



UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

***Information Security Policy Framework for a
Manufacturing Firm***

BY

Mulievi, Amos Matayo
P56/P/7840/00

Supervisor

P. M. Theuri

June 2009

Submitted in partial fulfillment of the requirements of the Master of Science in
Information Systems

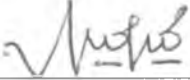
University of NAIROBI Library



0378890 8

DECLARATION

This project, as presented in this report, is my original work and has not been presented for any other University award.

Signature  _____

Date 04/08/2009

Amos Mulievi Matayo

P/56/P/7840/2000

This project has been submitted as part fulfillment of requirements for the Master of Science in Information Systems in the School of Computing and Informatics of the University of Nairobi with my approval as the University supervisor.

Signature  _____

Date 12.02.2009

P. M. Theuri

Lecturer SCI

Acknowledgement

In this world nothing is ever successfully accomplished without God giving us the ability to exploit our potential and showing us the people we can work with. In this regard, I humbly thank the Almighty God for giving me an opportunity and knowledge to accomplish this work. I also thank Him for showing me wonderful people who worked with me and ensured that this work is done to completion.

I wish to give my sincere gratitude to my supervisor, Mr. Peter M. Theuri for his guidance and invaluable support during my project work. Mr. Peter M. Theuri encouraged and pushed me even when I was overwhelmed with other demanding tasks at my place of work. I really appreciate your effort. Thank you for allowing me to access and reach you whenever need arose.

I cannot forget to acknowledge University of Nairobi, School of Computing and Informatics administration for their invaluable support during the project. I thank the academic staff for directing my project work. They analyzed, evaluated and criticized my work towards the desired result. School of Computing and Informatics Director, Professor Okello Odongo, on behalf of School of Computing and Informatics, kindly accept my sincere gratitude for offering me an opportunity to pursue a Master of Science in Information Systems (MSc. IS).

There is another group of special people who played a major part in this project, and at whatever cost I cannot forget to appreciate their effort. This group enabled me gather and present sufficient data for the research project. Information Security Policy Research respondents, data collectors and analysts may God bless you for sparing time to take part in this project.

Finally, I wish to thank my colleagues, family members and friends who always encouraged me in the entire process of the research work. I particularly appreciate my family's acceptance to deny them valuable time to work on the research project. I also sincerely acknowledge their financial and moral support in meeting the obligations of this MSc. IS program.

Dedication

Faith Muronji and Blessing Naliaka

ABSTRACT

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security is essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Information Security Policy is necessary to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Damages caused by events such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated. Information security should protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting in failures of availability, confidentiality, integrity, authenticity, and non-repudiation.

The objective of this research project was to define and develop an Information Security Policy Framework that is representative of the Kenyan manufacturing setup. The research involved evaluation of a number of Information Security models; to design a framework that can be adapted, customized and extended to address all areas of an organization. ISO/IEC 27002: 2005 Information Security model was used to ensure a more comprehensive security framework that is representative and complete.

This research project also identified gaps in the existing local and global standards by carrying out a detailed gap analysis to design a security policy framework that addresses all security requirements of an organization. It also recommended implementation and maintenance procedures that will ensure that security policy frameworks are complete, practical and effective.

Information Security Policy Framework for a Manufacturing Firm

TABLE OF CONTENTS

1 INTRODUCTION..... 11

1.1 INFORMATION SECURITY DEFINITION 11

1.2 RESEARCH PROBLEM 12

1.3 INFORMATION SECURITY PROJECT OBJECTIVE 14

1.4 PROJECT MOTIVATION/JUSTIFICATION..... 14

2 LITERATURE REVIEW 18

2.1 BUSINESS CONTINUITY MODELS..... 18

 2.1.1 *Virtual Business Continuity Maturity Model (Virtual Corporation) 18*

 2.1.2 *Public Available Specification 56 (PAS 56) BCM (Phil Carter)..... 22*

 2.1.3 *Business Continuity Models Conclusion..... 26*

2.2 RISK MANAGEMENT MODEL..... 27

 2.2.1 *360 Degree RISK Management Model (Infosys Technologies limited) 27*

 2.2.2 *Understanding RISK – Positive and Negative Implications..... 27*

 2.2.3 *Drivers of a Holistic Risk Management Model 28*

 2.2.4 *Constituents of the 360 Degree Risk Management Model 29*

 2.2.5 *Implementation Approach and Efficiency Index..... 29*

 2.2.6 *Processes and Tools to Effectively Identify Risks and Plan Risk Response 31*

 2.2.7 *Mechanisms to Exploit Opportunities in a Risk 34*

 2.2.8 *Knowledge Sharing Mechanisms to Enhance Competencies 35*

 2.2.9 *Benefits of the 360 Degree Risk Management Model..... 35*

 2.2.10 *Implementation Challenges and Solutions 36*

 2.2.11 *360 Degree Risk Management Model Conclusion..... 36*

2.3 ISO/IEC 27002:2005 INFORMATION SECURITY STANDARD 37

3 RESEARCH METHODOLOGY..... 44

3.1 RESEARCH METHODS USED 45

 3.1.1 *Questionnaires..... 45*

 3.1.2 *Electronic Mail and Internet Surveys 46*

3.2 SAMPLING PROCEDURES USED 47

Information Security Policy Framework for a Manufacturing Firm

4 RESEARCH FINDINGS AND DISCUSSIONS..... 49

4.1 POPULATION SAMPLE..... 49

4.2 RESEARCH DATA ANALYSIS 51

 4.2.1 *Bar Charts Showing Respective Frequency Responses 52*

 4.2.3 *Correlation Analysis..... 76*

4.3 CRITIC OF THE CURRENT INFORMATION SECURITY MODELS..... 84

5 INFORMATION SECURITY POLICY FRAMEWORK..... 86

5.1 FUNCTIONS AND CONTENT OF ESSENTIAL ELEMENTS OF A SECURITY PROGRAM 87

5.2 INFORMATION SECURITY POLICY IMPLEMENTATION 88

5.3 RECOMMENDED INFORMATION SECURITY POLICY MODEL..... 90

6 CONCLUSION AND RECOMMENDATIONS 93

7 REFERENCES AND BIBLIOGRAPHY 96

8 APPENDICES..... 97

 APPENDIX A 97

 APPENDIX B..... 107

9 GLOSSARY 115

List of Figures

Figure 2-1: Six Levels BCMM..... 19

Figure 2-2: PLAN-DO-CHECK-ACT (PDCA) cyclic model of ISO/IEC 27001..... 30

Figure 4-1: Bar chart of Approved Information Security Policy 53

Figure 4-2: Information Security communication to all employees 54

Figure 4-3: Security Policy management commitment..... 55

Figure 4-4: Risk assessment to determine impact of interruptions 56

Figure 4-5: Regular updates in organizational security policies and procedures..... 57

