A REFORMED INFORMATION SECURITY MANAGEMENT SYSTEM (R-ISMS)

Amarachi, A.A[1], Ajaegbu, C[2](PhD), Idowu, S.A[3] (PhD) and Ajaegbu, Oguchi O[4] (PhD).

[1]Researcher, Computer Science Dept, Babcock University, Ogun State, Nigeria
[2]Lecturer, Computer Science Dept, Babcock University, Ogun State, Nigeria
[3]Lecturer, Computer Science Dept, Babcock University, Ogun State, Nigeria
[4]Lecturer, Mass Communication Dept, Babcock University, Nigeria

---***---

***Abstract* - An Information Security Management System (ISMS) specifies the instruments and methods that an administration/management level of an institution uses to comprehensibly manage the tasks and activities aimed at achieving information security. ISMS evolved as a systematic and structured approach to managing information following advances in IT infrastructure, services and applications so that they remain secure. While there are various implemented ISMS frameworks, researchers continually try to emphasize and increase human participation in ensuring information security. The aim of this research study is to develop an algorithm-based model to facilitate effective ISMS services for organizations.**

This algorithm-based ISMS model employed Information Technology General Controls (ITGC) technique as an expansion of the vistas of known ISMS frameworks, to improve information security control in organizations. The purpose of refinement is to make the frameworks more easily understood, implemented, and measured in organizations by stakeholders.

Microsoft Office Visio 2010 software was used in designing the reformed model.

Bactracking and Branch-and-bound algorithms were used in developing the model. The model utilises the above named methods to address the problem of inadequate management systems for information security.

The results of this study showed that, with the level of usability, International Organization for Standardization (ISO) standards are more easily implemented and well recognized by stakeholders (top management, staff, suppliers, customers/clients, regulators) unlike the other security frameworks.

In conclusion, this study showed that R-ISMS is a customized algorithm model that assists organizations to enhance the ability in monitoring the performance of their activities, policies and procedures.

Keywords: Information Security Management Systems (ISMSs), Reformed ISMS, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Backtracking / Branch-and-bound algorithms.

1. INTRODUCTİON

As organizations become increasingly dependent on information systems (IS) for strategic advantage and operations, the issue of information systems security also becomes increasingly important. In the interconnected electronic business environment of today, security concerns are paramount (Kankanhalli et al., 2006). Management must invest in IS security to prevent abuses that can lead to competitive disadvantage.

The need arises for every organization, small or large, to possess ISMS in order to detect, manage and protect the valuable resources such as hardware, software and skilled people. The components (hardware, software, processes, policies, people) are required to be linked into a system which should be implemented carefully to tackle the existing and newer security threats. Such a system is called *Information Security Management System (ISMS)*, the outcome of one of the most strategic corporate decisions and foundation of information security in an organization. The process of ISMS is illustrated in Figure 1:

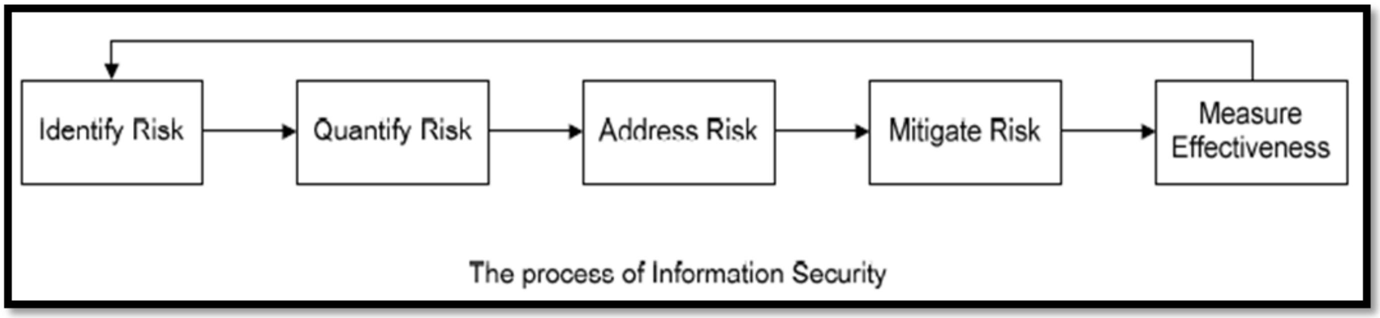


Figure 1: The Process of Information Security
Source: Ramakrishnan, P. (2012). "CISSP: Information Security Management Systems".

2. Chronological Developement of ISMS

2.1 The Plan-Do-Check-Act (PDCA) Cycle

The concept of the PDCA Cycle was originally developed by Walter Shewhart, the pioneering statistician who developed statistical process control in the Bell Laboratories in the US during the 1930s. It is often referred to as 'the Shewhart Cycle'. It was taken up and promoted very effectively from the 1950s on by the famous Quality Management authority, Edwards Deming, and is consequently known by many as "the Deming Wheel". The current process based approach to management systems is derived from the work of Edwards Deming and the world of Total Quality Management (TQM).

His holistic and process based approach to the manufacturing sector was initially ignored, and eventually embraced after the rapid rise in quality of Japanese products in the 1960s. Although initially viewed as relevant only to a production line environment, the concepts have since been successfully applied to many other environments. The Deming Wheel is illustrated in Figure 2.

