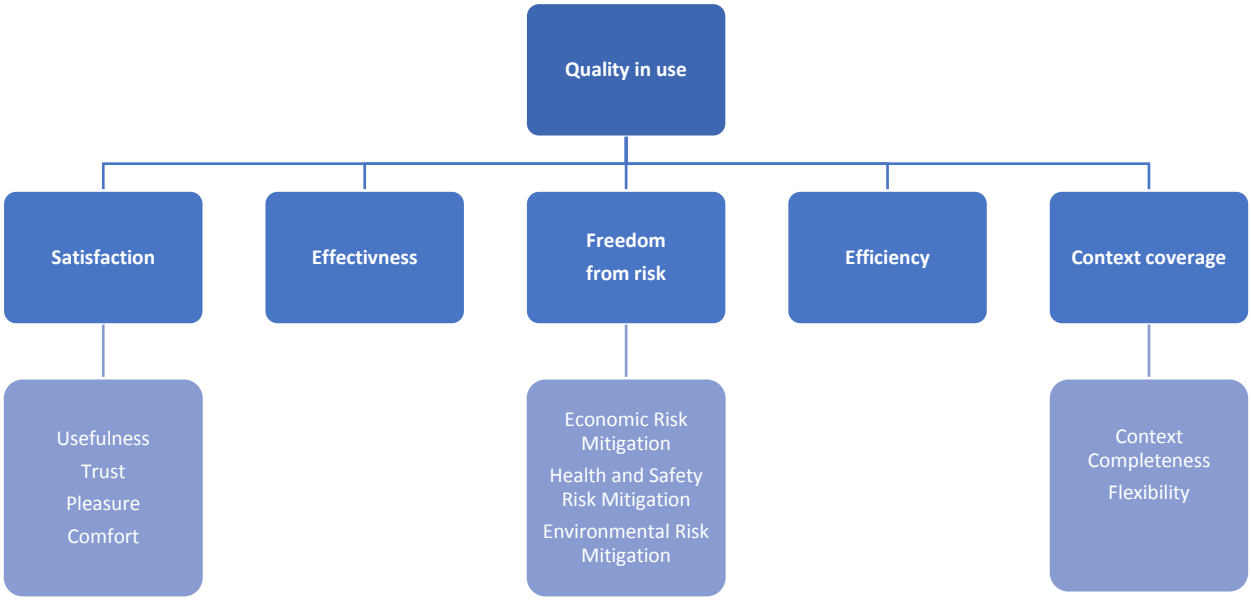

Figure 2 - Software quality in use as depicted in ISO/IEC 25010

Software metrics are defined as standards of measurement, used directly to weight the software attributes, such as security, in an objective manner, or indirectly - e.g. exclusively relaying on expert judgement. However, not all metrics could be measured due to their subjectivity. For example, "usability", from a software quality perspective, is referred to as a set of multiple concepts, such as execution time, performance, user satisfaction and ease of learning.

Software specifically in complex environments like AML never runs alone. For example, know your customer (KYC) module should be logically linked and interfaced with the activities detection and rules engine. Therefore, as part of a larger system, an AML COTS product would typically include multiple interrelated software module products (most of the time from different vendors) which have interfaces, hardware, human operators, and workflows that are closely

interrelated. Consequently, the whole software product can be evaluated by the levels of the chosen external measures. These measures describe its interaction with its environment, and are assessed by observing the software in operation. Quality in use can be measured by the extent to which a product used by specified users meets their needs to achieve specified goals, some of which are shown in **Error! Reference source not found.**.

Product and process characteristics for AML software

According to Research and, M. (0001, February)[10] the leading players in the global community for AML COTS software systems are ACI Worldwide, AML Partners, Accuity, BAE Systems, Company Overview, Experian, PLC, FICO, Fiserv Inc., Global, Radar, Inetco, Systems Limited, Infrasoft Technologies Ltd., LexisNexis, NICE Actimize, and Targens. The study also offers a comprehensive analysis of the market and is presented by deployment models (on-premises and cloud-based) and geography (the Americas, Asia-Pacific, and Europe, the Middle East and Africa).