Figure 4-6: Specialist information security advice 58

Figure 4-7: Employees and third party users' reception of appropriate security training..... 58

Figure 4-9: Security risks from third party access and appropriate security controls 59

Figure 4-10: Information Security policy independent review for assurance 60

Figure 4-11: Plans to restore business operations within required time frame s 61

Figure 4-12: Policy to account for risks of working with mobile computing facilities 62

Figure 4-13: Risk assessment to determine the impact of interruptions 63

Figure 4-14: Regular checking for compliance with security implementation standards..... 64

Figure 4-15: Access to system audit tools such as software..... 65

Figure 4-16: Have an approved published information security policy..... 67

Figure 4-17: Security policy management commitment 68

Figure 4-18: Employees and third party users' reception of appropriate security training..... 69

Figure 4-19: Procedure to report security incidents 71

Figure 4-20: Maintenance of audit trails and logs relating to the incidents..... 72

Figure 4-21: Management committee to set direction and support 74

List of Tables

Table 4-1: Have an approved published information security policy 67

Table 4-2: Security policy management commitment 68

Table 4-3: Employees and third party users reception of appropriate security training 69

Table 4-4: Procedure to report security incidents 71

Table 4-5: Maintenance of audit trails and logs relating to the incidents 72

Table 4-6: Management committee to set direction and support 74

Table 4-7: Definition and documentation of business requirement for access controls 75

Table 4-8: Have an approved published information security policy 77

Table 4-9: Communicated as appropriate to all employees 78

Table 4-10: Specialist information security advice where appropriate 79

Table 4-11: Identification of security risks from third party access 80

Table 4-12: Effective operational controls established where necessary 81

Table 4-13: Management of information processing facilities by an external party 82

Table 4-14: Regular checking of information systems for compliance 83

1 INTRODUCTION

1.1 Information Security Definition

Information is an asset, like other important business assets. Information is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of the increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (ISO/IEC 27002:2005). Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security is essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should be appropriately protected. Information Security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information Security is achieved by implementing suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done with other business management processes.

Protection of information and communications technology resources that support the enterprise is critical to the functioning of an organization. Information assets are at risk from potential threats such as employee error, malicious or criminal action, system failure, and natural disasters. Such events could result in damage to or loss of information resources, corruption or loss of data

Information Security Policy Framework for a Manufacturing Firm

integrity, interruption of the activities of the organization, or compromise to confidentiality or privacy.

1.2 Research Problem

Statement of Problem

Widespread use of information and communication technology, complex networks and interconnectivity has increased incidences of frauds and cybercrimes. Rogue persons are ever attempting and/or cracking unsecure applications and intercepting private networks for varied interests like monetary benefits or malice. To avoid such incidences, it is mandatory that a company invests in secure information systems.

There are many scandals in both government and private sectors. The scandals may range from simple theft to complicated frauds that may involve loss of large amounts of revenue. Many organizations turn to information and forensic investigations to investigate such instances because of the ability to produce inbuilt and reliable audit trails. Such investigations can only be possible if we have secure and complete information. This therefore calls for a policy to secure company's information resources. A secure information infrastructure will assure the company of the much valued information resource.

The research problem statement:

“Development of an Information Security Policy Framework for a Kenyan Manufacturing Setup”

The strategy of coming up with a suitable Information Security Policy Framework was to conduct a research to evaluate information security implementations in a representative number of organizations in Kenya. The research mainly focused on manufacturing establishments,

Information Security Policy Framework for a Manufacturing Firm

however, a few organizations in other sectors were considered to determine whether the security model developed could be generalized or extended to incorporate such organizations.

A study of known and acknowledged Information Security models was also done, to establish how well they can be adapted, customized and implemented. ISO/IEC 27002: 2005 Information Security model was considered to ensure a comprehensive Information Security policy framework that is representative and complete. Business Continuity Plans (BCP) and Risk Management models were also studied to give a guideline on the development of a model that would address these important information security components.

In the evaluation of locally developed information security frameworks and universally accepted security models, there are gaps which should be addressed. Most security models are quite general and therefore need to be localized to provide an effective solution to a particular setup. In other cases these models are supposed to serve as a guide for organizations to use them as a base of developing suitable security frameworks.

Developing a systematic, analytical, and continuous risk management process is critical to any successful security program. For the program to be effective, it must be implemented as a formal process. Determining the correct or appropriate level of security is dependent on the potential risks that an organization faces. These risks can be unique to each organization and should not be over generalized by applying risk factors across industries or regions.

Furthermore, having an adequate Information Security program is made more challenging by organizational, technological and business/operational change. Risk management should be a continuous and dynamic process to ensure that changing threats and vulnerabilities are addressed in a timely manner.

*Information Security Policy Framework for a Manufacturing Firm***1.3 Information Security Project Objective**

The main objective of this project was to develop a suitable Information Security Policy Framework for a Kenyan Manufacturing setup, to protect the organization's business information resources and other external party's information within its custody for safekeeping by safeguarding its confidentiality, integrity and availability resulting in business continuity, competitive edge, increased profitability, legal compliance, and commercial image. However, it is designed such that it can be easily adapted, customized and extended to address all areas of the organization.

One of the key factors enabling growth and maturity of the global business environment are information technology systems. Organizations depend upon these systems for day-to-day operations. However, risks are increasing; making security breaches a common occurrence. Not only have the number and economic significance of these breaches increased, many are going undetected.

In a manufacturing setup as opposed to other organizations like service or marketing businesses, Information Security is emphasized in the production processes as well as other areas like financial transactions and marketing. Production or manufacturing is the core business activity to determine the direction of the entire business enterprise.

To realize these objectives, a thorough analysis of implemented Information Security models was conducted to establish the most appropriate model for a Kenyan Manufacturing set up, and determine the possibility of extending it for other organizations.

1.4 Project Motivation/Justification

In today's interconnected global business environment, the importance of information is widely accepted, and information systems are truly pervasive throughout business and government

Information Security Policy Framework for a Manufacturing Firm

organizations. The growing dependence of most organizations on their Information Systems, coupled with risks, threats, benefits and opportunities IT carries, have made IT governance and related aspects of information security governance increasingly a critical facet of the overall organizational governance (ISO/IEC 27002:2005).

Boards and management alike need to ensure that IT is aligned with organizational strategies and that these strategies take proper advantage of IT opportunities. An important facet of IT governance is information security governance (IT Governance Institute). Information security governance provides assurance that information assets are given a level of protection commensurate with their value or with the risk their compromise poses to the organization. Therefore executive management should ensure that the definition of roles and responsibilities throughout the organization include information security.

