The Financial Services Maturity Model for Anti-Money Laundering (FSMM (AML))

Tom O'Kane, Tara Casserly, Peadar McCartney

Governance Risk and Compliance Technology Centre
University College Cork
College Rd., Cork, Ireland
E-mail: t.okane@ucc.ie*, t.casserly@ucc.ie, p.mccartney@ucc.ie
*Corresponding author

Abstract: All modern businesses rely on processes for the delivery of their products or services. While a skilled, well trained, motivated workforce and the most up-to-date technologies are vital to business performance, it is the processes that actually define the business. Well-designed processes, securely embedded in an organization, drive a culture of compliance and will largely dictate the quality, timeliness and cost of delivery of the business' products or services. However, organizational culture is typically described as the component that is most difficult to assess and change. Maturity models are well established in a number of different domains and differ significantly from audit-style compliance models in that they provide a roadmap to guide and drive for cultural change in the organization and answer the question – does the organization have the capability to be compliant?

The Financial Services Maturity Model (FSMM) for Anti-Money Laundering (AML) described in this paper is a Governance Risk and Compliance (GRC) framework that describes the essential business process components that are necessary for effective implementation of AML and Combatting the Financing of Terrorism (CFT). It has been devised based on two key fundamentals; the theory of maturity models which represent growth in capability as a progression through a series of levels, and the extant international legislation, regulation, and best-practice information that pertains to anti-money laundering. The key objective of the FSMM (AML) model is to facilitate the embedding of an AML culture in financial services organizations.

Keywords: Maturity, Capability, AML, Money Laundering, CFT

Biographical notes: Tom O'Kane is a lecturer in Business Information Systems, and is a principal researcher in the Governance, Risk and Compliance Technology Centre (GRCTC), University College Cork, Ireland. Tom has a PhD in business process improvement and has over 20 years' industrial experience. He has worked for a number of international companies and travelled extensively providing process assessments, consultancy and advice. He has a special interest in process modelling and systems design.

Tara Casserly is a Research Support Officer working in the Governance, Risk and Compliance Technology Centre (GRCTC), University College Cork,

Ireland. Tara has over 10 years' experience of financial services and business process management. She has consulted widely for a number of major international banks. Tara specialises in business process improvement and CRM, and has led the design of major systems to meet AML requirements.

Peadar McCartney is a research support officer working in the Governance, Risk and Compliance Technology Centre (GRCTC), University College Cork, Ireland. Peadar has extensive international experience in financial services, anti-money laundering, taxation and education. He has also conducted several assignments in Sub-Saharan Africa for the EU, World Bank, and Government of Lesotho.

1 Introduction

The December 2012 penalty of $1.9billion imposed on HSBC Holdings plc was just one of a string of highly publicised Anti Money Laundering (AML) and sanctions breaches in both the US and in Europe and was part of a sweeping investigation into the movement of tainted money through the American financial system. In 2012 the inter-governmental Financial Action Task Force (FATF) estimated the total cost of money laundering at 2-5% of worldwide GDP equivalent to US$1.5trillion – US$3.5trillion [1]. The last few years have brought further reports of breaches of money laundering legislation which end up costing financial services organizations billions of dollars in penalties and remediation plus serious reputational damage. This is despite the fact that the vast majority of these organizations will have invested heavily in people and technology to counteract money laundering activities. For instance, estimates of global spending on AML compliance in 2013 are expected to be in excess of US$5.8bn[2]. Attempts at mitigating AML risks are largely driven through an emphasis on compliance with specific requirements within legislation and regulation; essentially gap analysis of individual processes in an audit style approach within federalised silos, rather than addressing the processes on an enterprise-wide basis. The audit approach may be helpful but it is inadequate and thus the prevailing culture is one of ensuring AML compliance audits are successfully passed, rather than what is really needed - embedding a culture of consistently doing what is ethically correct, and making good AML judgements across the entire organization. Devising a method by which the business processes for AML could be improved and embedded in the culture of the organization, would be far more valuable and is the underlying rationale for this research.

2 AML and Cultural Change

The need to establish an ethical culture in the organization has been called for repeatedly. For instance, in a 2003 speech given by Lori A. Richards, Director, Office of Compliance Inspections and Examinations for the U.S. Securities and Exchange Commission[3] she stated:

"It's not enough to have policies. It's not enough to have procedures. It's not enough to have good intentions. All of these can help. But to be successful, compliance must be an embedded part of your firm's culture. It is critical that firms establish a strong culture of compliance that guides and reinforces employees as they make decisions and choices each day."

Many other regulatory authorities have made similar calls and through an analysis of these calls we have identified a set of four common requirements that need to be addressed.

