Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6– No.9, April 2017 – www.caeaccess.org

Requirement's for Proposed Frameworks for Secure Ecommerce Transactions

Kenneth Longo Mlelwa
PhD Student, School of CoCSE
NM-AIST, Arusha
Tanzania

Zaipuna O. Yonah, PhD
Senior Lecturer, School of CoCSE
NM-AIST, Arusha
Tanzania

ABSTRACT
This study proposes the best set of criteria for evaluating a secure framework that are to support eCommerce with security requirements analysis and elicitation, based upon the construction of a context for the system and satisfaction arguments for the security of the system. The novel contribution of this paper is an information security framework hail as the secure framework, comprising of technical, operational, business, process and maturity models to address information security requirements for eCommerce transactions.

General Terms
Secure Frameworks

Keywords
E-commerce Framework, eCommerce Framework Requirements, Secure eCommerce Framework, Security Framework.

1. INTRODUCTION
This part introduces the major concepts that will be referred to throughout this paper, which are eCommerce, Framework and Security.

Electronic commerce (E-commerce, eCommerce or EC) has various definitions1. E-commerce can be defined as a commercial exchange system, which makes use of computers, and communication network advancements. It is the use of production information in electronic form instead of paper, for business or government operations. This suggests that e-commerce means using technological advances to promote everything involving the exchange of business information among computers and humans or traders and customers [1].

For the purposes of this paper, eCommerce is defined as the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. Due to that; everyone who is using eCommerce needs to be concern about the security of their personal information. But how it can be ensured is a mountain to climb and need to be solved, hence security is the major concern in eCommerce.

A framework can be defined as a set of beliefs, ideas, or rules that is used as the basis for making judgment and decisions [2] in order to provide guidance and governance of business processes and operations. The IT governance frameworks have been developed to manage IT services, processes and infrastructures so that it can enhance security services such as; access control, confidentiality, integrity, availability and accountability. In this case, IT governance is the responsibility of leaders, security managers and security professionals to ensure that the enterprises IT systems are operated under high profile of information security. Generally, each business varies in the usage of IT governance framework and sometimes one combines more frameworks to manage effectively their IT business process and operations.

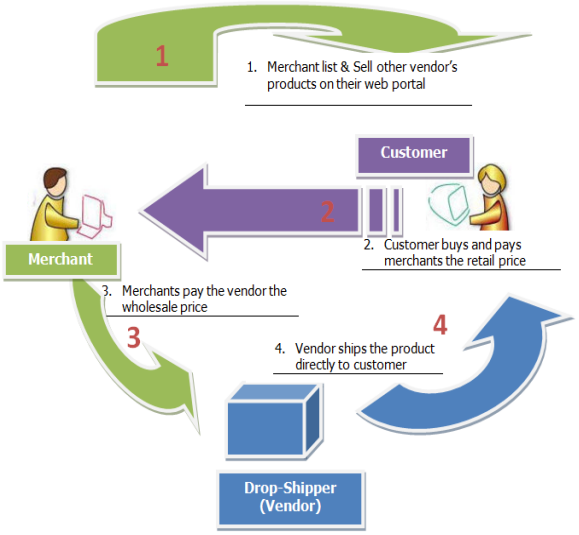

Figure 1: General E-commerce life Cycle

Security refers to the prevention of damage caused by the actions of attackers. Attackers are people who gain by utilizing system failures, intentionally or accidentally provoked. This gain usually results in some damage to the system owner. In the Computer Science and Communications Dictionary [3], Security in information technology has been defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Information security management is an area that has been addressed through guidelines and standards from various organizations [4]. Technical, operational and management perspectives on information security has been presented in standards and guidelines [5] [6]. These guidelines have been put into practical draw on various organizations and are chiefly based on attaining the

[1] WIPO report carries a 4 page Annex compiling 10 different definitions

security goals of Confidentiality, Integrity and Availability (CIA). Additionally, Accountability is now flattering another important principle as electronic transactions need to be traceable and parties held accountable for their actions. However, information security depends on the framework in which it is being applied and the tackling of information security initiate with a threat assessment and an understanding of the particular framework in which security is being addressed [7] [8]. This study particularly looks at information security frameworks for eCommerce transactions.

2. FRAMEWORK BASICS

The Framework provides a universal language for understanding, managing, and conveying security risk both within and outwardly. It can be used to help identify and prioritize measures for reducing security risk or threat, and it is a tool for aligning policy, business, and technological approaches to administering that risk. It can be used to manage security risk across the whole organizations or it can be focused on the rescue of vital services within an organization.

Different kind of entity – such as sector harmonizing structures, associations, and organizations, can deploy the Framework for different reasons, including the creation of common Profiles.

Holistically Framework is a risk-based advance to managing information Security risk, and is consist with three categories: The **Framework hub** (or Framework Core), the **Framework Implementation Levels** and the **Framework Profiles**. Every Framework components emphasizes the relationship between business drivers and information security behavior [9].

2.1 Framework Hub

The Framework Hub provides a set of actions to attain specific information security outcomes, and references examples of direction to attain those outcomes. The Hub is not a check-list of actions to perform. It presents key information security outcomes identified by industry as helpful in managing information security risk. The Hub includes four entities: Functions, Categories, Subcategories, and Informative References, depicted in Figure 1:

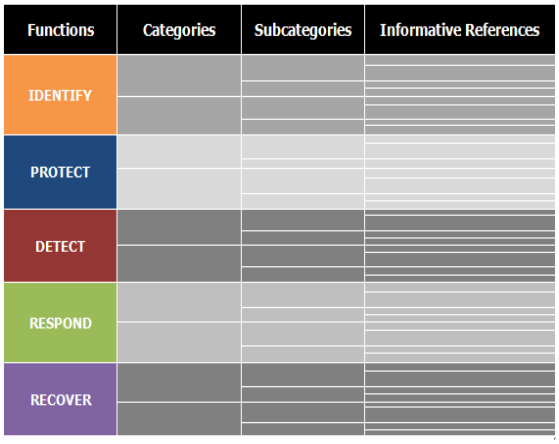

Figure 2: Framework Hub Structure [9]

The Framework Hub entities work mutually as follow:

- **Function** organizes fundamental information security activities at their highest stage. These are Identify, Protect, Detect, Respond, and Recover. They help a business in expressing its management of information security risk by organizing information, enabling risk management decisions, tackling threats, and improving by learning from preceding activities. It also aligns with existing methodologies for incident management and help show the impact of investments in information security. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.
- **Categories** are the subsection of a Function into set of information security outcome closely tied to programmatic needs and particular activities. Examples of Categories consist of "Asset Management," "Access Control," and "Detection Processes."
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category; such as "outside information systems are catalogued," "Data-at-rest is protected;" also "Notifications from detection systems are investigated."
- **Informative References** are specific sections of regulars, guidelines[2], and practices common among critical infrastructure sectors that demonstrate a method to achieve a certain goals in associated with every Subcategory. The Informative References presented in the Framework Hub are illustrative and not exhaustive. They based upon cross-sector guidance mainly frequently referenced throughout the Framework development process.