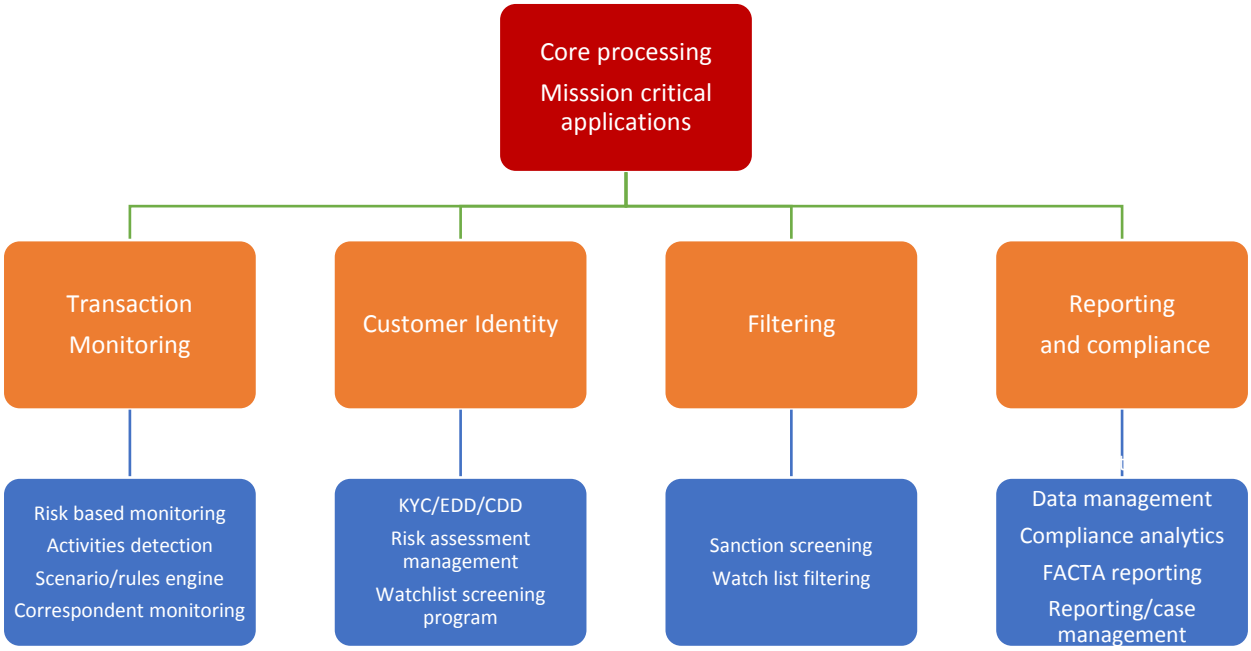

Figure 3 - High level AML COTS classification and attributes

I performed analysis of the essential features of the COTS offered by these vendors to derive key product components and process characteristics of the software in an attempt to relate those to the product qualities model for AML.

Our research indicated that that there is no single comprehensive classification of the characteristics and their attributes. Furthermore, the AML software systems possess

[10] Research and, M. (0001, February). Global Anti-Money Laundering Software Market 2017-2023: Market is Expected to Reach $1420.8 Million - Research and Markets. Business Wire (English)

characteristics that differ from the generic software systems. A significant challenge to that consistent classification structure presents the fact that the laws, regulations, and wrongdoers change constantly. The challenges to the AML software are amplified by the ever-increasing amounts of data fed from transactional combined and business perspective stand point. Nevertheless, our study indicated that major characteristics of AML COTS could be outlined in four major groups depicted in Figure 3. In addition,, these groups have supplementary attributes around providing software for analyzing of the transactions, identifying transactions or patterns of transactions, Suspicious activity report (SAR) filing, or other suspicious patterns that qualify for SAR. According to the Frequently Asked Questions section in [5], the AML software should be classified also against their risk from functional support on the overall bank operations; therefore that point of view is included in the overall considerations for classification.