1. Embed an AML risk aware and compliance culture in the organization
2. Move the organization to be compliant with the spirit as well as the letter of the law
3. Ensure the AML and compliance culture verifiably reflects the values and risk appetite espoused by the leadership within the organization
4. Drive for an AML culture where individual responsibility is stimulated and rewarded

AML compliance models focus on an organization's compliance with legislation and regulation and do not focus on bringing about cultural change, even though cultural change is what is required. By contrast the model we propose in this paper, the Financial Services Maturity Model for AML (FSMM (AML)), does address cultural change.

The FSMM (AML) assesses the organization's *process capability to be compliant* with legislation and regulation and strives for the *embedding of compliance capability* within the organization's culture. It is not a compliance model; it does not assess the organization's actual compliance with legislation or regulation but what it does do is enable early remediation, due to identification of weaknesses within the process.

3 Concept of Process Capability

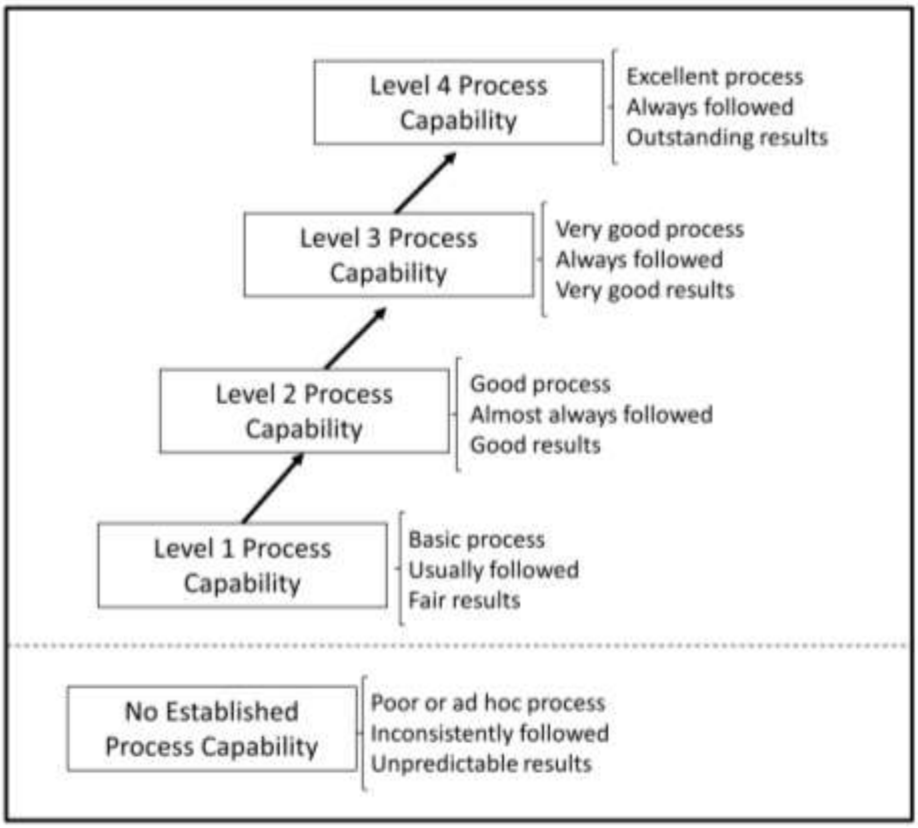
Maturity models describe how an organization can progress from having poorly performing immature processes that give highly unpredictable results to high performing processes that generate superior results. These quality improvement models, based upon Crosby's Management Maturity Grid[4], and the principles of continuous process improvement, originated in the 1980's, and have grown in popularity ever since. They are used in a diverse range of businesses including ERP, software development, project management, etc.

The fundamental concept is that business processes must undergo continuous incremental improvement following an evolutionary path through stages of increasing capability, as illustrated in Figure 1 below.

Performing a process effectively at one capability level provides a solid foundation for evolutionary progress to the next level. The progression of improvement in capability is demonstrated through:

- The strength and integrity of the process, advancing from poor or ad hoc processes, to excellent, world-class processes.
- The adherence to execution of the process, going from one that is inconsistently followed to one that is always followed without exception.
- The results that are achieved through the process, progressing from unpredictable outcomes to outstanding outcomes.

Figure 1 Capability Maturity Model Structure



The original need for such a model was raised with our research team by a financial industry consortium in 2012, who among other things noted that while credit and market risk models for banks have been mature for some time, the operational risk models have not.

Capability maturity models have been widely used to guide process improvement, and embed sustained and verifiable improvement in the culture of businesses around the world. Hence the maturity model approach is a very appropriate framework on which to base the FSMM (AML).

4 Literature Review

Literature review is standard research practice used to establish a theoretically sound basis for the research. Hence, an extensive and detailed literature review of international AML legislation, regulations, guidelines and standards was carried out to guide and ensure the architectural integrity of the FSMM (AML) model. Table 1 (below) shows a sample of the legislation and regulation we investigated.