Information security management is, to an increasing extent, a business issue and a legal requirement, and not only a technology issue. On the basis of identified and prioritized information resources that need protection, a security policy and baselines must be developed and implemented. Information security baselines represent the minimum acceptable security implemented to protect information resources. Baselines are normally set using commonly accepted, industrial wide standards, such as ISO/IEC 27002:2005, legal and regulatory requirements, and decisions by the business owners on what level of risk the organization is willing to accept.

Information security will ensure protection of valuable information assets against loss, operational discontinuity, misuse, unauthorized disclosure, inaccessibility or damage. In this context "valuable assets" are the information recorded on, processed by, stored in, shared by, or transmitted or retrieved from an electronic medium (ISACA, CISM Review Manual, 2009). The information must be protected against harm from threats that could result in business impact such as loss, inaccessibility, alteration, wrongful disclosure or unauthorized access. Threats include errors and omissions, fraud, accidents, and intentional damage.

Information Security Policy Framework for a Manufacturing Firm

Protection of information assets is ensured through a layered series of technological and non-technological safeguards, such as physical and environmental security measures, personnel security and employment measures, or authentication and identity management measures, deployment of intrusion detection and prevention systems, and the development and integration of supporting manual and automated procedures. These safeguards are necessary and should address threats and vulnerabilities in a balanced manner (ISO/IEC 27002:2005).

In a dynamic technological environment, security technology that is state-of-the-art today may be obsolete tomorrow. Security must keep pace with these changes. Business in the context of “global village” is highly dynamic and makes extreme demands from information systems. Therefore, it is imperative that the security strategy of an organization be dynamic to match the business demands. It must be considered an integral part of the system development life cycle process and be explicitly addressed during each phase of the life cycle. Security must be dealt with in a proactive and timely manner to be effective.

Information systems can generate many direct and indirect benefits, and at least as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the degree of protection applied (ISACA, CISM Review Manual, 2009). The gap is caused by internal and external factors including:

- a) Widespread use of technology
- b) Interconnectivity of systems
- c) Elimination of distance, time and space constraints
- d) Unevenness of technological change
- e) Devolution of management and control
- f) Social engineering
- g) Attractiveness of conducting unconventional electronic attacks against organizations
- h) External factors such as legislative, legal and regulatory requirements, or technological developments

Information Security Policy Framework for a Manufacturing Firm

These scenarios would imply that there are new risk areas that could have a significant impact on critical business operations such as: increasing requirement for availability, resilience and robustness, growing potential for misuse and abuse of information systems affecting privacy and ethical values, and external dangers from hackers, leading to denial-of-service and virus attacks, extortion, industrial espionage, and leakage of organization information or private data (ISACA, CISM Review Manual, 2009).

Because new technology provides the potential of dramatically enhanced business performance, improved and demonstrated information security can add real value to the organization by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation. It can also enable new and easier ways to process electronic transactions and generate trust (ISO/IEC 27002:2005).

The day is not far when in the global economy, an organization that wants to do business will be asked to present its information security policy and proof of performance in terms of penetration tests and independent security audits conducted to ensure security of its network and information resources. Publicly traded organizations and others in critical infrastructure sectors will soon be required to report significant security related events so that accurate information on attacks and losses can be compiled. (ISACA, CISM Review Manual, 2009).

The guideline is intended for manufacturing businesses of all sizes and types. To be applicable to a larger number of organisations, the guideline will benefit from being more flexible. Small businesses and large enterprises have different needs and therefore suitable planning strategies will be recommended. What will be appropriate for a global organisation won't necessarily suit a smaller operation. This flexibility will also apply to different industry sectors which have different needs, both in the daily running of their businesses and in regulatory requirements which govern specific industries.

2 LITERATURE REVIEW

In an effort to develop a suitable information security framework for a Kenyan Manufacturing setup, discussions of some past and on-going researches that exhibit commonalities were considered.

Business Continuity Plans (BCPs) were considered in this review to establish their effective implementation. They were also considered to ensure that information security implementations and business continuity deployment and tests are carried out without adversely affecting business operations. The implementations would be well structured and systematic with adequate support and backup procedures.

Research shows that a key driver for Business Continuity Management rise is regulatory requirement and an increasing reliance on technology, making business continuity and information availability a necessary cost of doing business rather than a 'nice to have' (PAS 56, Phil Carter).

A review of risk management models was also considered since risks provide opportunities for innovation. Project Managers and organizations' management must see opportunities in risks and add value to client services rather than avoiding them. Risk management model helps organizations rate, innovate and exploit opportunities.

2.1 Business Continuity Models

2.1.1 Virtual Business Continuity Maturity Model (Virtual Corporation)

Virtual Corporation has developed the Business Continuity Maturity Model (BCMM) as an objective means of measuring the effectiveness of Business Continuity implementations. The goal is achieved through defining the evolutionary path that Business Continuity


Information Security Policy Framework for a Manufacturing Firm

implementations follow as they mature over time coupled with baseline data on the BCM Model of organizations across industry, geographic and other relevant boundaries.

In this Six Level Model, levels one through three represent organizations that have not yet completed the necessary Program Basics needed to launch a sustainable enterprise BCM program. Levels four through six represent the evolutionary path of the maturing enterprise BCM Program.

Figure 1 chart below depicts these six levels of the Business Continuity Maturity Model and summarizes the key requirements to reach each level.

BCM Maturity Level	Program Basics			Program Development		
	Sr. Mgmt Commitment	Professional Support	Governance	All Units Participating	Integrated Planning	Cross-Functional
Level 1 Self-Governed	No	No	No	No	No	No
Level 2 Supported Self-Governed	Marginal	Partial	No	No	No	No
Level 3 Centrally Governed	Partial	Yes	Partial	No	No	No
Level 4 Enterprise Awakening	Yes	Yes	Yes	Yes	No	No
Level 5 Planned Growth	Yes	Yes	Yes	Yes	Yes	No
Level 6 Synergistic	Yes	Yes	Yes	Yes	Yes	Yes



 Increasing Business Continuity Management Maturity

© Virtual Corporation 1994 - 2002

Figure 2-1: Six Levels BCMM

Level 1 - Self-Governed

Business Continuity Management has not yet been recognized as strategically important by senior management. There is no enterprise governance or centrally coordinated support function. If the company has a BCM policy, it is not enforced. Individual business units and departments are “on their own” to organize, to implement and self-govern their business continuity efforts. The state-of-preparedness is generally low across the enterprise.