COTS quality characteristics related to AML

A simple search only in one scientific database Ebsco reveals extensive literature available regarding the software quality models. That examination returned more than 250 scientific publications about reviews of software quality models for the evaluation of software products. A plethora of these works are focused on domain-specific quality characteristics - Business-to-Business (B2B) applications from Behkamal B, Kahani M, and Akbari MK (2009)[11]; Andreou AS and Tziakouris M (2007)[12] do so for component-based software development, and Calero et al. (2007)[13] for eBanking applications. Those publications reveal that although the models are adapted to provision stakeholders in dealing with software quality, in most cases, the models do not fit precisely for the target application context. Moreover, approaches for efficiently adjusting quality models are essentially missing; many quality models in practice are built from square one or reuse only high-level concepts of existing models.

Interestingly enough, the search could not find scientific publications specific to this topic. Nevertheless, win this research I will use the guidance of [8] cross-referenced against the high-level characteristics classification of COTS depicted in Figure 3. In addition, I use the guidance of Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering InfoBase - Bank Secrecy Act Anti-Money Laundering Examination Manual. (2014, April 1)[14], the Development and Acquisition Booklet – FFIEC Information Technology Examination Handbook (IT Handbook). (2004, April)[15] and [5] to suggest ideas specific to AML COTS quality characteristics.

[11] Behkamal B, Kahani M, and Akbari MK (2009): Customizing ISO 9126 quality model for evaluation of B2B applications. In: Inf. Softw. Technol., 51(3), 599-609
[12] Andreou AS and Tziakouris M (2007): A quality framework for developing and evaluating original software components. In: Inf. Softw. Technol., 49(2), 122-141
[13] Calero C, Cachero C, Córdoba J, and Moraga M (2007): PQM vs. BPQM: studying the tailoring of a general quality model to a specific domain. In: Advances in Conceptual Modeling – Foundations and Applications, 192-201
[14] FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase - Bank Secrecy Act Anti-Money Laundering Examination Manual. (2014, April 1). Retrieved January 15, 2018, from https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm
[15] Development and Acquisition Booklet - Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook). (2004, June). Retrieved January 19, 2018, from https://ithandbook.ffiec.gov/media/274741/ffiec_itbooklet_developmentandacquisition.pdf

Overall quality evaluation criteria and audit considerations

According to Sandman, J. (2007)[16], one of the first considerations for a financial institution acquiring COTS software is the compliance of the product with the overall requirements of the quality model from the entire enterprise perspective. Sandman also suggests that the financial institution should weight on the risk that software imposes on the bank's operations and its overall IT strategy. The FFIEC examination handbook [15: p.8] provides a guidance for meeting the high level objectives of establishing the quality of system and software products that address compliance requirements and satisfy the users' needs. In addition, a closer-defined selection of measures for evaluation of software products COTS software for AML purposes should include evaluations of the risks related to the acquisition of the product. The independent auditors function would include an assessment of the quality requirements against predefined criteria and evaluation for each quality characteristic of the software product.

1. Risks during acquiring and operating COTS software for AML
   According to our research, one of the first objectives of the acquisition program should be the identification of critical areas and risks events during the purchasing, both from technical and non-technical perspectives. There should be essential risk mitigation controls in place to mitigate this risk before those convert into severe cost, schedule, or performance problems affecting the overall financial institution performance and compliance. Those concerns are reflected in [15: p.9] requirements, therefore when assessing the acquisition cycle for AML COTS software, the auditors should review the design and the effectiveness of the controls related the planning, contracting, monitoring, acceptance and follow up activities related to the purchase. More specifically the auditor should enquire, obtain, and inspect the entity's risk management policies and procedures, and assess the way the financial institution has defined their mission-critical business process in relation to the AML activities and the software applications that support them. This should include the quality assurance programs and criteria for COTS evaluation