Table 1 Literature Sources for FSMM (AML)

Jurisdiction	Legislation & Regulation
USA	• Bank Secrecy Act Regulations (31 CFR Chapter X, FinCEN, Department of the Treasury) [5] • Bank Secrecy Act Anti-Money Laundering Examination Manual. Federal Financial Institutions Examination Council [6] • OFAC Sanctions Programs [7]
EU	• Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. (4th Directive)[8] • Regulation No 1781/2006 on information on the payer accompanying transfers of funds [9]
UK	• The Money Laundering Regulations 2007 [10] • Prevention of Money Laundering/Combating Terrorist Financing: Guidance for the UK Financial Sector. Joint Money Laundering Steering Group [11] • Financial Conduct Authority Handbook [12]
Australia	• Anti-Money Laundering and Counter-Terrorism Financing Act [13] • AUSTRAC Regulatory Guide [14]
Netherlands	• Dutch National Bank Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act [15]
Ireland	• Criminal Justice (Money Laundering and Terrorist Financing) Act [16] • Criminal Justice (Money Laundering and Terrorist Financing) Act Guidelines [17] • International Financial Sanctions. Department of Finance [18]
International	• International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation . The FATF Recommendations [19] • ISO 31000, Risk Management – Principles and Guidelines. International Standards Organisation [20] • Wolfsberg Standards. The Wolfsberg Group. [21]

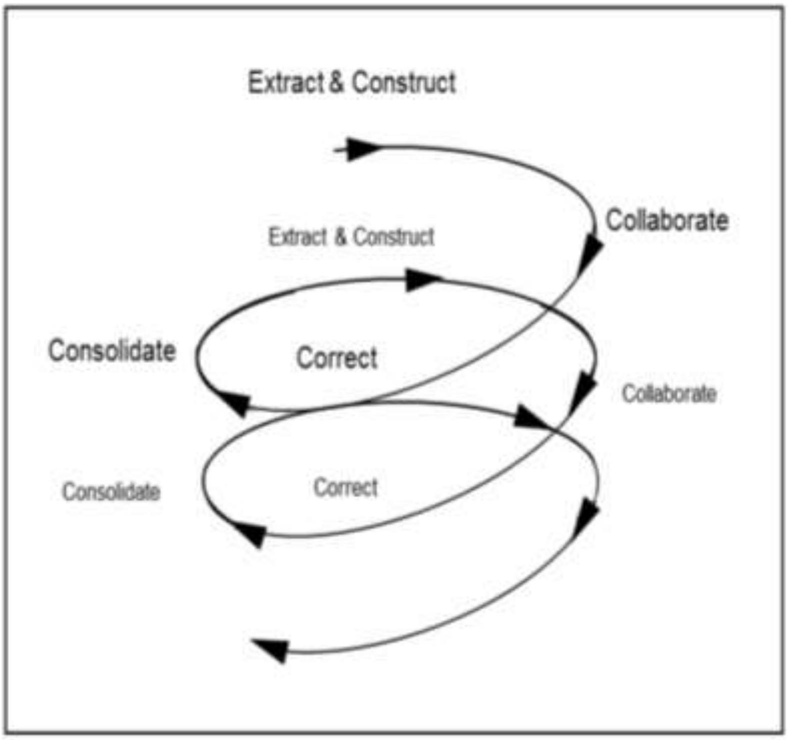
These literature sources were combined with contributions sourced through participation and interview with legal and industry experts in a range of financial institutions.

In addition to the literature sources on AML we also conducted an extensive literature review of process modeling techniques and especially the CMM/CMMI maturity models developed by the Software Engineering Institute of Carnegie Mellon University in Pittsburgh, USA, [22,23] which were used to inform the design and structure of the FSMM (AML).

5 Research Method

To conduct this research and develop the maturity model we followed an iterative Action-Research based approach. This research methodology is proven to be very effective in investigations into cultural and social phenomena and the development of theories and models in many other areas such as education, healthcare, and organizational development.[24,25,26] Practitioners with AML management responsibilities have extremely valuable expert knowledge and experience of the problem. Hence, frequent engagement with industry-based AML subject matter experts was also required to ensure the feasibility and applicability of the FSMM (AML) model. To produce the model we worked directly with representatives from Citibank, Bank of Ireland, Allied Irish Bank, and BAE Detica Systems. The research model is shown below in Figure 2.

Figure 2 Action Research Model for Creating the FSMM (AML)



The research spiralled through a series of four phases:

1. Extract and Construct
2. Collaborate
3. Correct
4. Consolidate

before recommencing with the Extract and Construct phase again.

In the Extract and Construct phase, information from legislation and regulation was extracted and this was used to construct a model component. Model components are individual Process Areas that contain process descriptions, goals, activities and institutionalization factors; they are described more fully later in the paper. This is also referred to as theory building.