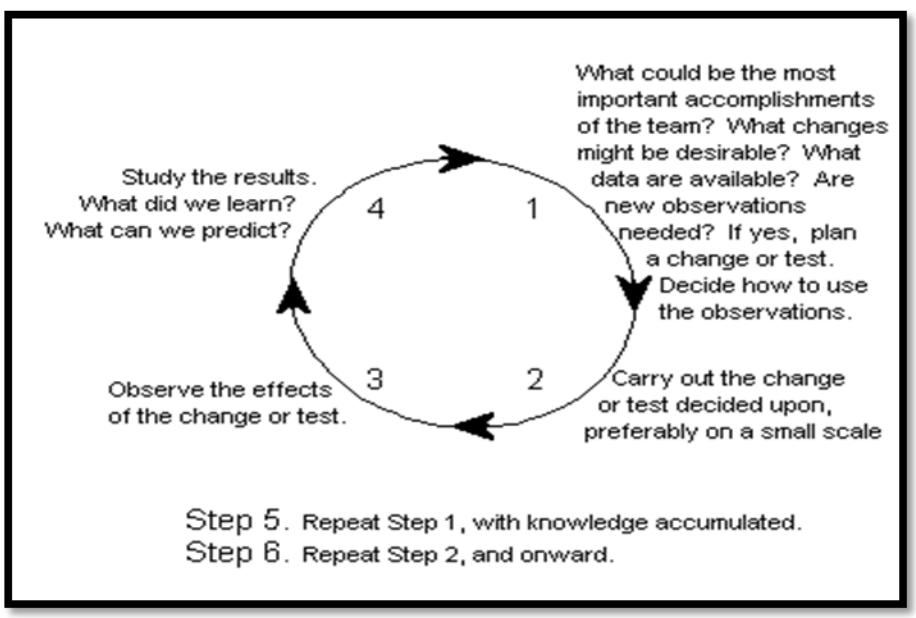


Figure 2: Deming Wheel, 1951
*Source:*Moen, R. & Norman, C. (2006). Evolution of the PDCA Cycle.

The basic steps of the Deming wheel are: (1) Design the product (with appropriate tests) (2) Make it; test it in the production line and in the laboratory. (3) Put it on the market (4) Test it in service, through market research, find out what the user thinks of it, and why the non-user has not bought it (5) Re-design the product, in the light of consumer reactions to quality and price.Then, reiterate the cycle.

This four step PDCA cycle which is essential for problem solving, includes planning (definition of a problem and a hypothesis about possible causes and solutions), doing (implementing), checking (evaluating the results), and action (back to plan if the results are unsatisfactory or standardization if the results are satisfactory). The PDCA cycle, illustrated in Figure 3, emphasized the prevention of error recurrence by establishing standards and the ongoing modification of those standards. Even before the PDCA cycle is employed, it is essential that the current standards be stabilized. The process of stabilization is often called the SDCA (standardize-do-check-action) cycle. Ishikawa (1985) stated: “If standards and regulations are not revised in six months, it is proof that no one is seriously using them.”

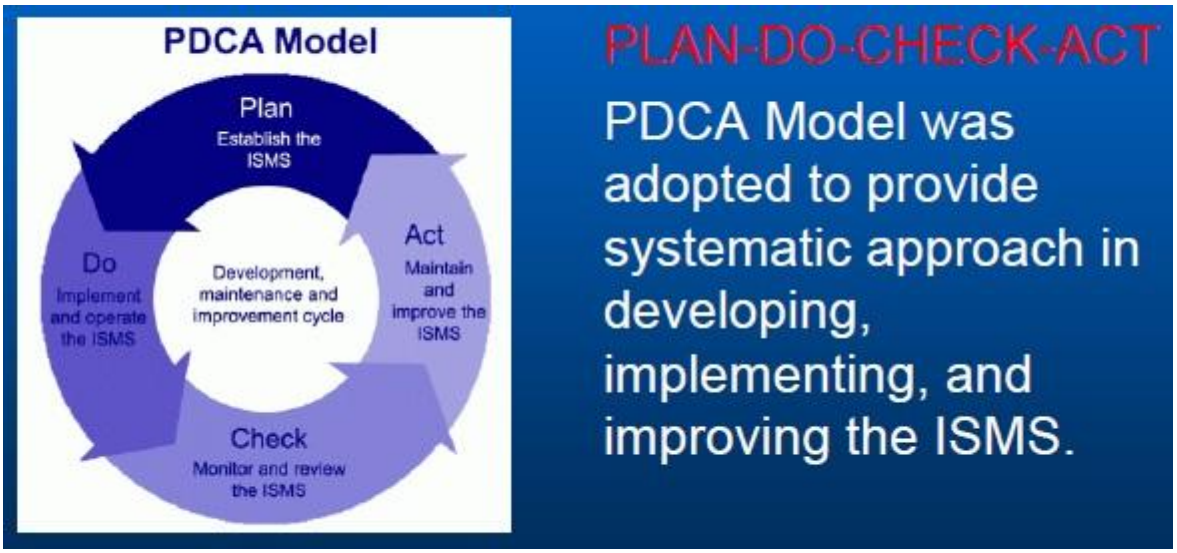


Figure 3: The PDCA Cycle
Source: Ramasamy, V. (2007). CISSP: Challenges of Information security management Systems.

Today’s information systems are complex collections of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. Information needs to be available, accurate and up-to-date to enable an organization make good business decisions. While various ISMS frameworks have been implemented and adopted by organizations, the focus has been more on the use of technology as a means of securing information systems. However, information security needs to become an organisation-wide and strategic issue, taking it out of the IT domain and aligning it with the corporate governance approach. Furthermore, an algorithm-based ISMS model demonstrating Information Technology General Controls (ITGC) concepts, is proposed with a more human-centred approach, in order to achieve a more efficient guide to information security management.