2. Critical control points
   The second most important factor affecting the overall quality of the COTS software is the entity's identification and documentation of the critical control points in the design of its information systems (IS). Main areas of audit interest related to AML COTS software are those control points that, if compromised, could permit an individual or group to gain unauthorized access to the IS or perform unauthorized or illegal activities on an entity's system or data. Those activities could lead directly or indirectly to unauthorized access or modifications to the key areas of audit interest, directly affecting areas such as transaction monitoring and customer identities.
   Control points characteristically comprise external access points to the entity's networks and interconnections with other external and internal applications. Since the AML systems are never run alone, these will be affected by the system components controlling the flow of data through the entire networks of the banks or to key areas, including critical storage and transaction processing servers, their corresponding operating systems, infrastructure applications, and business process applications.

[16] Sandman, J. (2007). AML Software Landscape Consolidates--and Expands. Securities Industry News, 19(24), 38

Most common control points also consist of network components where business process application controls are applied. For example, the input/output data points of the AML processes.

The USA PATRIOT Act (Sec. 362)[17] sets mandates for the FinCEN to establish highly secure networks as foundational requirements to "facilitate and improve communication between FinCEN and financial institutions". Furthermore, the Information Security Booklet – FFIEC Information Technology Examination Handbook (IT Handbook). (2004, April, p.13)[18] in section II.C.4 Control Implementation provides guidance for utilizing technology and software development processes, including quality. Additionally, this Booklet refers to the most recognized technology controls frameworks for assessment and evaluation of IT products into organizational information systems such as NIST Special Publication (SP) 800-53 Revision 4[19].

Detailed quality evaluation criteria considerations for AML software quality audit

The quality criteria are reviewed from two perspectives as noted in [8]:

A. A description of the criteria for evaluation to the extent the quality requirement specification in the AML context (various documents, and test results) are not executable at the development stage and what sort of quality is acquired when the system is made using measures – software product quality
B. Evaluating the realization degree of quality specifications of an AML software system in the light of its explicit domain usage and by specified users – software quality in use

These are outlined in Table 1 and Table 2.

Table 1 - Software product quality evaluation criteria

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
・ Monitoring functions need to work as expected – Risk - transaction monitoring does not ID the proper transaction for AML purpose; illegal/incorrect data processing may be carried out and waste of efforts to trace false	Functional suitability- "degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions"- [8:	Functional requirements traceability through the entire Software Development Lifecycle per [15: p.3] to include: ・ Functional requirement traceability result delivered with the COTS should be 100% trackable through the System Development Lifecycle (SDLC) from the processes of design, test, quality assurance, testing and software bugs resolution ・ Coordination to accurate calculation/reporting system of	・ Inquire to obtain and inspect documented set of functional requirements for the specific acquired AML COTS systems and its components ・ Compare bank's functional requirements against the developer's provided scope of functionalities come with COTS product. ・ Verify whether the functional documentation have been validated by the developer's