The model component was then presented in the Collaborate phase to our industry reviewers to peer review the component and provide their comments. Apart from gaining valuable insight from the practitioners this was also a means to provide on-going validation of the model construction through engagement with professional subject matter experts.

In the Correct (or learning) phase we incorporated the updates and refinements from the Collaborate phase into the newly created model component and we also incorporated any new learning for creating future model components.

In the Consolidate phase we integrated the new model component with the other already completed components and reviewed the domain for coherence and coverage. We also reviewed and refined the action-research approach. Then the research returned to the Extract and Construct phase to create the next model component.

On average creating a component could take between four and eight weeks depending on the difficulty of the area being investigated.

Data collection and component construction is on-going in this respect and the model has an expected completion date of December 2013, however plans for conducting pilot assessments are underway and are scheduled to begin during Q1 2014 in a number of selected financial services organizations.

6 Comparison of Maturity models and Audit models

Before detailing the structure and contents of the FSMM (AML) it is worth examining some of the key differences between Maturity models and Audit models.

In terms of their approach audit models tend to be adversarial or even confrontational, where typically an auditor who may be external or internal to the organization will examine work products or process execution for non-compliance. The organizational context may not be considered and the results are typically binary; compliant or non-compliant. In contrast maturity models tend to be more collaborative. The capability assessment team will work with the organization to indicate process strengths and weaknesses vis-à-vis the normative reference, i.e. the maturity model. The results are more likely to be richer textual descriptions that take into account the organizational context.

Having an emphasis on compliance, audit models have a tendency to focus on the “letter of the law”, which leads to a prevailing culture of ensuring AML compliance audits are successfully passed, rather than what is really needed - embedding a culture of consistently doing what is ethically correct and making good AML judgment’s, across the entire organization. Maturity models, while concerned that an organization’s processes have the capability to be compliant with the “letter of the law” are also concerned with embedding a culture of risk awareness for complying with the “spirit of the law”.

Hence, while the aim of audit models is to find instances of non-compliance with AML legislation and regulation, it is the aim of maturity models to guide process improvement, embed cultural change, and develop organizational compliance capability.

In terms of their perspective, audit models are essentially a ‘point-in-time’ examination of compliance for a few selected discrete areas of a firm’s business, whereas maturity models can take either an organization wide or, a deep, single process view of current capability and projected capability improvement.

Outcomes from audits are typically focused on recent activities and reported as a series of deficiencies with respect to AML legislation and regulation. Outcomes from maturity assessments are typically focused on process capability and how that capability can be improved and progressed.

Embedding cultural change features very highly in maturity models and is done through specific institutionalization factors, whereas this is not a feature of audit models.

7 The FSMM (AML)

The FSMM (AML) is intended, to define all of the processes required to meet an organization’s AML and Sanctions obligations under international legislation and regulation. The major contribution of the model is that it goes beyond identifying compliance obligations. When used as an assessment vehicle it will inform the organization of strengths in its AML processes, and opportunities for improvement of its AML processes. The model is independent of any single jurisdiction, is independent of organization size, and is informed by work conducted internationally for the development of continuous process improvement models and best practice in other areas, specifically in risk management. Again, the model does not assess the organization’s compliance with legislation or regulation but the organization’s *process capability to be compliant* with legislation and regulation by virtue of having essential AML processes established and followed.

Through in-depth consultations with industry experts and analysis of the need to have an enterprise-wide approach, the research team identified five Domains the FSMM (AML) needed to focus on. The FSMM (AML) domains are:

- Governance
- Risk
- Due Diligence
- Investigation and Reporting
- Organizational Support

The domains were created to provide repositories for logical groupings of AML model components. Hence, each domain contains Process Areas that were created for particular aspects of AML and are essential to process improvement and cultural change. There are a total of sixteen process areas distributed between the five domains. Figure 2 below shows the distribution of process areas across the various domains.

Table 2 FSMM (AML) Domains and Process Areas

FSMM (AML) Domains	Process Areas
AML Governance	○ AML Architecture Definition ○ AML Strategy Definition ○ AML Policy Formulation ○ AML Quality Assurance
AML Risk	○ AML Risk Identification and Assessment ○ AML Risk Mitigation
AML Due Diligence	○ Customer Onboarding ○ Transaction Monitoring ○ Customer Monitoring ○ Sanctions
AML Investigation & Reporting	○ AML Alert Disposition
Organizational Supports	○ Record Keeping ○ Human Resource Management ○ AML Training ○ Data Measurement and Analytics ○ AML Process and Technology Improvement

The process areas in the AML Governance Domain focus on the overall approach for directing and controlling the organization, using a combination of management information and hierarchical management control and reporting structures. The governance structures are the foundation for managing compliance with legislative and regulatory requirements for AML. There are four process areas in the domain:

- AML Architecture Definition establishes a governance infrastructure for effective AML risk management that supports the organisation's strategies, standards and policies. It describes the fundamental elements the organization utilizes to meet its legislative and regulatory obligations for AML risk management.