[2] NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Information security Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6– No.9, April 2017 – www.caeaccess.org

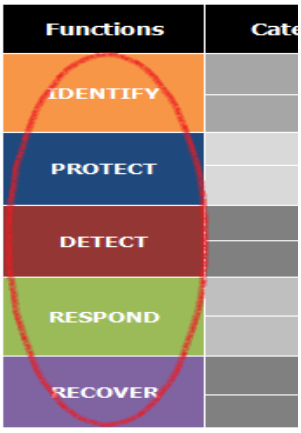

Figure 3: Five framework Hub's functions

The Five Framework Hub's Functions are defined here under. These Functions are not planned to form a sequential path, or guide to a static preferred final state. Rather, the Functions can be performed parallel and continuously to form an operational culture that addresses the dynamic information security risk.

- **Identify** – these build up the organizational understanding to manage information security risk to systems, assets, data, and capabilities. The actions in this Function are foundational for effective use of the Framework. Understanding the business background, the resources that sustain critical functions and the related information security risks permits a business to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Such outcome Categories within this Function are: - Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.
- **Protect** – these build up and implement the appropriate safeguards to guarantee delivery of critical infrastructure services. This Function supports the ability to contain or limit the impact of a potential information security event. Such outcome Categories within this Function are: - Information Protection Processes and Procedures, Awareness and Training, Maintenance, Data Security, Access Control and Protective Technology.
- **Detect** – these build up and implement the appropriate actions to identify the occurrence of a information security event. This Function enables well-timed discovery of information security events. Such outcome Categories on this Function are: - Anomalies and Events; Detection Processes and Security Continuous Monitoring.
- **Respond** – these build up and implement the appropriate actions to react regarding a detected information security event. The Respond Function enables the ability to hold the impact of a potential Information security event. Such outcome Categories on this Function are:- Communications, Improvements, Response Planning, Mitigation and Analysis
- **Recover** – these build up and implement the appropriate actions to maintain tactics for resilience and to restore any capabilities or services that were impaired due to an Information security event. The Recover Function enables timely recovery to normal operations to reduce the impact from an Information security event. Such outcome Categories on this Function include: Communications, Improvements and Recovery Planning

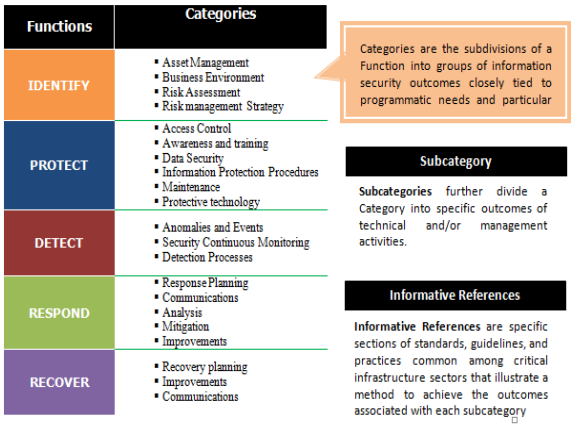

Figure 4: The Framework Hub identifies underlying key Categories and Subcategories for each Function and maps them to Informative references

2.2 The Framework Implementation Levels

Framework Implementation Levels shows context on how a business views Information security risk and the procedures in place to manage that risk. Levels describe the amount to which a business' Information security risk management applies exhibit the characteristics defined in the Framework (e.g., repeatable, adaptive and risk and threat aware). The Levels characterize a business, practices over a range, from Partial (Level 1) to Adaptive (Level 4). These Levels echo a progression from informal, reactive responses to approaches that are agile and risk informed. Throughout the Level selection process, a business should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints [6].

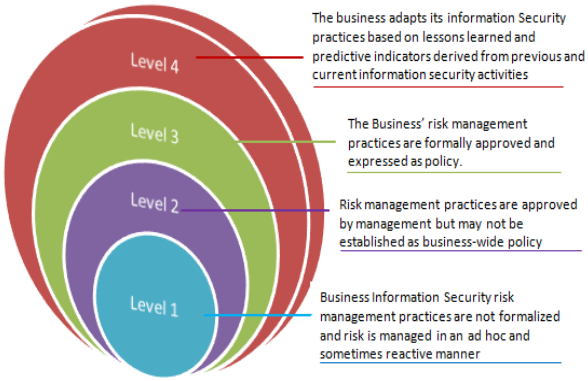

Figure 5: Framework Implantations Levels

2.2.1 Level 1: Partial

- **Risk Management Process** –Business information security risk management practices are not formalized, and risk is managed in an ad hoc and on occasion reactive manner. Prioritization of information security behavior may not be directly informed by business risk objectives, the business/mission requirements or threat environment.
- **Integrated Risk Management Program** – There is inadequate knowledge of information security risk at the business level and the business -wide approach to managing information security risk has not been established. The business implements information security risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The business may not have processes that enable information security information to be shared within the business.
- **External Participation** – A business may not have the processes in place to chip in coordination or collaboration with other entities [6].

2.2.2 Level 2: Risk Informed

- **Risk Management Process** – Risk management practices are accepted by management but may not be established as business-wide policy. Prioritization of information security behavior is directly informed by business' risk objectives, the business/mission requirements or threat environment.
- **Integrated Risk Management Program** – There is knowledge of information security risk at the business level but on business-wide approach to managing information security risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has sufficient resources to perform their information security duties. Information security information is shared within the business on an informal basis.
- **External Participation –** The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

2.2.3 Level 3: Repeatable

- **Risk Management Process** – The business' risk management practices are formally accepted and expressed as policy. Organizational information security practices are often updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- **Integrated Risk Management Program** – There is a business-wide approach to manage information security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- **External Participation** – The business understands its dependencies and partners and receives information from these partners that allows collaboration and risk-based management decisions within the business in response to events.

Level 4: Adaptive

- **Risk Management Process** – The business adapts its information security practices based on lessons learned and predictive indicators resulting from previous and current information security activities. During a process of continuous improvement incorporating advanced information security technologies and practices, the business actively adapts to a changing information security landscape and responds to evolving and sophisticated threats in a timely manner.
- **Integrated Risk Management Program** – There is a business-wide approach to managing information security risk that uses risk-informed policies, processes, and procedures to tackle potential information security events. Information security risk management is part of the business culture and evolves from knowledge of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- **External Participation** – The business manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve information security before an information security event occurs [6].

	Risk Management Process	Integrated Risk Management Program	External Participation
Partial	o Not formalized o Reactive	o Limited knowledge o Irregular risk management o Private information	No external collaboration
Risk Informed	o Approved practices o Not widely use as policy	o More knowledge o Risk-informed, processes & procedures o Adequate resources o Internal sharing	Not formalized to interact & share information
Repeatable	o Approved as policy o Update regularly	o Business approach o Risk-informed, processes & procedures defined & implemented as intended and reviewed o Knowledge & skills	o Collaborate o Receive information
Adaptive	Continuous improvement	o Risk-informed, processes & procedures for potential events o Continuous knowledge o actively	Actively Shares information

Figure 6: Detailed Framework implementation Levels

A. A Framework Profile

This Framework Profile (or "Profile") is elaborated as the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization [9]. A Profile allows business to establish a roadmap for reducing information security risk that is well aligned with business and sector goals, **considers legal/regulatory** requirements and **industry best practices**, and reflects risk management priorities. Given the complexity of many organizations, they may prefer to have multiple profiles, associated with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the initials/current state or the expected final/target state of specific information security activities. The Current Profile shows the information security goals that are currently being achieved. The Target Profile shows the goals needed to achieve the expected

information security risk management outcomes. This Profiles support business/mission requirements and helps in the communication of risk within and between organizations.