3. RELATED WORKS

Although organizations build unique systems, the management systems haveseveral common elements, and are still based around the Plan Do Check Act (PDCA) improvement cycle which is also concerned with famous Edwards Deming’s work.

Peltier (2002) provided key qualitative insights with a systems approach toward the humanistic side of information security. The research firmly presents two realms of information security: one lies in the humanistic communication of individuals and the other in information transactions over the computer (virtual). Peltier urges that an effective information security program cannot be implemented without the implementation of an employee awareness and training program that addresses the policy, procedures, and tools, so that each individual may understand and utilize.

Pattinson (2003) has written a paper to thoroughly investigate the pith of ISMS. He notes thus, "by using an ISMS an organization can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs". If they draw from a standardized ISMS framework they can be sure that they are drawing from the experience of many others and that the system has been reviewed and reflects best practices. Such a framework is a tried and tested tool that helps management ensure that security-resource is spent on the most effective areas for the business (Pattinson, 2003).

Carlson (2008) characterizes information security management systems as "coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information". He notes the concept of ISMS thus: "ISMS is an example of applying the management system conceptual model to the discipline of Information Security". Unique attributes of this instance of a management system include:

a. Risk management applied to information and based upon metrics of confidentiality, integrity, and availability
b. Total Quality Management (TQM) applied to information security processes and based upon metrics of efficiency and effectiveness.
c. A monitoring and reporting model based upon abstraction layers that filter and aggregate operational details for management presentation.
d. A structured approach towards integrating people, process, and technology to furnish enterprise information security services.
e. An extensible framework from which to manage information security compliance.

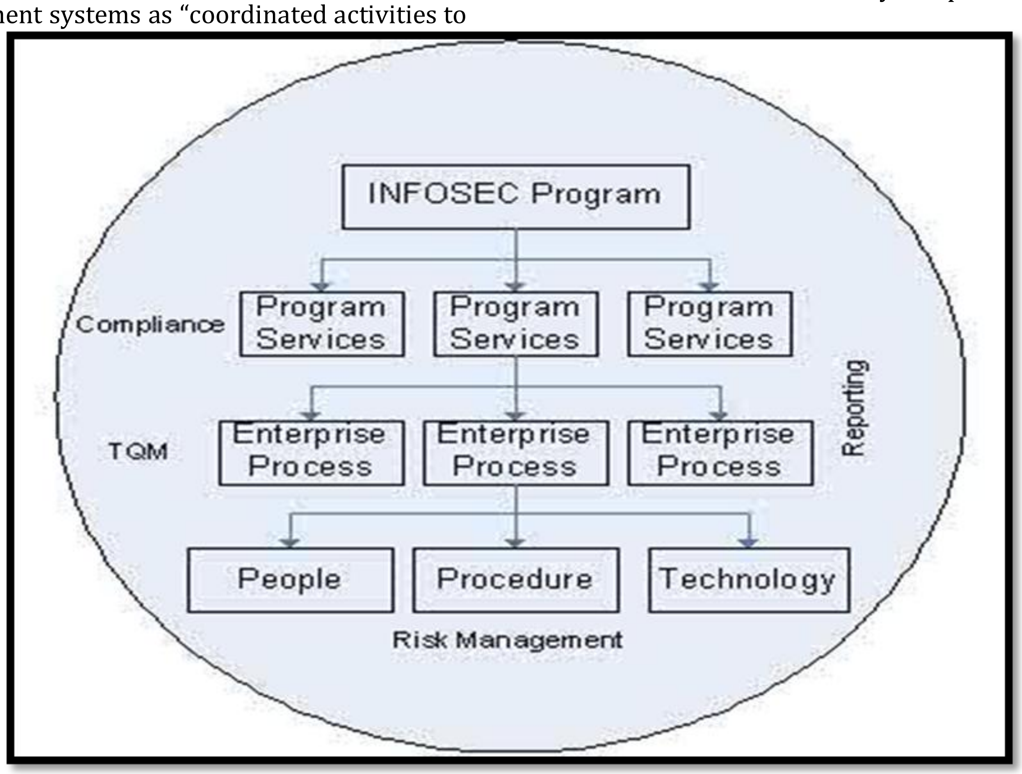


Figure 4*:* The Concept of ISMS
Source: Carlson, T. (2008). Understanding Information Security Management Systems. New York: Auerbach Publications.

ENISA (2010) notes that the chief target of Information Security Management is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, Information Security Management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e. availability of services, preservation of data confidentiality and integrity etc.). The framework of ISMS is illustrated in *Figure 5*.

The ENISA agency further explains that small businesses with limited information systems infrastructure, whose operation do not demand handling, storage and processing of personal or confidential data, usually face minor risks or risks with lower likelihood or impact. These organizations are more likely not to maintain independent ISMS and usually deal with information security risks ad-hoc or as part of a wider Risk Management process. Larger businesses and organizations such as banks and financial institutions, telecommunication operators, hospital and health institutes and public or governmental bodies have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmostattention and priority to information security risks.