Information Security Policy Framework for a Manufacturing Firm

Level 2 - Supported Self-Governed

At least one business unit or corporate function has recognized the strategic importance of business continuity and has begun efforts to increase executive and enterprise-wide awareness. At least one internal or external BCM professional is available to support the business continuity efforts of the participating business units and departments. The state-of-preparedness may be moderate for participants, but remains relatively low across the majority of the company. Senior management may see the value of a BCM program but they are unwilling to make it a priority at this time.

Level 3 – Centrally Governed

Participating business units and departments have instituted a rudimentary governance program, mandating at least limited compliance to standardized BCM policy, practices and processes to which they have commonly agreed.

A BCM Program Office or Department has been established, which centrally delivers BCM governance and support services to the participating departments and/or business units. Audit findings from these participants are being used to reinforce competitive and strategic advantage for their groups. Interest in leveraging the work already done is being promoted as a business driver for launching a BCM program. Several business units and departments have achieved a high state-of-preparedness.

However, as a whole, the enterprise is at best moderately prepared. Senior management, as a group, has not yet committed the enterprise to a BCM Program, although they may have a project underway to assess the business case for it.

Information Security Policy Framework for a Manufacturing Firm

Level 4 - Enterprise Awakening

Senior management understands and is committed to the strategic importance of an effective BCM program. An enforceable, practical BCM policy has been adopted. A BCM Program Office or Department has been created to govern the program and support all enterprise participants. Each group has acquired its own and/or utilizes the central BCM professional resources. BCM policy, practices and processes are being standardized across the enterprise. A BCM competency baseline has been developed and a competency development program is underway. All critical business functions have been identified and continuity plans for their protection have been developed across the enterprise. Departments conduct "unit tests" of critical business continuity plan elements. All business continuity plans are updated routinely.

Level 5 - Planned Growth

All business units and departments have completed tests on all elements of their business continuity plan, and their plan update methods have proven to be effective. Senior management has participated in crisis management exercises. A multi-year plan has been adopted to continuously "raise the bar" for planning sophistication and enterprise-wide state-of-preparedness. An energetic communications and training program exists to sustain the high level of business continuity awareness following a structured BCM competency maturity program. Audit reports no longer highlight business continuity shortcomings. Examples of strategic and competitive advantage achieved from the BCM program are highlighted in periodic enterprise communications. Business continuity plans and tests incorporate multi-departmental considerations of critical enterprise business processes.

Level 6 - Synergistic

All business units have a measurably high degree of business continuity planning competency. Complex business protection strategies are formulated and tested successfully. Cross-functional

Information Security Policy Framework for a Manufacturing Firm

coordination has led participants to develop and successfully test upstream and downstream integration of their business continuity plans. Tight integration with the company's change control methods and continuous process improvement keeps this organization at an appropriately high state-of-preparedness even though the business environment continues to change radically and rapidly. Innovative policy, practices, processes and technologies are piloted and incorporated into the BCM Program.

2.1.2 Public Available Specification 56 (PAS 56) BCM (Phil Carter)

Research shows that a key driver for Business Continuity Management rise is regulatory requirement and an increasing reliance on technology, making business continuity and information availability a necessary cost of doing business rather than a 'nice to have'.

With downtime costs so high and the real threat of terrorism, it is not surprising that companies are gravitating to business continuity for protection. **Publicly Available Specification 56 (PAS 56)** is the first step in the process towards a standard for business continuity provision and aims to set guidelines for best practice, to help businesses improve business continuity planning and management. PAS 56 is an informal standard, and the British Standards Institution (BSI) is currently brokering the process for it to become a full British Standard.

a. Driving Demand

There are a number of factors driving demand for a consistent approach to business continuity planning and PAS 56 provides a universal framework for businesses to follow, to ensure that Business Continuity plans are fit for purpose.

In the UK regulatory pressures are a key driver for a business continuity standard, with Basel II, FSA regulations and the Civil Contingencies Act all requiring various organisations to have business continuity plans in place. However, such regulations state that organizations must make

Information Security Policy Framework for a Manufacturing Firm

business continuity provision but do not give any detail on what this should entail or how comprehensive it must be, leaving it up to individual organisations to deem what is appropriate. The emergence of PAS 56 goes some way towards setting a benchmark for businesses on what planning they should have in place, making it easier for them to achieve compliance with the raft of existing and future regulations.

The prevalence among businesses to outsource key business functions to cut costs, and the reliance on supply chain processes to provide goods and services, also highlights a key area where business continuity provision must be made. Businesses are increasingly demanding that their suppliers or outsourced partners have appropriate business continuity plans in place because if they fail to deliver a service or can't access data due to an incident, the potential to have a huge impact on others in the supply chain exists. Working with a supplier who has achieved a recognised standard for business continuity provision will give organisations peace of mind that the supply chain won't fall over in the event of a disaster.

Insurers are also advising businesses to have contingency plans in place to benefit from lower premiums as a result of reduced risk. A British Standard will enable companies to meet this requirement and prove to insurers that the appropriate plans are in place.

b. Setting the Standard

The main aim of PAS 56 is to:

- a) Define the process, principles and terminology of business continuity management.
- b) Provide a generic framework for incident anticipation and response.
- c) Describe evaluation techniques and criteria.

PAS 56 advises how to implement good business continuity management which it outlines as: linking to corporate governance, having board level endorsement and accountability, clearly defining and documenting accountabilities and responsibilities, and making it a "business as

Information Security Policy Framework for a Manufacturing Firm

usual” process. The guidelines are intended for use by those charged with defining, developing, implementing and managing a business continuity management programme.

PAS 56 is a precursor to a full British Standard for business continuity. It must be based on a legal framework for it to become a national standard, be auditable and advise a consistent approach to business continuity. To become a national standard it must firstly have the full backing of all interested parties including government, businesses, trade associations and consumers. If the consensus is to make it a standard then the BSI will facilitate a full British Standard for business continuity.

c. Making the Grade

The wording of PAS 56 as it currently stands may cause concern for organisations, and during the consultation stage there are a few areas which must be reviewed and revised if the standard is to be taken up among businesses.

For example, the current document recommends live testing twice a year. Testing is a crucial part of business continuity as it supports, matures and develops the plan. A business continuity plan is no good sitting on a shelf – it has to be useful and usable and must reflect the fact that organisations are dynamic entities where the only constant is change. Regular testing ensures that the plan is fit for purpose and in step with the recovery needs of the business.