Similarity of Profiles (e.g., the Current Profile and Target Profile) may expose gaps to be addressed to meet information security risk management objectives. An action plan to address these gaps can lead to the roadmap described above.

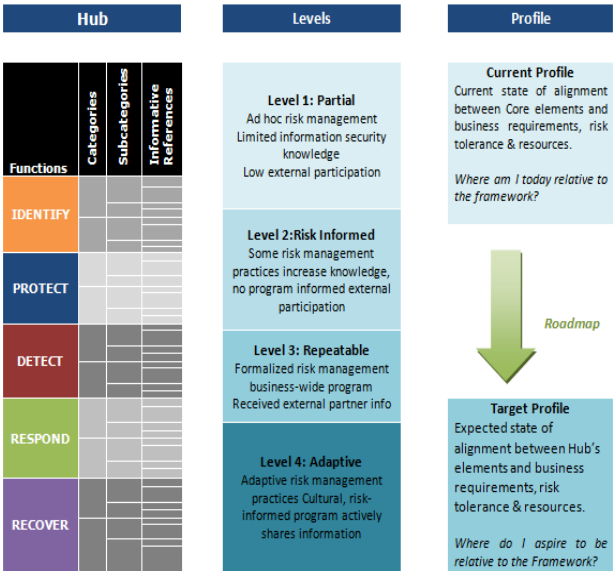

Figure 7: framework Profile

3. STANDARDS RELATED TO INFORMATION SECURITY

The term "*standard*" is at times used within the context of information security policies to differentiate between standards, procedures and written policies. Businesses Organizations should uphold all three levels of documentation to help secure their environment.

- *Information security policies* are high-level rules or statements about protecting systems or people. (For instance, a policy would state that "*Company X will maintain secure passwords*").
- A "*standard*" is a low-level instruction for the various ways the company will implement the given policy. (For instance, "*Passwords will be at least 8 characters, and require at least one number*.")
- A *"procedure*" can describe a step-by-step method to implementing various standards. (For instance, "*Company X will enable password length controls on all production Windows systems*.")

This use of the term "standard" differs from use of the term as it relates to information security and privacy frameworks. From above explanation a reference to the use of standards in addressing information security has been discovered, this part describes standards that are relevant to eCommerce transactions.

Open and freely available standards are referred to where possible. The exemption in standards issued by the ISO (International Organization for Standardization) since this is the de-facto standards body recognized worldwide.

The thorough investigation into use of standards is motivated by the need to develop a novel framework in eCommerce transactions which need not "re-invent the wheel", but rather concentrate on those specific mechanisms that will address context sensitive needs, as will be presented in this study. It also addresses some of the barriers to eCommerce including information exchange, resource constraints and technical platforms.

The following section, a depiction of standards and their relationship to information security for eCommerce transactions are describes.

3.1 Non-technical Standards

ISO/IEC 27001 –Information security management: The ISO/IEC 27000 family of standards helps organizations keep information assets secure [4]. This family of standards helps organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the well-known standard in the family providing requirements for an *Information Security Management System* (ISMS). An **ISMS** is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

The significance of this standard to eCommerce transactions is that individual Business-organization involved in an eCommerce transaction should have mechanisms or internal processes to address information security.

NIST SP 800 Series: The U.S. National Institute of Standards and Technology has been building an extensive collection of information security standards and best practices documentation. The NIST Special Publication 800 series was first published in 1990 and has increase to provide guidance on just about each and every aspect of information security. Even though not specifically an information security framework, NIST SP 800-53 is a model that other frameworks have evolved from. U.S. government agencies utilize NIST SP 800-53 to comply with the Federal Information Processing Standard's (FIPS) 200 requirements. Even though it is specific to government agencies, the NIST framework could be applied in any other industry and should not be overlooked by companies looking to build an information security program.

FIPS PUB 200 is the Minimum Security Requirements for Federal Information and Information Systems [10]. This standard can be obtained by downloading free from www.csrc.nist.gov. The standard specifies 17 security areas for which federal organizations are required to develop and adopt policies. Some of these that narrate to this study are [11]: Access Control, Identification and Authentication, Maintenance, Physical and environmental protection, Systems and Information Integrity, System and Communication protection.

This standard addresses information security requirements discussed in this study.

Network and Information Security Standards Report, Issue 6.2: The report identifies the increasing importance of the reliability, availability and security of networks and information systems to the economies in Europe as well as proposes standards to address current security threats. This

Report [12] can be downloaded for free from http://www.cen.eu.

This report is aimed to be used by Business-organizations with a curiosity in information security standards and guidelines; these business-organizations may represent stakeholders, small and medium sized enterprises (SMEs) or large organizations, may be governments or may be public interest bodies.

OECD 81829 2002: this standard is named Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [5]. This standard is available for free from www.oecd.org

It is outline nine principles intended at instilling a culture of security in organizations. It also identifies the need for the incorporation of security as an essential element of information systems and networks. These nine principles are [5], Awareness of the need for information security; Response to security incidences; Responsibility for the security of information systems; Democracy, that is, security of information systems and networks should be compatible with the essential values of a democratic society; Ethics, that is, respect for the legitimate interest of others; Risk assessment; security design and implementation; Security management and finally, Reassessment of information security management systems.

3.2 Technical Standards

The above section presented the standards and guidelines which mostly addressing the information security management process. For addressing the technical aspects of information security, a survey of existing technical information security standards is presented in this section. These standards which will be presented here are those related to the technical components/mechanisms that can be utilized to implement eCommerce transactions.

3.2.1 XACML

XACML (eXtensible Access Control Markup Language) is a policy language which uses XML statements to present access control policies. XACML version 2.0 was ratified as a standard by OASIS in February 2005 [12].

Table 1: XACML Components

XACML Components	Description
Policy Enforcement Point (PEP)	Point which manages access authorization policies
Policy Decision Point (PDP)	Point which evaluates access requests against authorization policies before issuing access decisions
Policy Retrieval Point	Point where the XACML access authorization policies are stored, typically a database or the file-system.
Policy Information Policy	The system entity that acts as a source of attribute values (i.e. a resource, subject, environment)
Policy Administration Point	Point which manages access authorization policies

XACML Stapes;

1. A user sends a request which is intercepted by the PEP
2. The PEP converts the request into a XACML authorization request
3. The PEP forwards the authorization request to the Policy Decision Point (PDP)
4. The PDP evaluates the authorization request against the policies it is configured with. If needed it also retrieves attribute values from underlying Policy Information Points.
5. The PDP reaches a decision (Permit / Deny / Not Applicable / Indeterminate) and returns it to the PEP

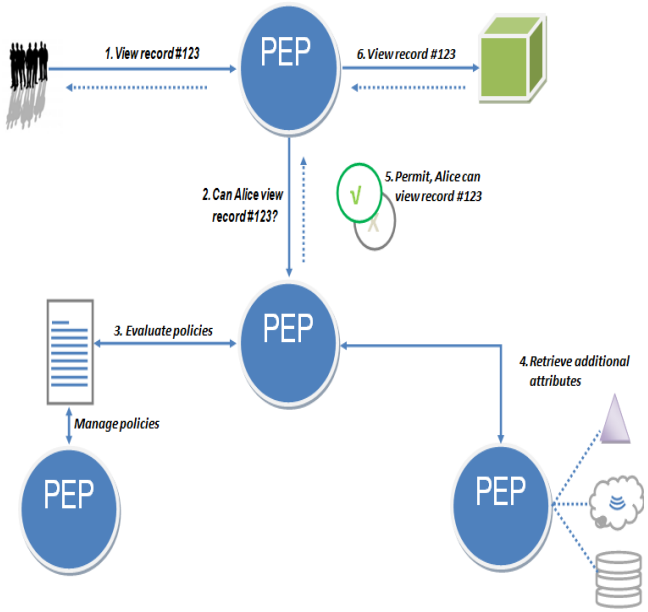

Figure 8: XACML architecture and a sample authorization flow

Here, an access control model, based on XACML and using SAML attributes is developed and presented as part of the information security framework for eCommerce transactions.