[17] USA Patriot Act 2001; Public Law 107-56 - October 26, 2001
[18] Information Security Booklet - Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook). (2016, September, p.13). Retrieved January 19, 2018, from https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
[19] NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
transaction could occur ・ Bank performs correct SAR filing ・ Need to verify that filtering works correctly.	4.2.1] Functional Completeness- "degree to which the set of functions covers all the specified tasks and user objectives" [8: 4.2.1.1].	insurance premium	internal software validation process (QA) or third independent party. Main criteria for AML should include accuracy, functional correctness of calculations, functional correctness of manual processes
・ Risk of the AML modules for accepting invalid input data elements (poor-quality, nonstandard data structures, non-valid country codes, accounts, etc.) ・ Need for the AML system to output non-skewed transactional analysis and results:	Functional suitability- Functional Correctness- "degree to which a product or system provides the correct results with the needed degree of precision" [8: 4.2.1.2].	・ The number of required specific accuracy requirements is actually delivered with the COTS ・ The quantity of items implemented in the COTS within the specific standard of accuracy required by the Bank and the number of data items requiring the specific standard of accuracy are in fact delivered ・ Accuracy of the calculation results against the calculation result stated in the specification. Evaluation of the number of incorrect calculations (false positives) detected during evaluation and the number of correct calculations delivered in the functional specification of the COTS ・ The number of functions for Transactions Monitoring, Customer ID, Filtering and Reporting compared against the stated in the implemented requirement specification. This includes the total of functions implemented incorrectly or fault functions ・ Traceability of the progress of the functions through the changes and revision history of the product(s)	Detection accuracy of the AML system itself is one of the most critical and risk prone elements from both quality and compliance perspective. This is because analytical tactics for customer risk scoring and transaction monitoring usually suffer from high false positives, which lead to substantial resources devoted to inspecting low-risk accounts and transactions. Furthermore, adding new calibration tools and thresholds habitually lead to additional spikes in the number of false alerts. Hence, an auditor should be obtaining and inspecting evidence that the bank applied due diligence in having records of developer's documentations about extensive tests coverages for accuracy within the logical flows covered by the software. Documentation should be available to demonstrate that the developer performed tests coverages for accuracy after significant software version changes. Inquire to obtain and inspect documented: ・ Developers documentation for tests for accuracy ・ Delivered proven results for false positives and thresholds
・ Monitoring the domestic	Availability- "degree to	・ Slow system becomes a compliance problem and bottleneck	Inquire to obtain and inspect documented test cases from the

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
or international transactions at high speed and with high reliability ・High target operation rate and ability of the users to use services when necessary ・When a problem occurs, the system should recover its capabilities within a short time	which a system, product or component is operational and accessible when required for use" [8: 4.2.5.2]	for the adjacent to the operations activities of the of bank ・System operates for 24/7/365 days, except during maintenance ・Recovery within 1 hour after a trouble is discovered	developer: ・Throughput capacity - the number of transaction per second. Both to read or to update data by more than one user or connected system(s) ・Fail over capabilities ・Batch processing normal finish rate ・Service switching time ・Service and reception times ・Handling time of job operation
・Data access control is regulated for each user through the systems ・All modules of the AML COTS product are furnished with security functions ・Risk of data breach	Confidentiality- "degree to which a product or system ensures that data are accessible only to those authorized to have access" [8: 4.2.6.1]	・Prohibiting access to the data points of the systems based on the roles played in the AML function ・Contents and number of operational limitations based on the functional roles ・Installation and usage limitation of software	Inquire to obtain and inspect documented from the developer specification for the: ・Encryption technology, operation control delivered through the COTS software ・Control of the access authority and individual authentication ・Considerations for personal information protection ・User authentication function ・Content control function ・Extent to which the access to system or data is monitored according to requirement. A test case from the developer should show a comparison of the number of accesses by a user to the system and data recorded in the access history database and actual number of accesses
・Risk of data falsification ・Preventive measures for data damage	Integrity- "degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data" [8:	・Segregation of operations and development is controlled. The COTS software is designed to prohibit accessing real data directly from the development side ・Encryption methods for the data once it enters the AML modules and the controls in place during operation ・Roles assignment capability ・Roles authorization capability ・Permission authorization	Inquire to obtain and inspect documented from the developer specification for the: •Validation tests of the integrity of the data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Programs •Data integrity and quality checks because Transaction monitoring systems (TMS)