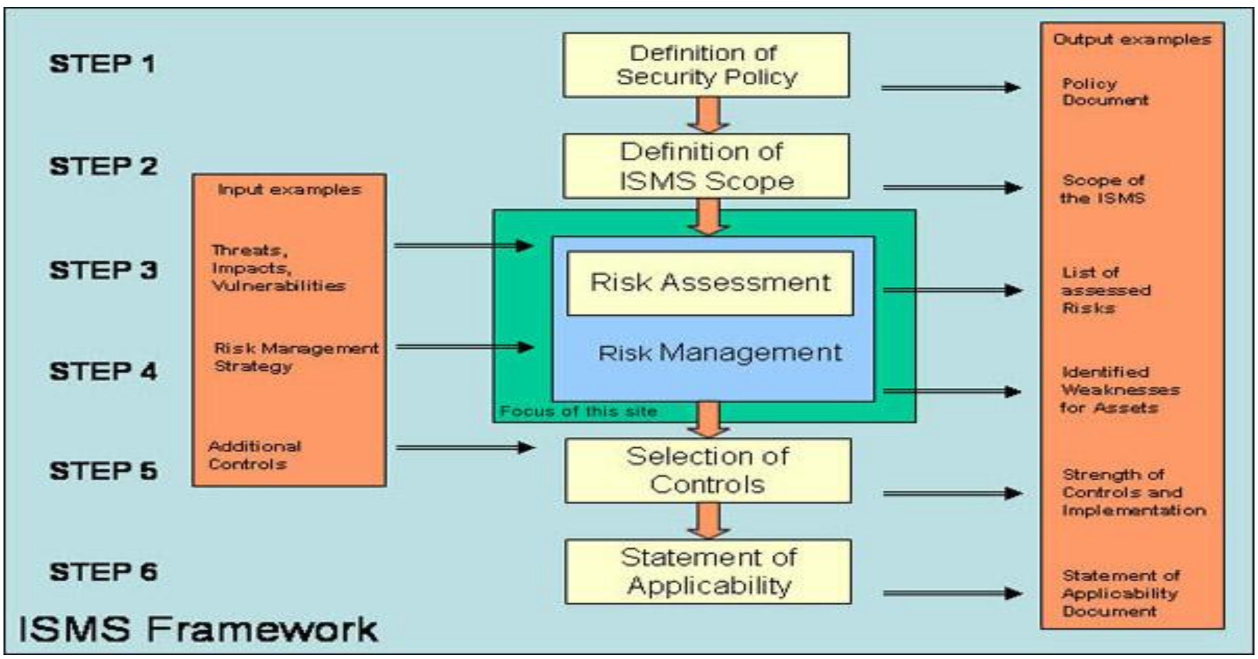


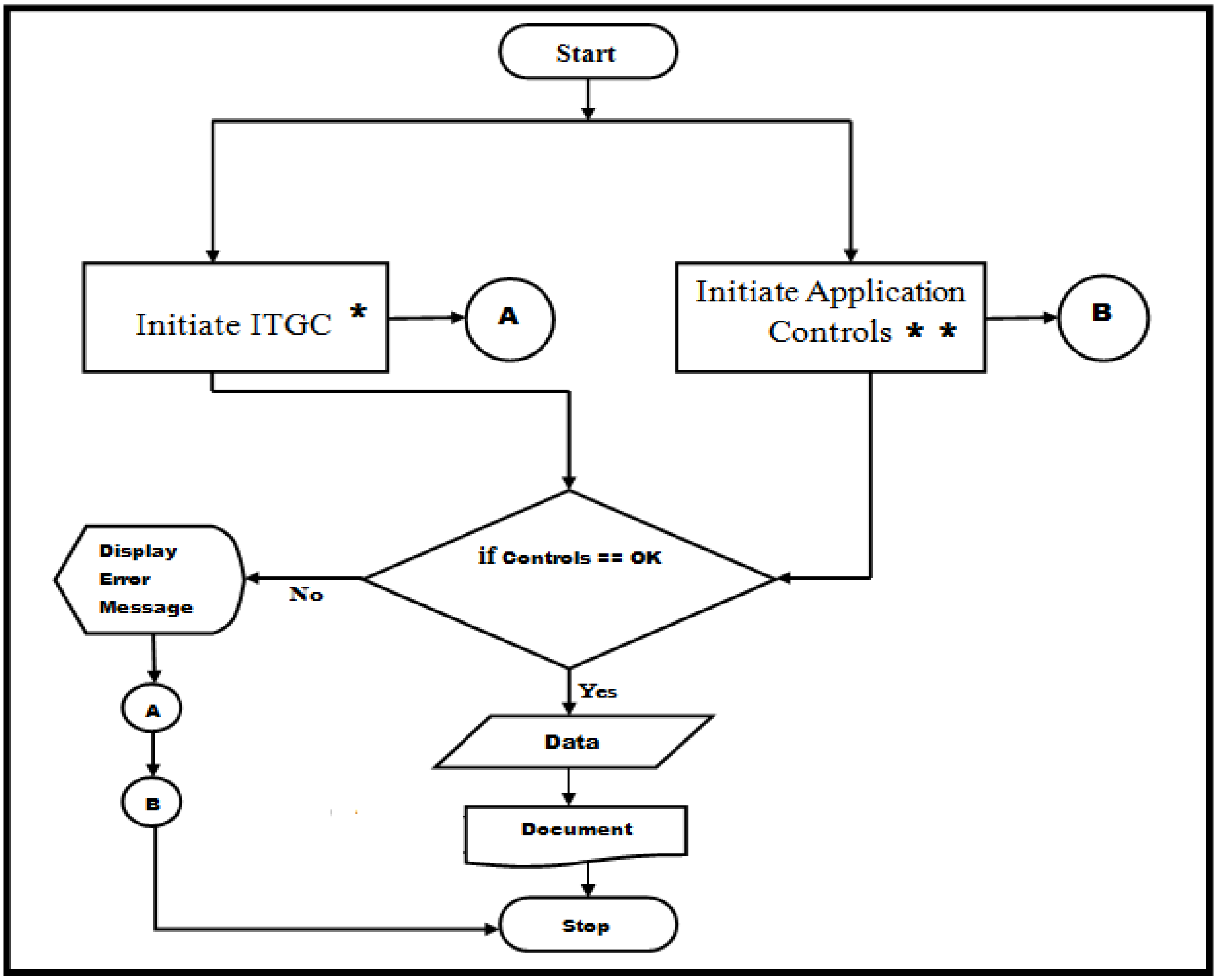
***Figure 5**:* ISMS Framework
Source: European Network and Information Security Agency (ENISA). (2010). ISMS Framework.