SAML: Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authorization and authentication data among parties, in particular, between a service provider and an identity provider. SAML is a product of the OASIS Security Services Technical Committee [12].

SAML assertions are of three categories that are, Authentication assertions, Attribute assertions and Authorization Decision assertions. An assertion is defined as a piece of data regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource. Assertions are created by a SAML authority, which is a conceptual system entity in the SAML domain model. The web service or user requesting assertions from the SAML authority is called the Requester. These assertions are then utilized in communicating with an entity called a Responder, who utilizes those SAML assertions to respond appropriately to the Requester. In a web services environment, SAML assertions may be carried within a SOAP message. Other than assertions, SAML is also consists of protocols, bindings and profiles. Protocols allow

service providers to request for assertions, authentication and name identifier registration and mapping. Bindings are the mappings from SAML request-response message exchanges into standard messaging or communication protocols such as SOAP and HTTP. A profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application.

The main SAML use case is called Web Browser Single Sign-On (SSO). A user wielding a user agent (normally a web browser) requests a web resource protected by a SAML service provider. The service provider, wishing to know the identity of the requesting user, issues an authentication request to a SAML identity provider through the user agent. The resulting protocol flow is depicted in the following diagram.

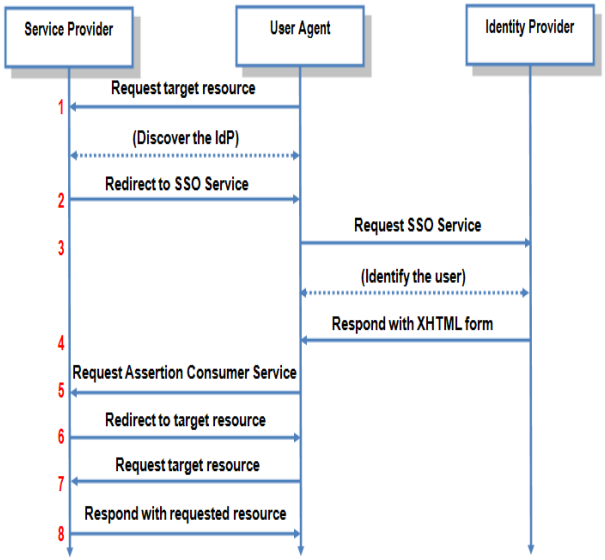

Figure 9: using SAML in a Web browser

3.2.2 Web Services (WS) Security Framework:

The goal of the WS Security Framework is to have a standard way of managing web services security in transactions derived from entities that might have different security policies/environments. This framework has been adopted by OASIS as a standard [12] this table here under summarizes the security standards for Web Services.

Table 2: WS Security Framework Components

WS Security Framework component	Description
SOAP Message Security	Portrayed enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.
Username Token	This describes how a web service consumer can provide a Username Token as a way of identifying the requestor by "username", and optionally using a password to authenticate that identity to the web service producer.
WS-Policy	A Web service provider may define conditions (or policies) under which a service is to be provided. The WS-Policy framework enables one to specify policy information that can be processed by web services applications, such as Oracle WSM.
Kerberos Token	This is a cross-platform authentication and single sign-on system. The Kerberos protocol provides mutual authentication between two entities relying on a shared secret (symmetric keys).
SAML Token	Describes how to use SAML assertions with the WS Security SOAP message specification
X.509 Certificate	This is a signed data structure designed to send a public key to a receiving party. A certificate includes standard fields such as certificate ID, issuer's Distinguished Name (DN), validity period, owner's DN, owner's public key, to name a few.

Web Service Security Requirements:

The following outlines the Web service security requirements:

Use transport security to protect the communication channel between the Web service consumer and Web service provider.

Use message-level security to ensure confidentiality by digitally encrypting message parts; integrity using digital signatures; and authentication by requiring username, X.509, or SAML tokens.

Web Services Security framework, is designed to implement and define Web services security in heterogeneous environments, including authentication, authorization, message decryption and encryption, signature generation and validation, and identity propagation across multiple Web services used to complete a single transaction.

The standards and guidelines presented above tackle security requirements that are applicable in many settings. On the other hand recognizing that a successful implementation should take context into consideration, standards organizations have started moving towards investigating context specific standards and guidelines.

4. FRAMEWORK REQUIREMENTS FOR PROPOSED SECURE ECOMMERCE TRANSACTION

The main difficulty with elaborating a framework is that many steps or outputs are unspecified or abstract. To conquer this difficulty, in this study we instantiate the framework using a combination of Goal-Oriented Requirements Engineering [13] and Problem Frames [14], describing it in terms of a set of activities.

4.1 Security Goals

Security goals are resultant of the business goals of the system [15]. A few numbers of actors, operations, and objects will be

needed to satisfy the business goals. To rephrase somewhat the introduction to this study, security goals occur when stakeholders found that they wish to avoid damage to some objects in the perspective of the system, be they tangible (e.g., cash) or intangible (e.g., information), that have direct or indirect significance. Objects signified in either way are called *assets*, and the stakeholders normally wish to protect themselves from any damage that might come from abusing these assets.

Security requirements for any system depend on its functions, the types of data it processes, the other systems (if any) with which it communicates, and the environment in which it operates [16].

Damage could not be to the asset itself (direct damage), but instead could be a result of some misuse or abuse of the asset (indirect damage). Examples of indirect damage include damage to reputation due to exposure of flawed hiring policies, loss of contracts results of exposure of pricing or costing detail, or loss of trade secrets during the theft of some newly designed widget. In other words, one is not necessarily protecting assets from damage, but is instead protecting against damage caused by abuse of assets.

The security community has itemized some common security concerns, cataloging them with the letters C, I, A, and more recently a second A (C,I,A,A) [14] (and other security textbooks):

- **C**onfidentiality: ensure that an asset is visible only to actors authorized to see it.
- **I**ntegrity: ensure that the asset is not corrupted.
- **A**vailability: ensure that the asset is readily accessible to agents that need it, when they need it.
- **A**uthentication: ensure that the identity of the asset or actor is known. A common example is the simple login.