With live testing, organisations would need to close down all applications as if a disaster had occurred and invoke their BCP. But running this type of test could have disastrous effects in itself, by putting businesses at risk and tempting fate. Testing the business continuity plan is designed to spot oversights and omissions such as holes in vital processes or to determine where upgrades are needed; but with live testing it's too late if the plan is not up to scratch and could result in lost business and customers not being able to access staff or services. The other advantage of testing is to engender staff confidence and competence in the BCP and how they

Information Security Policy Framework for a Manufacturing Firm

will utilise it in an emergency. To ensure that business continuity plan testing has the desired effect in this respect requires careful planning and preparation and a live approach may be counter-productive.

A better approach would be to suggest carrying out testing out of normal office hours, at the weekend or in the evenings, to minimise potential disruption to staff and critical business processes; but with a realistic scenario to put them through their paces with a degree of rigour.

The guidelines are intended for businesses of all sizes and types, but to be applicable to a larger number of organisations the guidelines would benefit from being more flexible. It should be taken into account that small businesses and large enterprises have different needs and recommend suitable planning strategies accordingly. What will be appropriate for a global organisation won't necessarily suit a smaller operation. This flexibility also applies to different industry sectors which have different needs, both in the daily running of their business and in regulatory requirements which govern specific industries. Although a framework suitable for all businesses would be hard to achieve, the standard needs to be as flexible as possible to enable all businesses to apply for certification, if they wish.

d. Delivering the Goods

In the UK over 3,000 organisations have bought the guidelines and the feedback has been encouraging. PAS 56 is a good starting point and with constructive feedback from the industry it will be a step in the right direction for a consistent approach to business continuity planning.

For businesses, PAS 56 will provide a valuable tool to putting appropriate Business Continuity plans in place. For the industry, it is recognition that business continuity is a necessary part of doing business: it is no longer appropriate to be satisfied with IT-centric reactive disaster recovery only – though this will always have its place; we need the resilience, continuity and

Information Security Policy Framework for a Manufacturing Firm

availability of the business to be regarded as a proactive management concern and PAS 56 provides a framework for this to happen.

Not only this, PAS 56 is indicative of the movement towards information availability – the process of keeping people and information connected. In the ‘always-on’ environment of today’s business and consumer world, where 24/7 and on-demand are part of the course, business continuity and information availability should no longer be considered optional or specialist concerns; they actually are - and should be perceived as - part and parcel of the way we live today. Business as usual – no matter what!

2.1.3 Business Continuity Models Conclusion

- a) Business Continuity models give an objective means of measuring the effectiveness of Business Continuity implementations
- b) Business Continuity provides an evolutionary path towards maturity coupled with baseline data and standards
- c) Business Continuity models provide guidelines for best practice and help businesses improve Business Continuity planning and management
- d) The models provide a universal Business Continuity framework and benchmark for compliance to regulatory requirements
- e) The models provide guidelines for definition, development, implementation and management of Business Continuity program
- f) The models provide a proactive management tool that provides resilience, continuity and availability of the business

Information Security Policy Framework for a Manufacturing Firm

2.2 Risk Management Model

2.2.1 360 Degree RISK Management Model (Infosys Technologies limited)

Risks provide opportunities for innovation. To differentiate from competition, project managers and organizations must see opportunities in risks and add value to client services.

360 degree RISK management model helps organizations rate, innovate and exploit opportunities. It focuses on enabling project managers and organizations to:

- a) Discover and seek the silver linings in the clouds of risk
- b) Periodically identify and mitigate the negative consequences of risks
- c) Utilize the experience from dealing with risks to enhance competency

2.2.2 Understanding RISK – Positive and Negative Implications

RISK stands for Rate, Innovative and Share Knowledge

Implications:

- a) The downtime of a site has financial repercussions due to business loss
- b) Violation of data disclosure and intellectual property laws can threaten the very existence of an organization.
- c) Lack of processes is manifested in the form of non-compliance, poor disaster management and ineffective business continuity
- d) Cyber crimes and instances of failure of implementing regulations depict the double-edged power of information technology

Due to the vital role of IT in business, software failure directly or indirectly results in business failure. The IT industry, unfortunately, seldom sees risks in positive light unlike finance or gambling who will see a risk as an asset. Risk by itself is not bad. The secret lies in striking the

Information Security Policy Framework for a Manufacturing Firm

right balance between negative consequences and the potential benefits of the associated opportunity.

2.2.3 Drivers of a Holistic Risk Management Model

The primary drivers are:

Qualitative Drivers

Risk models have generally been reactive, silo-based and have resolved risks in a project's immediate context. There has never been a focus on learning from the mistakes or experiences of others in the organization. Organizations have avoided risky projects and have even ignored possible opportunities due to their conservative approach.

A holistic or enterprise outlook can change the mindset of organizations. They may explore and venture into new opportunities to reduce time-to-market, exploit new product lines and enable participants to deal with risks in a mature way.

Quantitative Drivers

Independent analysts indicate that it is 10 times more expensive to deal with risks in a fragmented manner as compared to an integrated approach. Statistics show that 30% of IT investment is silo-based support for risk and compliance management is wasted.

Therefore requirement of a model that will help save costs, help generate more revenue, help people at operational level deal with risks in a streamlined fashion, enable us to be change agents to help ourselves and the organization.

2.2.4 Constituents of the 360 Degree Risk Management Model

The 360 degree risk management model comprises people, processes, tools, services and robust governance. People are stakeholders who belong to both the performing and outsourcing organizations. The governance model can be visualized as project management organization (PMO) with Subject Matter Experts in risk, providing services to units across the organization. Services rendered are portfolio and project support, training, tools support, corporate risk database maintenance, and innovation.

At the portfolio level, the model helps in analyzing trends in risks and providing recommendations. Guidance on responding to risks and mitigating them early is provided at the project level. Training and certification programs are conducted to increase awareness and address risks creatively. Tools are developed and maintained for managing risks. The model provides an agile set of processes that commence early in the project life-cycle. Senior management buy-in and involvement indicate the significance of addressing risks effectively.

2.2.5 Implementation Approach and Efficiency Index

The success of an idea lies in its implementation and ability to measure efficiency. The philosophy behind the approach recommended here is that the model should be agile, self-sustaining and evolving. The Software Engineering Institute (SEI) recommends the concept of continuous risk management. This is achieved by using the Plan-Do-Check-Act or PDCA cycle.