4. METHODOLOGY

A survey of business/IT professionals was conducted to ascertain the awareness of business/IT experts about the use of ISMS in securing their organization's information systems.the information gathered was used in the development of the reformed model using Microsoft Office Visio 2010 software along with bactracking and branch-and-bound algorithms.

5. RESULT

After analyzing some of the available widely used ISMS frameworks, an algorithm-based model that adequately provides reasonable assurance and support for the IT applications and business processes was proposed. Name the "R-ISMS", it allows some benefits of ITGC (such as improving IS performance in terms of improving the security, reliability, and integrity of data, facilitating the change management process, and lowering the risk of fraud).



Flowchart Illustration of R-ISMS
Figure 6: IT Technology Module

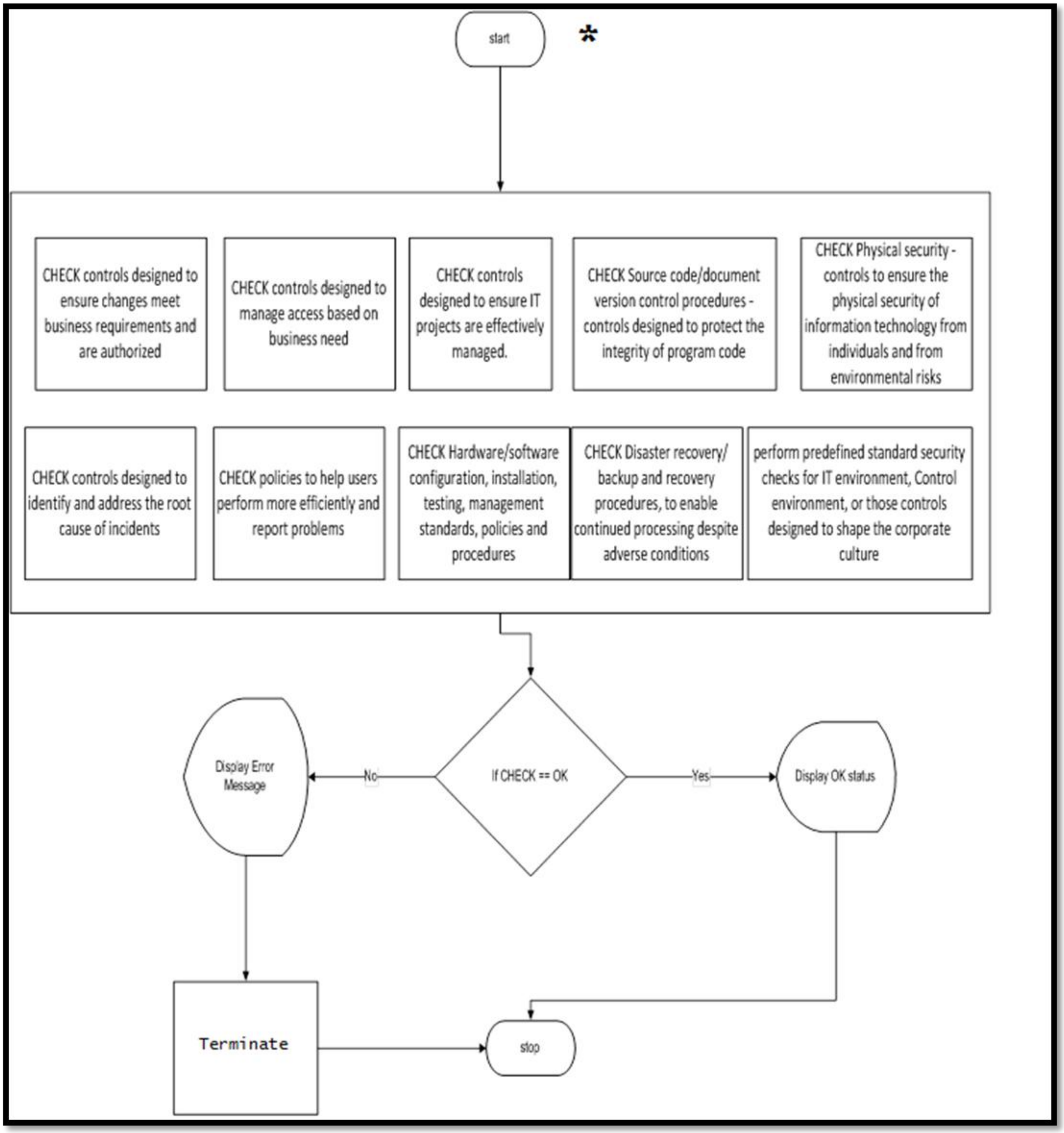


Figure 7: ITGC Module

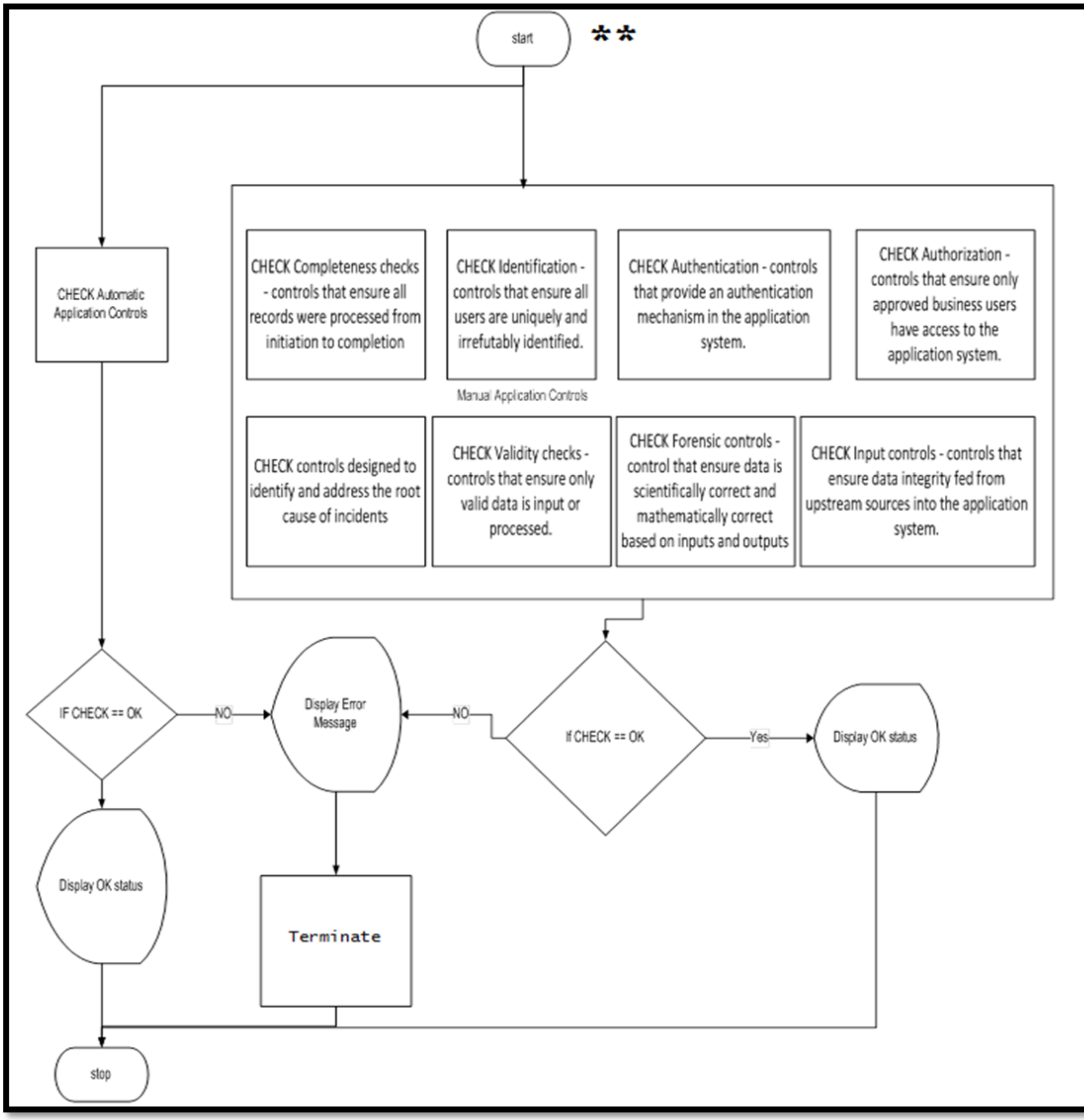


Figure 8: Application Controls Module

5.1Discussion of R-ISMS Process

The framework captures general computer controls in an IT environment. These controls relate to the IT environment within which computer-based application systems are developed, maintained and operated. They are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. The main process of the R-ISMS has been categorized into five main components as enumerated below:

a. *Hardware controls*: Provide reasonable assurance that data are not altered or modified as they are transmitted within the system.
b. *Program development*: Provide reasonable assurance that:
   i. acquisition or development of programs and software is properly authorized, conducted in accordance with entity policies, and supports the entity's financial reporting requirements;
   ii. appropriate users participate in the software acquisition or program development process;
   iii. programs and software are tested and validated prior to being placed into operation; and
   iv. all software and programs have appropriate documentation.
c. *Program changes*: Provide reasonable assurance that modifications to existing programs:
   i. are properly authorized, conducted in accordance with entity policies, and support the entity's financial reporting requirements;
   ii. involve appropriate users in the program modification process;
   iii. are tested and validated prior to being placed into operation; and,
   iv. have been appropriately documented.
d. *Computer operations*: Provide reasonable assurance that the processing of transactions through the computerized information system is in accordance with the entity's objectives and actions are taken to facilitate the backup and recovery of important data when the need arises.
e. *Access to programs and data*: Provide reasonable assurance that access to programs and data is only granted to authorized users.