- AML Strategy Definition produces an operational definition of the AML strategy that will be followed by the organization. This includes identifying the set of strategic objectives that AML risk management seeks to achieve, to drive for compliance with legislation and regulation, and to embed a culture of risk awareness in the organization.

- AML Policy Formulation translates the organization's AML risk strategies into tangible assets that can be used for the day to day management of risks associated with AML. It results in a broad outline of the policies to be implemented for key risks and operational activities.

- AML Quality Assurance provides the board with assurance of the compliance and effectiveness of all AML processes and visibility into AML operations, processes and controls within the organization.

The necessity for an AML Risk Domain is based on legal and regulatory requirements. The process areas in the AML Risk Domain reflect the fact that AML legal and regulatory requirements are founded on a risk-based approach which has two elements: identifying and evaluating risks, and then deciding what can be done to mitigate those risks.

- AML Risk Identification and Assessment enables the organization to identify and quantify potential AML risks inherent in its business profile, the selection of the necessary assessment tools and the creation of a risk classification system. This results in the development of a risk register that provides the basis for strategy, policies and risk mitigation activities.

- AML Risk Mitigation reduces the extent of exposure to AML risk and formulates measures to be taken should a risk become an issue. Risk mitigation has three key components – the procedures or additional controls that are put in place to reduce the risk, technology tools applied to monitoring the risk, and the actions required once the risk materialises.

The process areas in the AML Due Diligence Domain are necessary for knowing who your customer is (KYC) and therefore meeting Customer Due Diligence (CDD) obligations as well as identifying suspicious behaviours or transactions by customers.

- Customer Onboarding establishes a consistent approach to meeting the customer due diligence (CDD) obligations as set out in the relevant legislation and regulations. It is concerned with the capture of KYC data enabling the customer to be classified and assigned to a risk category prior to establishing a relationship or carrying out any transactions, as appropriate.

- Transaction Monitoring is intended to systematically review customer transactions and transaction patterns to detect potentially suspicious events and to comply with directions from regulatory and enforcement agencies regarding restricting certain transactions.

- Customer Monitoring is the systematic review of customer activities to detect potentially suspicious events and changed circumstances, and to comply with directions from regulatory and enforcement agencies regarding restricting certain activities or transactions.

- Sanctions implementation follows a consistent process that enables the organization to effectively monitor transactions for sanctions breaches, to block transactions where appropriate and to report attempted and actual breaches.

The process area in the AML Investigation and Reporting Domain is key for managing alert investigations and reporting of suspicious transactions.

- AML Alert Disposition establishes a consistent approach to investigating transactions or transaction patterns and reports of suspicious activities. The scope of the investigation process will involve the collection of the due diligence information and the transaction or activity information giving rise to the alert..

Finally, the process areas in the Organizational Supports Domain are not necessarily AML specific, in this model they focus on two distinct AML requirements: 1. Obligations under legislation and regulation (Human Resource Management, AML Training, and Record Keeping) and, 2. Internal management issues (Process and Technology Optimization, and Data Measurements and Analytics).

- Record Keeping ensures there is a consistent approach to meeting all legislative and regulatory obligations regarding the retention and maintenance of data and records. This is of special significance for AML.

- Human Resource Management ensures that with regard to AML there is a consistent approach to meeting all legislative and regulatory obligations regarding the hiring, retention, and promotion of staff. The aim is to assure the organisation that as well as monitoring customer behaviours and transactions the organisation is performing employee due diligence by monitoring its employee’s fitness and probity.