The PDCA cycle is illustrated in **Figure 2-2** below:

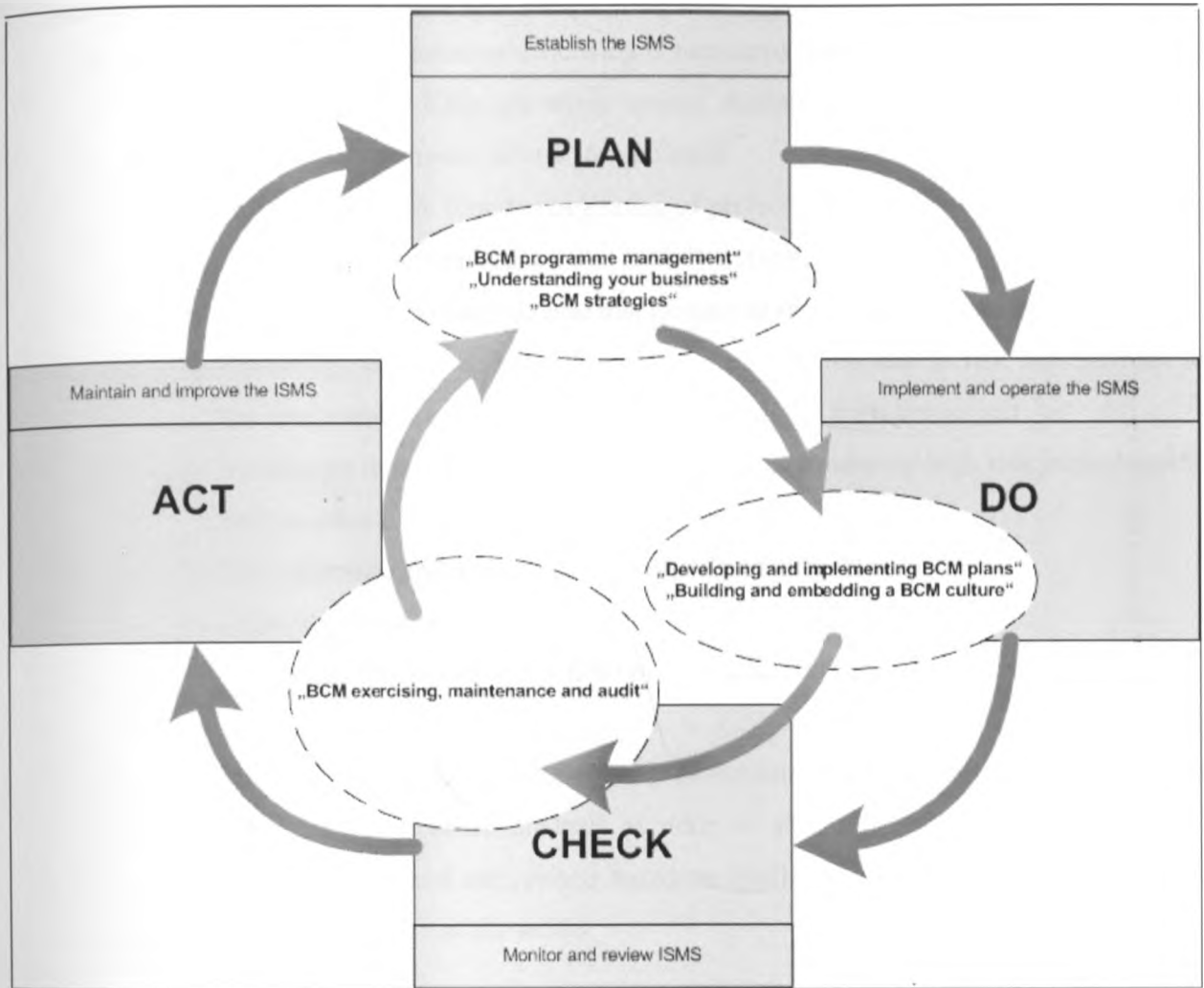


Figure 2-2: PLAN-DO-CHECK-ACT (PDCA) cyclic model of ISO/IEC 27001

- a) Plan phase – Key stakeholders are identified and the framework is defined
- b) Do phase – After the processes and governance model are set up, the focus shifts to execution of services. Tools are deployed. Receivers of the service utilize the model right from the stage of project contract formulation to project closure. Recommendations of the risks are implemented.

Information Security Policy Framework for a Manufacturing Firm

- c) Check phase – Implementation efficiency is measured through a set of key performance indicators (KPIs). The KPIs are along several dimensions and help in measuring the positive and negative impacts of risk, for example
- 1) Percentage of risk found at beginning of project to those found at later stages
 - 2) Percentage of revenue saved due to early mitigation of risk
 - 3) Percentage of revenue increase due to innovation in risk management
 - 4) Percentage of knowledge sharing documents shared due to risk management to the total number of knowledge sharing documents from the project
 - 5) Percentage of project managers who are willing to take up high risk projects to the total number of project managers
 - 6) Risk exposure amount as a percentage of total project value
 - 7) Usability of the service
 - 8) Customer satisfaction index from projects that were serviced
- d) Act phase – this is a self-correcting and evolutionary step. Base on the parameters computed above, root cause analysis is done to find out why risks appeared. The components of the model are revised based on feedback so that better services can be provided to the receivers of the model.

2.2.6 Processes and Tools to Effectively Identify Risks and Plan Risk Response

Identifying risks and planning the right risk response is a core service provided by the model.

Processes required are:

- 1) Opportunity-level processes – All proposals are vetted to review the level of risk and reasonableness of the clauses in the project contract. These processes help in prioritizing projects and scheduling projects within a program.

Information Security Policy Framework for a Manufacturing Firm

- 2) Portfolio/Program-level processes – There are several interesting mechanisms for the portfolio and program to understand how different components contribute to overall risk of the portfolio
- a) Project in a portfolio are profiled with respect to risk using a formal risk assessment process.
 - i. Gather project-related information from internal systems and capture details bi-monthly using a risk assessment sheet
 - ii. A standard workbook is created and used for project risk assessment for a 360 review of the project. Delivery Managers, Portfolio and Project Managers, Software Quality Analysts are interviewed for their inputs. The list of risks is made available to the team for discussions.
 - iii. Depending on the complexity of the situation, the PMO and Risk Subject Matter Experts may review or group review the project/account problems to arrive at the best possible solutions.
 - iv. A risk assessment report is generated at the end of the exercise. The focus of this report is on converting solutions into action items.
 - v. Most projects then move to the monitoring stage to be followed up until action items are closed and/or project moves back to the normal category.
 - b) Status tracker reveals project risk parameters due to time, quality and schedule. They also report the progress of risks.
 - c) Depending on the nature of the project, indices are used to indicate the level of product quality risk. Product quality metrics are used for development and maintenance projects, the service satisfaction index is used by production support.
 - d) Project health and risk are reported through dashboards to senior management. Finer details can be drilled down based on role-access. All risks are updated to corporate risk database.
- 3) Review and audits – Periodic review and audits by senior management and internal auditors help in gauging risk response effectiveness and checking if experiences are adequately captured and used.