5.2Benchmarking R-ISMS with ISO 27001

As previously determined, the ISO 27001 standard is the framework that rates above all others based on the 11ECs controls. With 18,500 international standards and a circulation/usability in163 national-member industries, it easily transcends the profiles of the other five widely used ISMS frameworks. However, over the years, its standards and the range of issues it covers have evolved. This evolution of issues beyond the scope of Information Security (the purview of ISO 27001) into aspects related to IT Governance, Information Security, and Service Management necessitates the conception and formulation of new and improved standards that will efficiently and robustly cater for issues under this expanded scope. R-ISMS nonetheless surpass ISO 27001 in the benchmarks that are relevant to the standards as aforementioned. Incorporating the scope of COBIT (IT Governance), BS 7799 (Information Security), and ITIL (Service Management) - all of which cut across all other standard organizations like the PCIDSS and COSO, R-ISMS proves itself a more robust and encompassing standard that improves upon what ISO 27001 offers. It is in this benchmarking that ISO 27001 falls behind R-ISMS.

Table - 1: Profile of ISO 27001 and R-ISMS

Features	ISO 27001 SERIES	R-ISMS
Profile of Standards	*is an information security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is the first international standard for management of information security that also allows certification. ISO is a* ***nongovernmental organization*** *that forms a bridge between the public and private sectors. Many of its member institutes are part of the governmental structure of their countries, or are mandated by their government.*	*Reformed Information Security Management System (R-ISMS) is a customized algorithm model created in 2012 by the researcher of this study that assists organizations to enhance the ability in monitoring the performance of their activities, policies and procedures. It shows Information Technology General Controls (ITGC) concepts which include controls over the Information Technology (IT) environment, computer operations, access to programs and data, program development and program changes.*
Initiated By	*Delegates from 25 countries*	*Researcher of this study*
Launched On	*Feb 23, 1947*	*In view*
Standards and Components	*18,500 international standards*	*5 main components*
Certificate Name	*ISO 27001series*	*In view*
Scope	*Information security*	*Information security, Service management, Corporate and IT Governance*
Usability/Circulation	*163 national members out of the 203 total countries in the world*	*In view*
Evaluation Method	*Follow each certification evaluation procedure*	*Plan-Do-Check-Act cycle*

6. CONCLUSİON

The level of current ISMS in organizations assessed was determined to be insufficient. Establishment of adequate ISMS is necessary to ensure organization privacy and the safe use of business records for versatile purposes. Implementation of ITGC which meet international standards with a long-term and comprehensive perspective is of great essence.

The proposed new model "The Reformed ISMS Model" (R-ISMS) shows Information Technology General Controls (ITGC) concepts which include controls over the Information Technology (IT) environment, computer operations, access to programs and data, program development and program changes. In this manner, it demonstrates the IT control structure which helps ensure the reliability of data generated by IT systems and support the averment that systems operate as intended and that output is reliable. This new model highlights the benefits of ITGC such as improving IS performance in terms of improving the security, reliability, and integrity of data, facilitating the change management process, and lowering the risk of fraud. In addition to the aforesaid outstanding features, it can be said that a new awareness that can compare favorably with any of the ISO/IEC standards for information security, has been created.

REFERENCES

[1] Carlson, T. (2008). Understanding Information Security Management Systems. New York: Auerbach Publications.

[2] European Network and Information Security Agency (ENISA). (2010). ISMS Framework.Retrieved from http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework.

[3] Ishikawa, K. (1985). *What is Total Quality Control? The Japanese Way* (pp. 56-61). Translated by David J. Lu. NJ: Englewood Cliffs, Prentice-Hall, Inc.

[4] Kankanhalli A., Hock-Hai T., Bernard C.Y., Kwok-Kee W. (2006). An Integrative Study of Information Systems Security Effectiveness, (pp. 1-4). Institute of Southeast Asian Studies. Singapore.

[5] Moen, R. & Norman, C. (2006). Evolution of the PDCA Cycle. *Deming Wheel.* Retrieved fromhttp://deming.ces.clemson.edu/pub/den/deming_pdsa.htm.

[6] Pattinson, M. R. (2003). Americas Conference on Information Systems.

[7]7 Peltier, T. R. (2002). *Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management* (pp. 1-3), Boca Raton, FL: CRC Press.

[8] Ramakrishnan, P. (2012). CISSP: Information Security Management Systems. Retrieved from http://www.cccure.org/Documents/ISMS/isms.pdf.

[9] Ramasamy, V. (2011). CISSP: Challenges of Information security management Systems. Retrieved fromhttp://ebookbrowse.com/il-isms-implementation-sgsi-sp-v3-0-pdf-d120245019