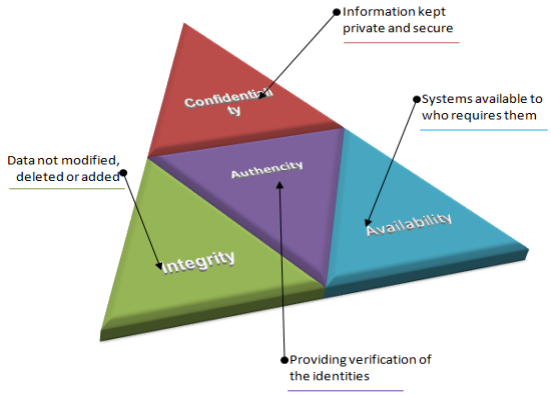

Figure 10: Common Security goals.

Another set of security goals can be originated by combining *Actors*, *management/Operational* control principles and *application/technical* business goals. Actors here are those who participate during business transaction these include *Merchants* and *Clients.* Again Management control principles consist of common security principles for instance least privilege and separation of duties [18]. Application/technical business goals will determine the applicability of management control principles to the system, such as by defining those privileges that are needed for the application, and excluding those that are not.

Figure 11: Other Security Concern

4.2 Security requirements

Security requirements can be defined as constraints on the functions of the system, where these constraints functionalize one or more security goals as follows:

1) They are limitations on the system's functional requirements, rather than themselves being functional requirements.
2) They express the system's security goals in functional terms, precise enough to be given to a designer/architect.

The truth is, security requirements are constraints on functional requirements rather than different functional requirements is vital for validation of the functional requirements. Validating a set of functional requirements in the face of constraints is trouble-free than validating requirements comprising of the original functional requirements and the additional functional requirements appended for security. In the first case, one requires checking only that prior the functions are constrained; they still do what they originally were intended to do. In the second case, the system designer decides how the requirements interact and how the interactions are realized. Only after design is complete one should check to see if functionality has changed beyond acceptability.

5. TOWARD SECURE FRAMEWORK

This proposed Framework is a process designed to evolve with changes in information security threats, processes, and technologies. In achieve, this Framework visualizes effective security as a dynamic, continuous circle of reaction to all threats and solutions. Thus, businesses that implement this Framework will be in better positioned to comply with future security and privacy regulations. At the least, businesses that operate in regulated industries should begin screening how regulators, examiners, and other sector-specific entities are changing their review processes in response to the security Framework.

Based on above explanations their some parameters and steps need to be considered on designing the secure ecommerce transactions; the framework is a unified framework, which consists of five models which are based on the perspectives discussed in above part of Security goals. These are:

1) Technical Model: The technical model presents technical mechanisms that work together to address the information security requirements for eCommerce transactions.

2) Operational Model: The operational model presents operational mechanisms that need to be implemented during eCommerce transaction to address information security requirements. The Operational Model makes no assumptions about the technical capabilities of actors, or even that the transactions that are taking place in the eCommerce transaction are entirely electronic transactions.
3) Business Model: this model presents governance mechanisms that need to be implemented at a policy level within an organization. These include organizational policies, national and regional legislation.
4) Process model: The process model presents the way that the secure framework can be implemented within an organization and amongst businesses that plan to undertake eCommerce transactions. This process model captures the context whereby resources to carry out whole security implementations at one go may not be available and where there may be lack of coordination across businesses with regards to eCommerce implementations.
5) Maturity model: The maturity model provides a mechanism for businesses to continually measure progress with regards to meeting information security requirements for eCommerce transactions.

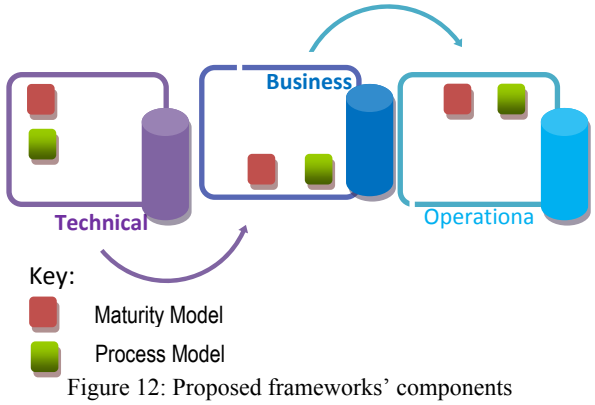

Figure 12: Proposed frameworks' components

Figure 10 depicts the five parameters. Three of them, are the technical, business and operational models, appear as pillars and the remaining two models, which are the process and maturity models, are found inside of it across those pillars. This means that in every model, the technical, operational and business pillars can be applied independently to meet information security requirements for eCommerce transactions, as and when resources are accessible. The process and maturity models help the business to continually move towards a holistic information security framework, by inserting mechanisms in the technical, operational and business models onto each other.
The players in an eCommerce transaction are individual personals and business organization who have to comply with national and regional legislation set by the Government and with organizational policies that are set by the businesses. The functions of each of the major player determine who implements the models of the Framework as shown in Table 1.

Table 3: Secure Framework implementation by main Players in a Secure eCommerce Transaction

Player	Function	Secure model Implemented
Business	Launch legislation and policies that tackle the information security objectives and requirements; approve or accept standards that address the information security requirements.	Business / Organization
Business-Executive	Launch policies within the organization to tackle the information security requirements	
Business-Operational	Set in place operational plans and mechanisms to tackle the information security requirements	Operational
Business-Technical	Apply technical mechanisms to meet information security requirements	Technical

The process model presents steps to implement the business, operational and technical models, while the maturity model allows merchants and businesses to track how their information security practices are growing to fully meet the information security objectives.

These models are independent and can be developed in parallel. The common aspect is that all the models are implemented with similar security objectives and requirements in mind. It serves as the mapping mechanism from one model to another, and the maturity model provides guidance to ensure that businesses are continually improving towards a holistic information security framework.

The details of every model are presented here under;

5.1 Secure Technical Model

The technical model of a secure framework summarizes technical components that can be used to meet the information security requirements.
Any confirmed solution that can tackle the security requirements can be integrated in the technical model. Currently, four components that can tackle the security objectives are described in more detail. These can be deployed by technical team by themselves or in collaboration with operational team. These four components are Attribute Based Access Control; eCommerce Ontologies, SOA and third Part

Trustee.

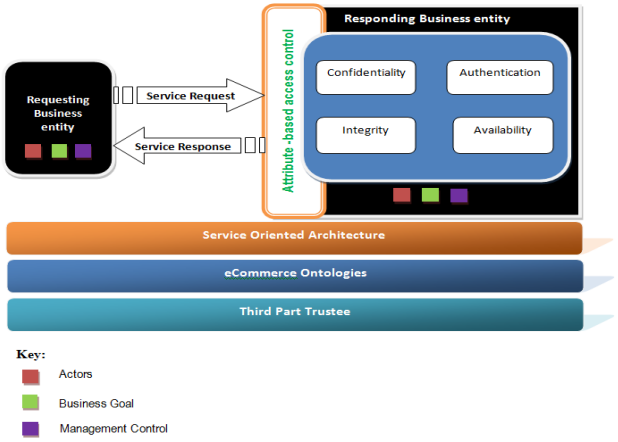

Figure 13: Secure Technical model

The base of figure 11 above shows the components to be used to meet the eCommerce Information Security: requirements. ABAC is a novel mechanism proposed in this study as being particularly suited to eCommerce transactions. The security model components are described in further details in the sections below, jointly with implementation guidelines for the technical departments of business.