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
	4.2.6.2]	capability	generally require some level of transformation logic which categorizes various transaction types into groups, which are monitored by different AML models ▪Tests against detected unauthorized access/operations and the number of illegal operations stated in the specification ▪Tests of acquisition of log, their ranges and contents for monitoring unauthorized access to business process within and on the boundaries of the systems, storage and on the network ▪Specific system policies configurations that comes with the COTS on the contents of application timing regarding application of security patches for handling vulnerabilities on the target system
▪ Contents of key management - key management using COTS software ▪ Deployment of digital signature that enables proof that the data is correctly processed and stored through the various AML modules ▪ Detect falsification of information	Non-repudiation- "degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later" [8:4.2.6.3]	▪ Access auditability for all transactions ▪ Presence of encryption of transmission data ▪ Access controllability ▪ Identification and authentication of all parties ▪ Authorization to perform the functions required for all parties must ▪ The integrity of the transaction content must be intact throughout the entire process ▪ Certain transaction information needs to be confidential for authorized users only	Inquire to obtain and inspect documented from the developer specification for the capability of the AML COTS software to comply to non-repudiation services for conformance for: ▪Non-repudiation of Origin: This capability would enable the verification for a signed message's originator and content through a data validity check – e.g. upon when the data enters the AML function ▪Non-repudiation of Delivery: This capability would enable the verification for digitally signature and a proof of delivery message - e.g. upon when the data exist the AML function and is received for example at FinCEN ▪Non-repudiation of Submission: This capability would enable the verification for digitally sign on a proof of submission message-

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
			e.g. from Customer Identity module to reporting and compliance module •Non-repudiation of Transport: This capability would enable the verification for providing proof that a delivery authority has delivered the message to the intended recipient
・Changes in business environment promptly and flexibly ・Risk of changes in launderers patterns ・Risk of changes in the compliance laws	Adaptability- "degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments" [8:4.2.8.1]	・Changes in the business processes ・Changes in technology – e.g. cloud ・Requirement on adaptability on the contents support from open source or the 3rd party products ・Changes in the data structure – e.g. ability to support various languages	Inquire to obtain and inspect documented from the developer specification for the capability of the AML COTS software to: ・Changes in the business processes, modeling and using services can be adapted as well as the capabilities for configuring and combining those in new and different ways ・Capabilities for adding additional services or adapting services can or swapping in where needed. ・Evaluate what will require changes (time/efforts) in the underlying application using these services. ・Assess the way the changes in business environment and capabilities that must operate on new or different computer platforms, in different computing environments (including internal development and testing environments), using different combinations of data sources, various and diverse communication protocols, including the human-computer interaction (HCI), and applications Tracking new or different AML patterns requires the AML COTS software to have range of configuration capabilities and adaptability to the environment in which they will reside. This includes interoperability between

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
			dissimilar platforms, and backwards compatibility to multiple previous releases

Table 2 - Software Quality in use evaluation criteria

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
・Work effectiveness and waste of resources and money that could lead to non-compliance ・Frequency of failures ・Completeness of the reports and compliance	Effectiveness- "Accuracy and completeness with which users achieve specified goals" [8: 4.1.1]	・Accuracy of the specified goals achieved ・Number of operational failures have occurred during work	・Inspect, observe, and compare the number of SAR completed accurately against the total number of SARs tasks put through the system ・Inspect, observe and compare the number of operational failures in several SARs that failed end to end completion against the total number of operations required to complete a SAR.
・Maintain compliance with AML regulations ・Process maturity and cost reduction ・Optimizing operations	Efficiency- "resources expended in relation to the accuracy and completeness with which users achieve goals" [8: 4.1.2]	・Time spent before and after a major module or the entire COOTS product is deployed ・Work duration ・Frequency of the updates for the reports to FinCEN ・Work efficiency on the accuracy of achieving the tasks	Inspect, observe and compare the number of: ・The time required to complete a SAR task before the product was implemented, and a month and a year after the deployment
・Risk of economic damage	Economic risk mitigation- "degree to which a product or system mitigates the potential risk to financial status, efficient operation, commercial property, reputation or other resources in the intended contexts of use" [8: 4.1.4.1]	・The way the IT investment in AML COTS software is effective from viewpoints of finance, customer, business operation processes and compliance (i.e. penalties) ・Missing item cases reported to FinCEN ・Delays in deliveries of the reporting and compliance due to not utilizing all the functions of the systems, rework, long and not efficient business process that the software product supports ・Reduction in personnel expenses, savings on inventory of the IT assets, lessening of material cost through COTS purchase	・Inspect, observe and review the IT Balance scorecard for adequacy of IT control mechanisms. The scorecards may uncover major problems in AML where it may be possible that the Board of Directors of a bank decides to go for electronic banking only. However, the AML solution modules chosen requires many "swivel chair" operations connecting automated and manual business thus inserting a significant economic risk into the operation by introducing a high probability for errors ・Inspect, observe and compare