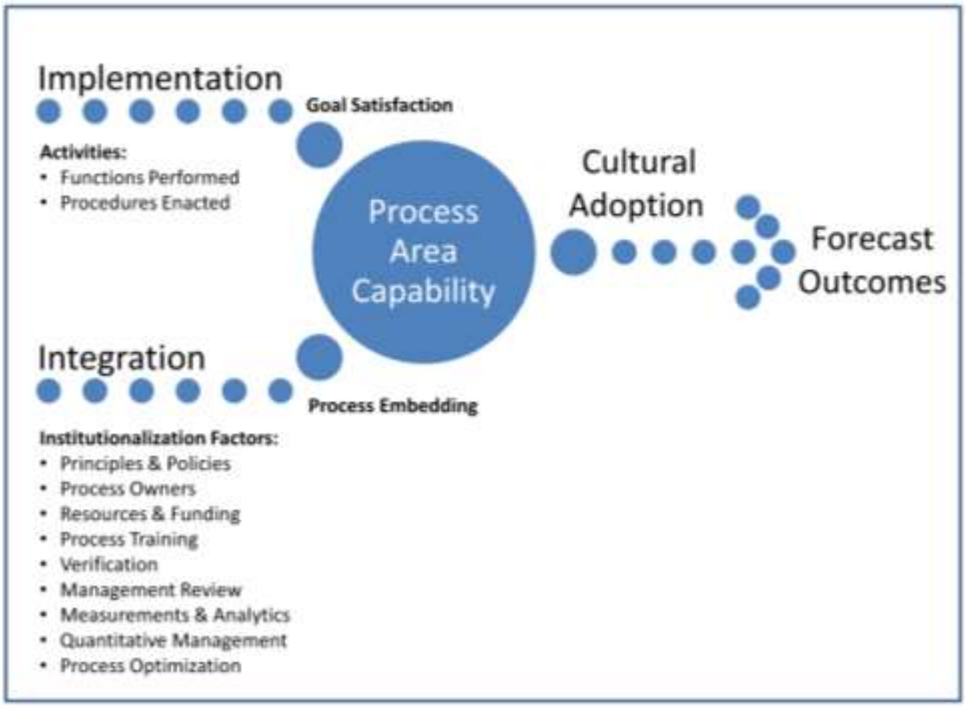
- AML Training develops the skills and knowledge of people within the business so they can perform their roles effectively and efficiently to support the organization’s strategic business objectives for AML. The scope of the training process area will cover the establishment of a training responsibility and the development and delivery of training courses.

- Data Measurement and Analytics establishes a quantitative understanding of business performance and enables an objective approach to decision making. The focus in the context of this model will be on the usage of appropriate metrics and their correct application for AML.

- AML Process and Technology Improvement drives for continuous incremental and discontinuous innovative change that measurably improves the processes and technologies used for AML by the organization.

Every process area follows a common structure containing: Process Area descriptions, Goals, Activities and Institutionalization Factors. An outline structure for each process area and what they are intended to achieve is shown in Figure 3.

Figure 3 Process Area Components, Usage and Outcomes



Each Process Area has a process description that outlines the purpose, necessity, ownership, objectives, and outputs of the process area. This is followed by a number of Goal descriptions that collectively fulfil the intent of the process area and provide a means for logically grouping the practices that are intended to *implement* and *integrate* the process area.

Implementation is achieved by the organization performing Activities for specific AML practices associated with the process area. Typically these activities are functions that people actually perform in their day-to-day roles, and at all levels of responsibility in the organization, and could cover for instance, performing risk assessment, reviewing transactions, engaging with customers, and so on. Each activity will be associated with a specific level of capability.

Integration is achieved through following Institutionalization Factors that are designed to embed the AML practices within the organization. Typically factors for institutionalizing a process could include, for instance, having defined policies, having process owner's assigned, appropriate resources and sufficient funding available, and so on. Each institutionalization factor will be associated with a specific level of capability.

As stated previously the process areas, goals, activities, and institutionalization factors were all created through intensive literature review of legislation and regulation to identify and inform their development.

Appraisal of process area capability can be performed by comparing what the model advocates as expressed in the Activities and Institutionalization Factors, with what the organization is actually doing. This is akin to holding a mirror up to the organization to gauge how well it's processes compare with the 'ideal' and how well institutionalized they are. The outputs generated will be process strengths and clearly identified opportunities for improvement that may enable the organization to take remedial action before their next compliance audit is due to take place.

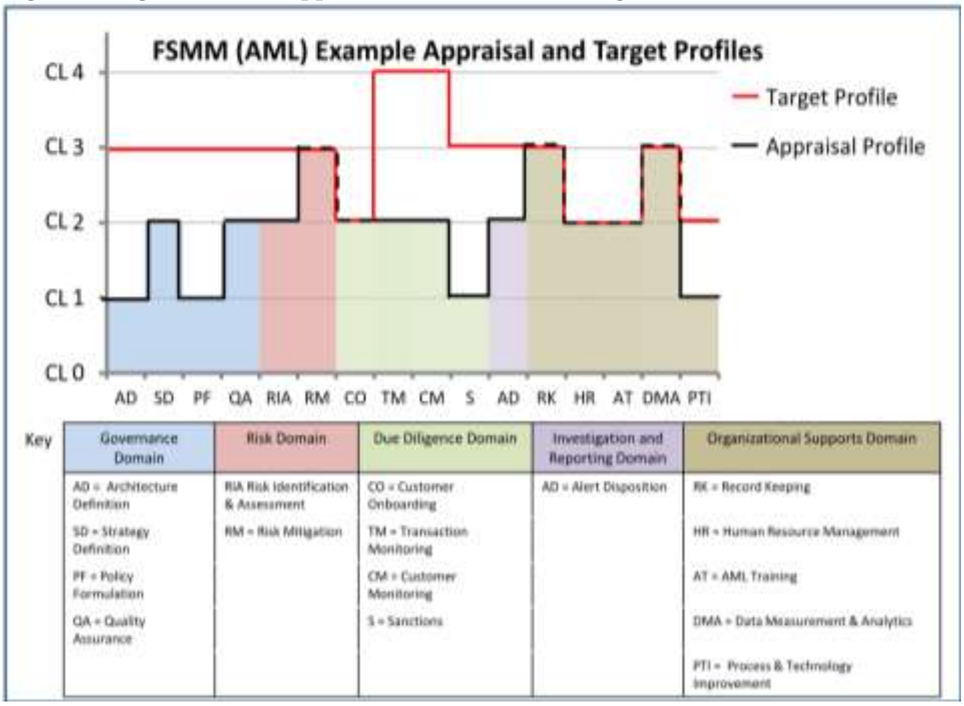
The FSMM (AML) assesses a *process area's capability to be compliant* with legislation and regulation and strives for the *embedding of compliance capability* within the organization's culture. The extent of the organization's goal satisfaction and process embedding will in effect give an indication of the Process Area's Capability, its Cultural Adoption, and the Forecast Outcomes. These are characterised for each capability level in Table 3 (below).