5.1.1 Attribute-based access control (ABAC)

Attribute-based access control (ABAC) defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action. For example: IF the requestor is a manager, THEN allow read/write access to sensitive data.[19]
The rationale of the ABAC is that it is a robust access control mechanism that tackles the authorization, access control and privacy security requirements in eCommerce transactions. This mechanism is based on open standards i.e. SAML[3] and XACML[4] and takes into consideration prevailing legislation. SAML assertions are used for authentication while XACML is used to formulate policies and to provide a rule combining algorithm and delegation in policy decisions.
This is helpful in eCommerce transactions in cases where a service may involve information that crosses legislative domains. One organization can delegate part of the authorization decisions based on the law and policies in the participating organizations. SAML may be used jointly with XACML Authentication, Authorization Decision and Attribute assertions being issued by the Certificate Authority which is part of the operational guidelines.

[3] Security Assertion Markup Language (SAML, pronounced sam-el) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.
[4] XACML stands for "eXtensible Access Control Markup Language". The standard defines a declarative fine-grained, attribute-based access control policy language, architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies.

5.1.2 E-commerce Ontologies.

The use of standards such as XACML and SAML as integrated in the ABAC model tackles syntactic interoperability. Ontologies are a helpful tool for attaining semantic interoperability. Ontology is a formal representation of concepts in a particular domain. The ontologies developed can be deployed to ensure accurate access control decisions in eCommerce transactions. The ontologies will be based on the familiar terminology in the operational model.

The reason of eCommerce ontology in the secure technical model is to allow the definition of attributes that will be deployed in access control and authorization decisions. In an eCommerce transaction where there may be no human being involvement, an incorrect authorization may be made since an assertion originate from the requesting machine may be interpreted in other way round from the consumer's policies. By using a familiar ontology, semantic interoperability is achieved.

5.1.3 Service Oriented Architecture (SOA)

A SOA is defined by World Wide Web Consortium (W3C) as a set of components which can be invoked, and whose interface descriptions can be published and discovered. W3C also define a Web Service as a software system designed to support interoperable machine-to-machine interaction over a network [20]. It has an interface expressed in a format that machines can process. Other systems act together with the Web service in a way prescribed by its description using SOAP messages, typically conveyed using HTTP with XML serialization in conjunction with other Web-related standards. Web Services are used to implement service-oriented architectures.

In a eCommerce transaction, exchanges are typically machine to machine interaction. The reason of a SOA in the Secure Technical Model is to attain the availability security goal, when implemented with web services. This is due to the fact that web services are technically neutral, so a web service produced by any business can be utilized by another business organization regardless of differences in technical platforms in the two businesses.

5.1.4 Third Part Trustee

Third Part Trustee (TPT) contains of components that permit parties to communicate securely over public networks with the use of public key cryptography. A certificate authority provides/issues and verifies certificates that are given to the parties during a transaction. For eCommerce transactions, a TPT could be agreed upon to act as a certificate authority for businesses organizations.

The use of PKI in the Secure Technical Model would permit organizations to use the internet as a means of communications, as a result avoiding expensive point to point secure links between businesses

Supportive Resource for implementing the Secure Technical Model

For a sustainable implementation, Businesses organization can keep the latest advances in access control similar standards or research that would be useful for eCommerce transactions. The list is not complete but provides a direction as to where a starting point for those standards and mechanisms are referred to in this model.

Table 4: Supportive Resource for implementing the Secure Technical Model

Source	Resource	Reason
http://webstore.iec.ch/preview/info_isoiec14516%7Bed1.0%7Den.pdf	ISO/IEC TR14516	Source of information on updates to IT security mechanisms and techniques from ISO and IEC
www.w3c.org	World Wide Web Consortium	Source of updates on standards associated to web services and web service security
www.protege.stanford.edu	Protégé Ontology development tool from Carnegie Mellon University	Free tool for development of ontologies
www.oasis.org	Organization for the Advancement of Structured Information Standards – OASIS	Source of information on updates to the XACML and SAML standards that form part of the ABAC.

5.2 The Business Model

This Business model of the proposed framework summarizes policy level mechanisms for tackling the information security requirements for eCommerce transactions. And this has been motivated by the following factors:

1) An eCommerce transaction typically takes place across more than one organization. Therefore multiple organizational and security domains may be involved. That is handling of security must be at a level higher than just an individual organizational level.
2) The framework must take into consideration of the existing legislation, and meanwhile be flexible enough to anticipate new laws or changes to existing legislation.
3) In many areas, implementation of international frameworks without adaptation has proved not to work, as developing countries need context-sensitive approaches [21].

The components of the business model consist of Organizational policies, Regional and National laws and regulations as well as International standards. Every component will have elements that apply to some or all of the information security requirements. The Business model is implemented by top level management in an organization. Consider the Figure 11 Below

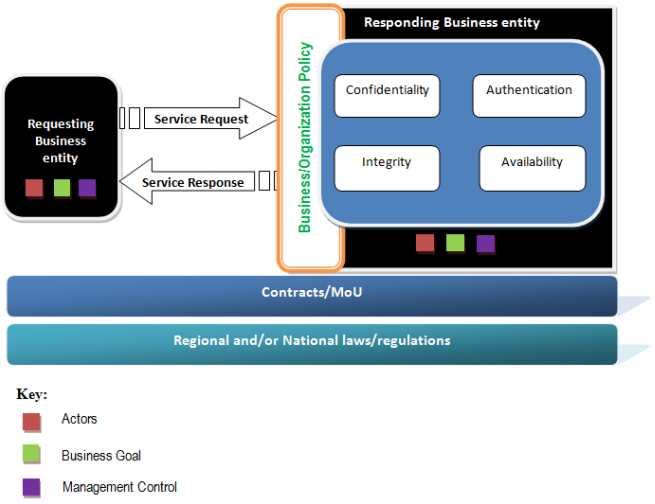

Figure 14: Business Model

Supportive Resource for implementing the Business Model

In implementation of the business model the resources shown in Table 4 here under may be found helpful in getting updates on mechanisms such as international standards and national legislation.

Table 4: Supportive Resource for implementing the Business Model

Source	Resource	Reason
www.iso.org	ISO/ IEC 27000 series of security standards.	Source of security standards issued by ISO and IEC
www.parliament.go.tz www.parliament.go.ke	Legislation of the United Republic of Tanzania, Kenya	Sources of national legislation in Tanzania and Kenya
www.nist.org	National Institute of Standards and Technology	Information security standards and guidelines issued by the United States Government

5.3 Operational Model

The Operational Model of the proposed framework summarizes organizational plans and practices that an individual business organization can use to tackle the information security requirements. And this has been motivated by the following factors:

1) This proposed framework is cognizant of this practice, however it is necessary for Businesses organizations to map their initiatives onto policies or legislation as and when they come into effect. This is by matching organizational plans to the required business components that tackle a specific information security requirement.
2) Technical mechanisms for tackling information security should be backed by organizational practices and plans to allow for holistic addressing of information security.

Its components include organizational programs and plans, common terminology for eCommerce transactions and certificate authority agreements. This model is implemented by operational departments in individual businesses organization and some components are implemented across Businesses as shown here under.