APPENDIX . The R-ISMSALGORITHM (PSEUDOCODE)

```
10      START main procedure
20      GO
30      INITIATE IT Technology Control Module
40      G0
        10      INITIATE ITGC Module
                10      check environment (CE)
                        10      START CE
                        20      GO
                        30      PERFORM predefined standard security checks for IT environment, Control environment, or
those controls designed to shape the corporate culture
                        40      IF (40-10-10-30 === Completed)
                        50      RETURN controlled
                        60      ELSE RETURN ERROR INFORMATION
                        70      END
                20      IF (CE === controlled)
                30      GOTO 40-10-60
                40      ELSE re-initiate CE module /* Back tracking Algorithm paradigm Applied here */
                50      GOTO 40-10-10
                60      CHECK management Procedures (MP)
                        10      START MP
                        20      GO
                        30      CHECK controls designed to ensure changes meet business requirements and are authorized
                        40      IF (40-10-60-30 === Completed)
                        50      RETURN controlled
                        60      ELSE RETURN ERROR INFORMATION
                        70      END
                70      IF (MP === OK)
                80      GOTO 40-10-110
                90      ELSE re-initiate MP module
                100     GOTO 40-10-60
                110     CHECK Document Version Control Procedures (DVC)
                        10      START DVC
                        20      GO
                        30      CHECK Source code/document version control procedures - controls designed to protect the
integrity of program code
                        40      IF (40-10-110-30 === Completed)
                        50      RETURN controlled
                        60      ELSE RETURN ERROR INFORMATION
                        70      END
                120     IF (DVC === OK)
                130     GOTO 40-10-160
                140     ELSE reinitiate DVC
                150     GOT0 40-10-110
                160     CHECK Software Development Lifecycle Standards (LCS)
```

```
        10    START LCS
        20    GO
        30    CHECK controls designed to ensure IT projects are effectively managed.
        40    IF (40-10-160-30 === Completed)
        50    RETURN controlled
        60    ELSE RETURN ERROR INFORMATION
        70    END
170   IF (LCS === OK)
180   GOTO 40-10-210
190   ELSE re-initiate LCS  /* Back tracking Algorithm paradigm Applied here */
200   GOTO 40-10-160
210   CHECK Access Policy Standards and Procedures (APS)
        10    START APS
        20    GO
        30    CHECK controls designed to manage access based on business need.
        40    IF (40-10-210-30 === Completed)
        50    RETURN controlled
        60    ELSE RETURN ERROR INFORMATION
        70    END
220   IF (APS == OK)
230   GOTO 40-10-260
240   ELSE re-initiate APS /* Back tracking Algorithm paradigm Applied here */
250   GOTO 40-10-210
260   CHECK Incident/Problem Management Policy Procedure (MPP)
        10    START MPP
        20    GO
        30    CHECK controls designed to address operational processing errors.
        40    IF (40-10-260-30 === Completed)
        50    CHECK controls designed to identify and address the root cause of incidents.
        60    IF (40-10-260-50 === Completed)
        70    RETURN OK
        80    ELSE RETURN ERROR INFORMATION
        90    ELSE RETURN ERROR INFORMATION
        100   END
270   IF (MPP === OK)
280   GOTO 40-10-310
290   ELSE re-initiate MPP /* Back tracking Algorithm paradigm Applied here */
300   GOTO 40-10-260
310   CHECK Technical Support Policies and Procedures (TSP)
        10    START TSP
        20    GO
        30    CHECK policies to help users perform more efficiently and report problems.
        40    IF (40-10-310-30 === Completed)
        50    RETURN OK
        60    ELSE RETURN ERROR INFORMATION
        70    END
320   IF (TSP === OK)
```

```
        330     GOTO 40-10-360
        340     ELSE re-initiate TSP /* Back tracking Algorithm paradigm Applied here */
        350     GOTO 40-10-310
        360     CHECK Hardware/software config, installation, testing, mgt Policies and procedures HSP
                10      START HSP
                20      GO
                30      CHECK Hardware/software configuration, installation, testing, management standards, policies and procedures.
                40      IF (40-10-360-30 === Completed)
                50      RETURN OK
                60      ELSE RETURN ERROR INFORMATION
                70      END
        370     IF (HSP === OK)
        380     GOTO 40-10-410
        390     ELSE re-initiate HSP /* Back tracking Algorithm paradigm Applied here */
        400     GOTO 40-10-360
        410     CHECK Backup and Disaster Recovery Procedure (BRP)
                10      START BRP
                20      GO
                30      CHECK Disaster recovery/backup and recovery procedures, to enable continued processing despite adverse conditions.
                40      IF (40-10-410-30 === Completed)
                50      RETURN OK
                60      ELSE RETURN ERROR INFORMATION
                70      END
        420     IF (BRP === OK)
        430     GOTO 40-10-460
        440     ELSE re-initiate BRP /* Back tracking Algorithm paradigm Applied here */
        450     GOTO 40-10-410
        460     CHECK Physical Security Measures and Procedure (PSM)
                10      START PSM
                20      GO
                30      CHECK Physical security - controls to ensure the physical security of information technology from individuals and from environmental risks.
                40      IF (40-10-460-30 === Completed)
                50      RETURN OK
                60      ELSE RETURN ERROR INFORMATION
                70      END
        470     IF (PSM === OK)
        480     GOTO 40-10-510
        490     ELSE re-initiate PSM /* Back tracking Algorithm paradigm Applied here */
        500     GOTO 40-10-460
        510     END
    20  INITIATE Application Controls
        10      CHECK Automated Application Controls (AAC)
        20      IF (AAC=== OK)
        30      GOTO 40-20-50
```

```
        40      ELSE RETURN ERROR INFORMATION
        50      CHECK Manual Application Controls (MAC)
                10      START MAC
                20      GO
                30      START CHECKS
                        10      CHECK Completeness checks - controls that ensure all records were processed from initiation to completion
                        20      CHECK Validity checks - controls that ensure only valid data is input or processed.
                        30      CHECK Identification - controls that ensure all users are uniquely and irrefutably identified.
                        40      CHECK Authentication - controls that provide an authentication mechanism in the application system.
                        50      CHECK Authorization - controls that ensure only approved business users have access to the application system.
                        60      CHECK Input controls - controls that ensure data integrity fed from upstream sources into the application system.
                        70      CHECK Forensic controls - control that ensure data is scientifically correct and mathematically correct based on inputs and outputs
                40      END CHECKS
                50      IF (CHECKS === COMPLETE)
                60      RETURN OK
                70      ELSE RETURN ERROR INFORMATION
        60      IF (MAC == OK)
        70      GOTO 40-20-90
        80      ELSE RETURN ERROR INFORMATION
        90      END
   30   END
50 END
```