Table 3 Capability Level Characteristics

Capability Levels	Process Performance	Cultural Adoption	Forecast Outcomes
CL 4	The AML Process Area performance is proactive – leading to a predictive capability influencing business decision making	Full deployment of institutionalisation factors – excellent cultural adoption	Likely to have excellent compliance outcomes
CL 3	The AML Process Area performance is understood quantitatively – risk decisions are based on transparent, accurate and rigorous analytics	Majority deployment of institutionalisation factors – solid cultural adoption	Likely to have good compliance outcomes
CL 2	The AML Process Area performance is consistent across the organisation – following an enterprise wide approach	Reasonable deployment of institutionalisation factors – good degree of cultural adoption	Likely to have reasonable compliance outcomes
CL 1	The AML Process Area minimally performed – giving repeatable results but are localised and lack an enterprise-wide approach	Less fragmented deployment of institutionalisation factors - weak cultural adoption	Likely to have unpredictable compliance outcomes
CL 0	The AML Process Area is incomplete - significant gaps leading to inconsistent decision making and poor risk management	Very fragmented or no deployment of institutionalisation factors – poor or no cultural adoption	Likely to have poor compliance outcomes

Performing an appraisal of all sixteen process areas covering the five domains allows the organization to build up a composite picture of process capability across the organization such as that shown in figure 4 (below).

Figure 4 Organizational Appraisal Outcomes and Target Profile



This representation of the process is very flexible as it enables the organization to create a target profile as shown in figure 4. The target profile is used to express the desired capability the organization would like to have for its process areas and the relative importance that the organization places on one process area versus another. So it allows the organization to focus on a single area or multiple process areas. It also enables the organization to assess the resources that will be required in order to improve their processes and the relative order in which improvement should take place and where the gaps are greatest between the desired capability level and the assessed capability level.

The capability levels also provide a longitudinal record of continuous improvement that shows the organizations willingness to improve its AML processes and the actual progress made.

7 Business Advantages of the FSMM (AML)

It has been known for many years, for different businesses in a wide range of industries, that increasing process capability will reduce wastage, improve quality and increase operating efficiencies. Early feedback the researchers have received from industry sources indicate that by using the FSMM (AML) to increase process capability and to instil a culture of compliance, an organization will greatly reduce the possibility of AML infringements and of failing regulatory reviews.

An organization that possesses reliable knowledge about its legislative and regulatory obligations for AML and the ability of its processes to meet those obligations has a marked advantage over organizations that do not have this knowledge or insight. Knowing exactly where processes are failing and where remedial action is required means resources are not being wasted on constant 'fire fighting' and are instead improving areas that really matter to the business for AML compliance.

Process variability is typically due to human error. This is because either a standard process doesn't exist and people have to take decisions by themselves which turn out to be flawed and compromise the business, or a process does exist but it isn't followed due to the prevailing culture within the organization and again the business is put at risk. By using the FSMM (AML) the business can clearly identify all the essential AML processes that it needs to create and deploy for consistently doing the right thing.

The FSMM (AML) can provide a mechanism for independent and, if necessary, anonymous benchmarking of the process capability of the business with an established standard, with other divisions or departments within the firm, or between businesses. This facility could allow businesses to evaluate how they compare with peer organizations within their firm, how they compare with competitors, or how they compare with expected standards set perhaps by regulatory bodies.

Risk management is a key concern for all financial services businesses. Awareness of AML risk and compliance with legislation and regulation are essential if the business is to avoid falling foul of regulatory authorities and incurring severe financial penalties. The FSMM (AML) will not alone improve the organization's AML processes but through the institutionalization factors will also enable high quality risk management by embedding a risk aware and compliance culture across the organization.