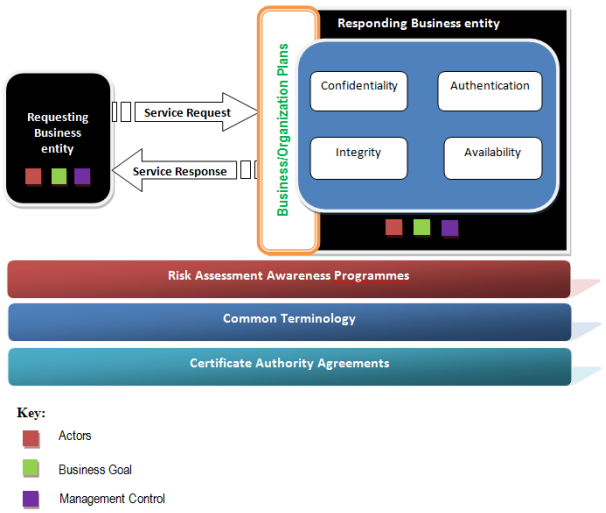

Figure 15: Operational Model

This Model is implemented by operational or business units within organization.

Table 5: Supportive Resource for implementing the Operational Model

Source	Resource	Reason
www.isaca.org	Information Systems Audit and Control Association	Source of information on standards and white papers related to audit and risk assessment of information systems
www.cert.org/octave	CERT Program, Software Engineering Institute – Carnegie-Mellon University	Source of information on the OCTAVE Risk assessment methodology

5.4 Process Model

The previous three models proposed here above represent distinct actors with diverse roles within each Business. For the business organization to move towards holistic addressing of information security requirements, there has to be inserting to each of three models. This process model that is proposed in this section allows a business to identify what technical, operational or business mechanisms are in place and use them appropriately in an eCommerce transaction.

This has been motivated by the need to tackle the three relative factors discovered which are:

1) Resource limitation: These include financial constraints due to limited budgets allocated and inadequate ICT skills;
2) Regulatory or Legal constraints: such as, lack of sufficient legislation and national policy frameworks associated to information security in eCommerce.
3) Organization Culture constraints: such as unstructured or uncoordinated national government initiatives related to eCommerce.

The tackling of these factors is completed by designing the process model such that it exploits a 'plug and play' approach, that each Business organization applies the mechanisms that it can in a particular model, and insert those onto the corresponding models. Where cultural constraints or resource exist, the implementation still continues, and a maturity model is proposed to guarantee continual improvement in the businesses efforts to comprehensively meet information security requirements.

This model is consists of two levels which are formally presented using the ebXML[5]. ebXML Business Process Specification Schema (BPSS) was developed specifically for e-business. This process model is relevant at two levels. The first level is an eCommerce transaction between two businesses entities, and the second level represents any two or more actors in a Business who is putting in place mechanisms to meet up the information security requirements.

At a high level, a Process Model consists of a set of roles collaborating through a set of choreographed Business Transactions by exchanging Business Documents.

These basic semantics of a Business Collaboration are illustrated in Figure 11. Here two or more business partners participating in the Business Collaboration through roles. The roles often exchange messages in the context of Business Transactions. Each Business Transaction has one or two predefined Business Document Flows. One or more Business Signals MAY additionally be exchanged as part of a Business Transaction to ensure state alignment of both parties. The Business Collaboration is defined as choreography of Business Transactions performed relative to each other.

Business Collaborations

A Business Collaboration in a Process Model is a set of Business Activities executing Business Transactions among collaborating parties or business partners. Each business partner plays one or more abstract partner roles in the Business Collaboration. The status of the Business Collaboration is logical among the parties interacting in a One-to-One rather than a controlled environment. The virtual status of the Business Collaboration lies with the involved partners. One-to-One collaboration may involve business partners and distributed collaborating parties.

[5] ebXML (Electronic Business XML) is a project to use the Extensible Markup Language (XML) to standardize the secure exchange of business data.

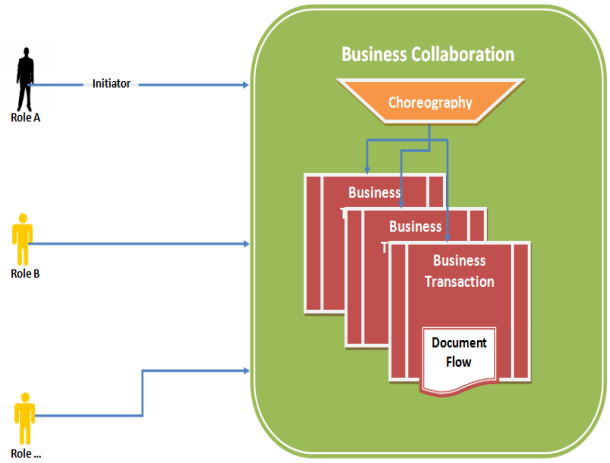

Figure 16: Illustration of Process Model

Business Transactions

Here a Business Transaction in Process Model represents an atomic unit of work that may be connected with a trading arrangement among two business partners. The scale of the ebXML technical specification is to articulate more fully the Business Transactions, rather than primarily focusing on their relationship to trading arrangements among business partners.

This Transaction will often either thrive or fail. If it thrives it may be designated as legally binding among the two partners, or else govern their collaborative activity. If fails, it is null and void, and every partner must renounce any mutual claim established by the transaction.

Business Document Flows

This is realized as Business Document Flows among the Requesting and Responding parties performing roles. There is often a logical Requesting Business Document, and optionally a logical Responding Business Document, depending on the desired Business Transaction configuration: The actual Business Document definition is achieved by using the ebXML and/or by some methodology contracted to by the business partners that have roles in the service collaboration.

Choreography

On this model approach is characterized definitively by the Business Transaction Choreography. The Business Transaction choreography describes the ordering and transitions among service transactions or sub collaborations surrounded by a binary collaboration. Thus the choreography in this framework describes how insertion is across different technical, operational and business mechanisms are achieved.

ebXML Implementation

This technical specification must be used wherever software components are being specified to execute a role in an ebXML Business Collaboration. Particularly, this technical specification is projected to provide the business process and document specification for the formation of ebXML trading partner Agreements and Collaboration Protocol Profiles.

However, this technical specification might be used to specify any eCommerce or shared collaboration. It can also be used for non-commerce collaborations, for example in defining transactional collaborations among non-profit organizations or between applications, within the enterprise.

5.5 Maturity Model

The principle idea of a maturity model is to recommend a roadmap through which an entity can continually progress towards a set goal. This maturity model is intended at helping Businesses continually progress information security practices through the secure framework with the aim of achieving a sustainable information security framework for eCommerce transactions.