Need criteria and risks	COTS Quality characteristics (from the model)	Quality Requirements	Evaluation and audit criteria
			whether there are gaps or missing cases that have occurred – sanctions, correspondent monitoring, FACTA not reported, etc.

Ranking the quality criteria

The research indicates that selecting a quality model for AML systems that meets both the users' needs and compliance requirements is a challenging endeavor. This is partly because these software systems have been in operation for many years without academic engagement in the development and proposal of domain specific software quality models. "Engagement" in this sense would include the process of selecting measures that can be used for establishing quality requirement definitions, characteristics, measurements, and evaluations for an audit. Therefore, given the fact that there are many trade-offs between the software product capabilities and the reality of the requirements of specific domain such as AML, it is not possible to satisfy all the software requirements at the same time. However, it is essential at least to provide some criteria ranking with the aspects of the quality in the software product. The criteria chosen and ranking are based on the evaluation and our analysis of the quality needs reflected in the data in Table 1 and Table 2.

Table 3 - Ranking the quality criteria

Quality criteria	Rank
Functional Suitability	1
Security	2
Reliability	3
Portability	3
Performance Efficiency	4
Effectiveness	4
Freedom from Risk	4
Efficiency	5
Maintainability	7
Satisfaction	9
Context Coverage	10
Compatibility	11
Usability	12

In most cases, the identified criteria do not fit perfectly to the target application context and need to be adapted in a next step to fine tune the model. In that case, unrelated criteria have to be removed, other ones require some modification, and missing criteria have to be created. Scientific literature on efficient adaptation of software QMs for the AML domain is largely missing. Specifically, to the AML COTS software, such customization is a compound, fault prone, and effort-intensive task for real-world QMs, involving intensive interactions with the business users, final users, and the compliance stakeholders. I identified quality characteristics that are either non-existent in the model [8] or require far more tailoring than the one described in the definition. For example, higher *flexibility* should be defined more precisely in the context of COTS AML software as the enhanced ability to configure the system to keep pace with emerging threats, so the enterprise will still be protected, even as the needs change. *Traceability* as a separate characteristic should enable the business for exploring the correctness of the information

processing in different stages of the AML process from account opening, transaction monitoring, through customer identification, reporting, and compliance.

The audit function's role in such a case is the independency and the expertise both in the specific AML domain as well as the subject matter proficiency in SDLC and software quality assurance. The auditors verify and validate whether the expected requirements and functionalities are in are fact delivered with the COTS solutions. This also includes policies/procedures for acquisition and independent test plans for evaluation of the fitness of the COTS product before and during the deployment and operation.

Conclusions

The application and use of software metrics for software processes and products is a multifaceted task that that allows us to track the status of the process and / or software product of software against goals. I provided consistent and mutually supportive sets of definitions, distinctions, guidelines, and proposed metrics for consideration from three perspectives: compliance, developer, and user. Although this framework is not complete, it has been brought to a point sufficient to support the metrics for evaluating COTS AML software. This work can also serve as a viable basis for future refinements and extensions. A number of software quality-evaluation metrics have been defined, classified, and evaluated with respect to their potential benefits and quantifiability factors.

The study reported in this paper provides clarity and defined outlines for assessing and tailoring the metrics associated with COTS AML. The overall quality can be measured using the standard characteristics in SQuaRE model mentioned in our research. Measuring quality-in-use is challenging because of the complexity of current standard models and the incompleteness of other, related customized models. However, specific metrics related to the AML domain by tailoring and customizing the main model can be derived.