7 Conclusion

In this paper we have described a capability maturity model for AML. We have identified the essential processes that an organization must have in place if it is to perform its AML functions successfully. We acknowledge our research is still at an early stage, but from comments and enquiries the research team has already received from the financial services industry we believe the development of the FSMM (AML) will make a major contribution, to the management of AML and CFT. It will give organizations a significant risk mitigation capability, and will also inform the theory of how models based around organizational capability can be leveraged to yield superior business performance and compliance for financial services. Finally, while the model is limited to AML and CFT, it does open up research opportunities for similar models in other areas of financial services.

Acknowledgements

This work was supported by Enterprise Ireland, East Point Business Park, Dublin 3, Ireland

References

1 FATF (2012) *FATF steps up the fight against money laundering and terrorist financing*, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html

2 Katkov, N. (2011) *Trends in Anti Money Laundering 201*', Celent Report, http://www.celent.com/reports/trends-anti-money-laundering-2011

3 Richards, L.A. (2003) *The Culture of Compliance*, U.S. Securities and Exchange Commission, Spring Compliance Conference: National Regulatory Services, Tucson, Arizona, http://www.sec.gov/news/speech/spch042303lar.htm

4 Crosby, P., (1979) *Quality is Free: The Art of Making Quality Certain*, McGraw Hill, New York

5 FinCEN (Financial Crimes Enforcement Network) (2011) *Bank Secrecy Act Regulations*, Department of the Treasury, 31 CFR Chapter X, http://www.fincen.gov/statutes_regs/bsa/

6 Federal Financial Institutions Examination Council (2011) *Bank Secrecy Act Anti-Money Laundering Examination Manual*, http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf

7 US Department of the Treasury (2013) *OFAC Sanctions Programs*, http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

8 European Commission (2013) *Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, 4th Directive, http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm#moneylaundering

9 The European Parliament and of the Council (2006) *Regulation No 1781/2006 on information on the payer accompanying transfers of funds*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF

10 United Kingdom Statutory Instruments (2007) *The Money Laundering Regulations 2007*, http://www.legislation.gov.uk/uksi/2007/2157/pdfs/uksi_20072157_en.pdf

11 The Joint Money Laundering Steering Group (2010) *Prevention of Money Laundering/Combating Terrorist Financing: Guidance for the UK Financial Sector*, www.jmlsg.org.uk/download/6130

12 Financial Conduct Authority (2013) *Financial Conduct Authority Handbook*, http://www.fshandbook.info/FS/html/FCA/

13 Government of Australia: Australian Transaction Reports and Analysis Centre (2006) *Anti-Money Laundering and Counter-Terrorism Financing Act*, http://www.austrac.gov.au/aml_ctf.html

14 Government of Australia: Australian Transaction Reports and Analysis Centre (2009) *AUSTRAC Regulatory Guide*, http://www.austrac.gov.au/regulatory_guide.html

15 Dutch National Bank (2011) *DNB Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, http://www.toezicht.dnb.nl/binaries/DNB%20Guidance%20on%20the%20Anti-Money%20Laundering%20and%20Anti-Terrorist%20Financing%20Act%20and%20the%20Sanctions%20Act_tcm50-223813.pdf

16 Irish Statute Book (2010) *Criminal Justice (Money Laundering and Terrorist Financing) Act*, http://www.irishstatutebook.ie/2010/en/act/pub/0006/index.html

17 Irish Government Department of Finance (2012) *Criminal Justice (Money Laundering and Terrorist Financing) Act Guidelines*, http://www.finance.gov.ie/documents/guidelines/Criminaljustice2012.pdf

18 Irish Government Department of Finance (2008) *International Financial Sanctions*, http://www.finance.gov.ie/viewdoc.asp?fn=/documents/FinancialSanctions2008/Finsanctionsindex08.htm

19 FATF (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation . The FATF Recommendations*, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

20 International Standards Organisation (2009) *ISO 31000-2009, Risk Management – Principles and Guidelines*, http://www.iso.org/iso/home/standards/iso31000.htm

21 The Wolfsberg Group (2013) *Wolfsberg Standards*, http://www.wolfsberg-principles.com/standards.html

22 Paulk, M. C., Weber, C. V., Curtis, B., Chrissis, M. B. (1993). *Capability Maturity Model for Software (Version 1.1)*. Technical Report (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University). CMU/SEI-93-TR-024 ESC-TR-93-177.

23 Chrissis, M. B., Konrad, M., Shrum, S. (2003) *CMMI, Guidelines for Process Integration and Product Improvement*, Addison-Wesley

24 Susman, G. I. (1983) *Action Research: A Sociotechnical Systems Perspective*, in Beyond Method, Morgan, G. (ed), Sage Publications, London, pp.95-113

25 Reason, P., Bradbury, H. (2007) *Handbook of Action Research*, 2nd edition, Sage Publications, London.

26 French, W.L., Bell, (1973), *Organization development: behavioral science interventions for organization improvement*, Prentice-Hall, Englewood Cliffs, New Jersey