Maturity model has the following levels of maturity as illustrated here under:-

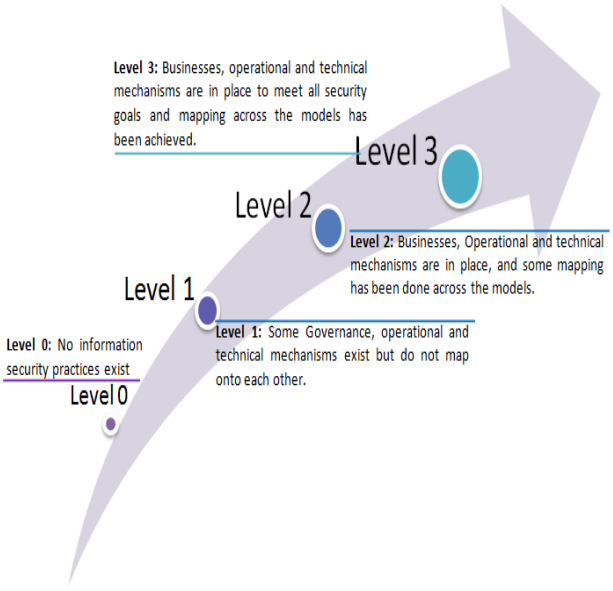

Figure 17: Illustration of Levels in a Maturity Model

6. CONCLUSION AND DISCUSSION

In order to design an information security requirements framework for eCommerce transactions, it is necessary to come up with a design that convenes the information security requirements. The discoveries on mechanisms and perspectives that are presented in this study are used to develop blueprint artifacts that will form elements of the framework. Blueprint artifacts might be builds, methods, instantiations or models. In addition to developing blueprint artifacts, the blueprint processes bases on a proposal by Carlson to include an object blueprint, realization design and a process design in an information systems research initiative purposely to come up with a thriving problem solution. An object blueprint is the intervention necessary to solve the problem. The realization blueprint is guidance on how to implement the object design, and the process design is the techniques and methods to implement the object blueprint.

The primary three models include mechanisms or components that tackle the meeting of information security requirements declared in this study. For every model, guidelines on implementation of the model are developed and helpful resources to be deployed by the implementing Businesses are included. This forms the attainable design. The Process Model fine points a process cycle through which businesses can implement the Technical, Operational and Business Model whereas the Maturity Model summarizes how the businesses

can gradually progress on their aptitude to meet the Information Security requirements over time.

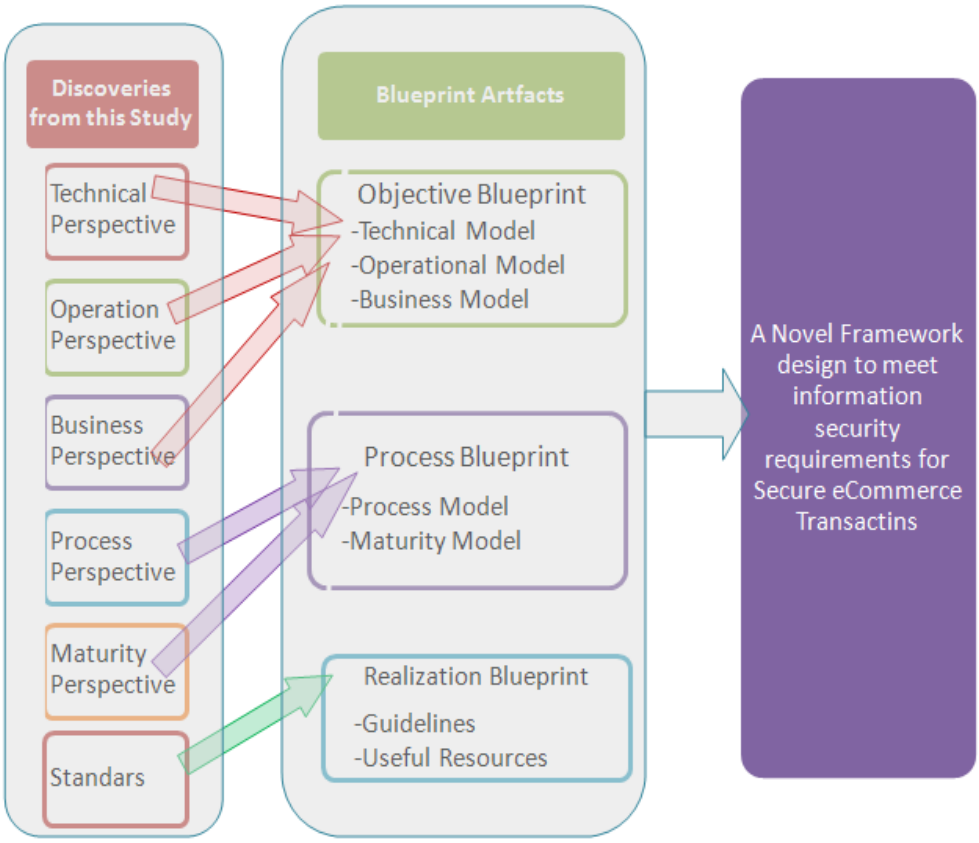

Figure 18: The design process of the resultant framework

7. REFERENCES

[1] Kenneth Mlelwa (2011) "E-Commerce Awareness and Its Impact on the Small Scale Tourism", research Report

[2] Weik, M. (2001). Computer Science and Communications Dictionary. Springer.

[3] NIST. (2006). Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology, Computer Security Division.

[4] ISO/IEC. (2005b). ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management. Geneva: International Organization for Standardization.

[5] OECD. (2002). OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Retrieved June 13th, 2016, from Organisation for Economic Cooperation and Development: http://www.oecd.org/dataoecd/16/22/15582260.pdf

[6] Talleur, T. (2000) E-Commerce and Cybercrime. eBusiness Forum

[7] Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46, 267-270.

[8] Hayat, Z., Reeve, J., & Boutle, C. (2007). Ubiquitous security for ubiquitous computing. Information Security Technical Report, 12(3), 172-178.

[9] NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

[10] CEN. (2007). Network and Information Security Standards Report. Final Version, ICT Standards Board.

[11] OASIS. (2010b). OASIS Standards and Other Approved Work. Retrieved June 15, 2016, from OASIS: http://www.oasis-open.org/specs/

[12] International Organization for Standardization. Information Technology; Security Techniques; Information Security Management Guidelines for Telecommunications Organizations Based on ISO: Technologies de L'ìnformation: Techniques de Sécurité: Lignes Directrices Pour Les Organismes de Télécommunications Sur la Base de L'ISO/CEI 27002. International Organization for Standardization, 2009

[13] Dardenne, A., van Lamsweerde, A., & Fickas, S. (1993). "Goal-Directed Requirements Acquisition," Science of Computer Programming (Elsevier), vol. 20 no. 1-2, pp. 3-50.

[14] Jackson, M. (2001). Problem Frames: Addison Wesley.

[15] Allen, J. H. (2001). "CERT System and Network Security Practices," in Proceedings of the Fifth National Colloquium for Information Systems Security Education

(NCISSE'01). George Mason University, Fairfax, VA, USA, 22-24 May.

[16] Published as Landwehr, C.E., and J.M. Carroll, "Hardware Requirements for Secure Computer Systems: A Framework," Proc. 1984 IEEE Symposium on Security and Privacy, Oakland, CA, April 23-26, 1984.

[17] Pfleeger, C. P. & Pfleeger, S. L. (2002). Security in Computing: Prentice Hall.

[18] NIST (1995). "An Introduction to Computer Security: The NIST Handbook," National Institute of Standards and Technology (NIST), Special Pub SP 800-12, Oct.

[19] "ABAC (Attribute Based Access Control), jerichosystems.com". Retrieved 2016-07-11.

[20] W3C. (2004, February 11). Web Services Glossary. Retrieved July 15, 2016, from W3C Working Group: http://www.w3.org/TR/ws-gloss/

[21] Dada, D. (2006). The Failure of e-Government in Developing Countries: A Literature Review. The Electronic Journal of E-Government in Developing Countries, 26.