Information Security Policy Framework for a Manufacturing Firm

- 4) Risk reporting is very important for communicating and distributing information. Its usefulness depends on the level details provided. Weekly alerts to Project Managers contain Earned Value Management statistics and defect deviation of actual from planned. In the report, risks are viewed on a time-scale – short, medium and long term. Progress of risk is monitored. Dependencies, impact and steps taken to meet risks are also presented.
- 5) Trends analysis helps to confirm if proper methods are followed. The quality team studies the qualitative and quantitative risks and impacts. Checks are made to see if the mitigation measures followed are compliant with processes. Milestone reports provide a peek into residual and secondary risks. Other trends analyzed are stability of requirements, defect density, errors due to incorrect releases, critical path changes, and productivity.

The toolset provided by this model is fine-tuned for practical use:

- 1) Corporate risk database – From various business units within an organization, statistics with respect to risk situations like risks, choices available to address them, decisions taken and their success/failure are collated in a single repository called the corporate risk database.
- 2) Pop-up tools – Risks faced in the project based on similar projects across the company. The tool offers lessons learned from all other projects in the organization.
- 3) Program dashboards provide the state of risks in the program. Elements illustrated are Earned Value Management, quality of service, coverage of projects under the model, percentage of projects in risk, process metrics trend, productivity, customer feedback index, and financial analytics.
- 4) The “money at risk calculator” is a tool that tracks the dollar value at stake due to impending risks.

2.2.7 Mechanisms to Exploit Opportunities in a Risk

It is better to be prepared for an opportunity and not have one than to have an opportunity and not be prepared. Companies that initially saw risks in outsourcing later identified it as an opportunity and exploited it by setting up bases across the globe. The techniques presented below help in solving problems innovatively and exploiting them for positive impact:

SWOT analysis – A strategic business planning tool. Opportunities and threats are external factors that we may not have direct control over whereas strengths and weaknesses are internal to the organization and can be addressed. This analysis can be deployed to select projects and formulate strategies to achieve business goals.

TRIZ – Russian acronym; for the theory of inventive problem solving. It provides ways to search patent databases and solutions in other industries to help solve problems by identifying contradictions in them.

Portfolio-Level Innovation Techniques – Used to study risk trends at the portfolio level. Experiences are used to create new ideas for other projects. The specific solution to a risk can be converted into a more generic one and applied to other projects in the portfolio.

Project-Level Opportunities Tracking – identifies/creates new tools and services. For example, if there is a schedule risk and code documentation is yet to be developed, creating a tool to automate documentation will save effort and help meet the schedule. This document generator will be the project's contribution to services like tool-based code documentation.

Organization Process Changes – Corrective actions taken in various portfolios in the organization over a time period (e.g. annual) after a risk is analyzed for root causes. Thus,

Information Security Policy Framework for a Manufacturing Firm

risks also provide an opportunity to review and make organizational-level process changes.

2.2.8 Knowledge Sharing Mechanisms to Enhance Competencies

Competent managers must address various issues including financials, performance, regulatory and management issues to create winning products. In order to facilitate “R” or Risk response skills of managers, the following methods are proposed:

- a) Establish education and programs to enhance skills in risk management tools
- b) Create a network of managers who have handled high-risk projects to share their learning and experiences.
- c) Create a forum of risk experts who can be conducted when projects are faced with the need to take informed decisions and trade-offs in critical risk situations.
- d) Create a portal of lessons learnt from various projects
- e) Conduct knowledge sharing colloquiums to gather lessons and best practices from other companies in the industry.
- f) Build a compendium of all possible risks in the lines of business undertaken by the organization, their causes and impact on product quality and performance metrics.
- g) Create a knowledge asset of risk lists and a comprehensive set of generic protective actions.
- h) Build risk management into the goals of project managers and business units to encourage risk evaluation

2.2.9 Benefits of the 360 Degree Risk Management Model

The 360 degree risk management model helps:

- a) Gain competitive edge by providing depth and rigor
- b) Ensure operational continuity, mitigate risks early, and avoid financial loss
- c) Calculate the risk impact holistically through Key Performance Indicators (KPIs)

Information Security Policy Framework for a Manufacturing Firm

- d) Increase predictability, trust worthiness and enhance brand value
- e) Seek and exploit opportunities in risks, while avoiding unnecessary risks
- f) Expand the business footprint, and product and service diversification
- g) Move uncertainties from blind spots to areas where they can be measured, monitored and responded to

2.2.10 Implementation Challenges and Solutions

This is a base model with constituents for most situations; it does not provide solutions for all situations all the time. It needs to be adapted, customized and extended based on the risk trends in the organizational and business needs.

The first response to any change or movement is to resist it and avoid it by stating different reasons why it is difficult to practice or how it might fail. Concerns regarding how the organization will react to failures or crisis can be overcome by providing incentives to risk takers.

When managers see the shift in the risk postures of the senior management and perceive the openness to learn from failures and success, they will be inclined to embrace change.

2.2.11 360 Degree Risk Management Model Conclusion

The benefits of the 360 degree risk management model are; to provide enough incentive for practitioners to adopt it as the framework to innovate, share knowledge and holistically respond to risks.

Based on the inherent strengths and weaknesses of an organization, risk handling strategies have to be modified to enable managers to make their programs and projects successful. The concepts

Information Security Policy Framework for a Manufacturing Firm

and skills need to be woven into day-to-day business decision making. They must be self correcting and self sustaining for continuous improvement of products and services.

The 360 degree risk management framework is designed to take the IT industry to a whole new plan of responsibility. From merely providing technical solutions to customers, we can become their trusted partners.

2.3 ISO/IEC 27002:2005 Information Security Standard

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

The standard details a comprehensive set of information security control objectives and a selection of best-practice controls.

These major components of ISO/IEC 27002:2005 are:

- a) Security policy
- b) Organization of information security policy
- c) Asset Management
- d) Human Resource security
- e) Physical and environmental security
- f) Communications and operations management
- g) Access control
- h) Information systems acquisition, development and maintenance
- i) Information security incident management
- j) Business continuity management
- k) Compliance

Information Security Policy Framework for a Manufacturing Firm

a) Security Policy

Information security policy should provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Establishing and maintaining information security policies that support business goals and objectives is the responsibility of the information security manager. A process should be in place for the development and maintenance of security policies. An organization need to ensure that these policies become an integral part of its overall governance. Standards must then be reviewed and modified as needed to address the changes of the policies. Information security policies that support business goals and objectives are normally approved by the board of directors. Security procedures and guidelines are derived from security policies.

b) Organization of Information Security Policy

A management framework should be established to initiate and control the implementation of information security within the organization.

Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

Information Security Policy Framework for a Manufacturing Firm

c) Asset Management

An information security policy should ensure that an appropriate protection of organizational assets is achieved and maintained. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

d) Human Resource Security

Human resource security must be considered to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

e) Physical and Environment Security

Physical and environment security should be enforced to prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Information Security Policy Framework for a Manufacturing Firm

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

The protection provided should be commensurate with the identified risks.

f) Communication and Operations Management

Communication and operations management should be considered to ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

g) Access Control

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

Information Security Policy Framework for a Manufacturing Firm

h) Information Systems Acquisition, Development and Maintenance

Security requirement of information systems acquisition, development and maintenance is to ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

i) Information Security Incident Management

Information security incident management is required to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

j) Business Continuity Management

The main objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Information Security Policy Framework for a Manufacturing Firm

A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization.

Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

k) Compliance

The main objective of compliance is to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and

Information Security Policy Framework for a Manufacturing Firm

may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

It is important to note here that Information Security Policy Framework implementations may vary from one organization to another. Most organizations will develop their Information Security Policies from established models like the ISO/IEC 27002:2005 to address their security requirements. A number of companies may implement an entire Information Security Policy Framework that will incorporate various security components cutting across the company establishment. A majority of other organizations would prefer having a number of Information Security Policy Frameworks for different sections or business processes.

3 RESEARCH METHODOLOGY

In this information security research project, evaluation of some Business Continuity Models gave an insight in the designing of an appropriate Information Security Framework that can assure organizations of Business Continuity. BCP's were evaluated to enable coming up with a security model that would consider all the important aspects of Business Continuity. BCP's are important in businesses, and hence information and communications technology. ICT is now a must for an effective business enterprise and hence it's continued security.

The research also involved evaluation of Risk Management Models to design an Information Security Framework that can be adapted, customized and extended based on prevailing risk trends. Risk management also provided an innovative approach of exploiting opportunities in risks. More often than not, risks have been seen as a threat to enterprises and information. Organizations have avoided high risk projects, but risks can provide opportunities for creativity and innovation. Proposed information security model, having considered risk management in detail, has incorporated these innovations and opportunities.

The project research also involved a thorough evaluation of the ISO/IEC 27002:2005 Information Security Policy Framework standard. The standard was used as a guide in the analysis and development of an appropriate Information Security Framework for a Manufacturing setup. ISO/IEC 27002:2005 is a standard that has been thoroughly tested and hence was considered an important tool in coming up with a comprehensive information security model that addresses all aspects in the selected study area of manufacturing enterprises.

The research project involved analysis of major manufacturing organizations information security implementations. Other organizations were also considered in the research to establish similarities in information security implementations and discover major security challenges faced. Besides a majority of manufacturing organizations, the research also considered some service, telecommunications and education institutions among others. The findings of other

Information Security Policy Framework for a Manufacturing Firm

industries' information security requirements would enable coming up with appropriate recommendations for generalizations later.

An evaluation of Information Security compliance of selected organizations was done to establish whether the organizations met commonly agreed upon security standards. The information security project research was geared towards establishing the degree of compliance to legal and statutory requirements. The research aimed at establishing whether information security policy implementations were practical in real operational environment and if they complied with industry best practices.

3.1 Research Methods Used

Methods used in the formulation of an Information Security Policy framework were mainly structured questionnaires, electronic mail and internet surveys as described below:

3.1.1 Questionnaires

Questionnaire research method was chosen because it is cheap compared to other types of surveys; it did not require much effort as compared to verbal or telephone surveys. It was also appropriate because it was possible to get as much information as possible for better analysis and objective reporting. The responses were also easily standardized as required for easier compilation of findings. The questionnaires used in this research were closed-ended for simple and directed responses. Ordinal-polytomous scale was used in this research to determine implementation of specific Information Security topic.

In order to come up with a complete questionnaire that would address the research project topic, the security models discussed earlier in the literature review were considered as a guideline. ISO/IEC 27002:2005 was particularly used to ensure that all business processes were adequately covered.

Information Security Policy Framework for a Manufacturing Firm

Questionnaires were formulated targeting specific information security areas and circulated to target respondents by either electronic mail or in hard copies. They were then duly completed and returned either by electronic mail or hard copies. A follow up was done to maximize the response levels. Questions were asked from a written questionnaire and all answers from respondents recorded. The questionnaire was simplified with directed response to capture full attention of the respondents. The questionnaire was also classified in a logical order to assure at least one response in key areas to facilitate good analysis. **Appendix A** shows a typical questionnaire response from one of the respondents.

A representative sample of target respondents was taken from the population to make the research more objective. Each response was thoroughly vetted for integrity and accuracy before being considered as a part of the research findings. The trend of the responses was reviewed to establish common mistakes and inconsistencies which were corrected before further analysis. Only meaningful information was considered for analysis.

The main areas covered in the questionnaire were to find out whether:

- Sampled organizations have an Information Security Policy in place
- Security Policies are fully supported by Senior Management
- Security Policy objectives are in line with business strategies
- Developed Information Security Frameworks are fully enforced
- Information Security Policies are periodically reviewed and audited
- Security Policy reviews and audits are documented and followed up
- Security Policies are Compliant with legal requirements and standards

3.1.2 Electronic Mail and Internet Surveys

Electronic Mail was a cost effective and fastest method of distributing questionnaires to prospective respondents and getting feedback. To ensure maximum response to questionnaires, and make the data collection method more effective, there was consistent follow up by electronic

Information Security Policy Framework for a Manufacturing Firm

mail, telephone calls and personal visits. There was also response confirmations and reminders attached to the electronic mails circulated.

Internet survey was quite instrumental in the literature review to find out various information security policy implementations and security models from varied industries and countries. From the internet, information about statutory and legal requirements, information security compliance, and industry best practices of various establishments was found. This information was pertinent in designing an appropriate information security model for a manufacturing setup.

Internet is a powerful source of information with forums of expert information and discussions. Internet is the most immediate and fastest source of information. Information Security model changes, enhancements and continuing research could easily be found on the internet. Internet gave the most current status of the information security models studied.

3.2 Sampling Procedures Used

Contacting, questioning, and obtaining information from a large population, can be extremely expensive, difficult, and time consuming. A properly designed probability sample, however, provides a reliable means of inferring information about a population without examining every member or element. When properly conducted, a probability sample of this size provides reliable information with a very small margin of error for the whole population.

In this research, probability sampling was used because the possibility of selecting each member of the population was known in advance. This research methodology was considered because probability samples are the only type of samples where the results can be generalized from the sample population. Probability samples also allow calculating the precision of the estimates obtained from the sample and specifying of the sampling error.

Information Security Policy Framework for a Manufacturing Firm

Probability sampling was considered to be more accurate than a census of the entire population. The smaller sampling operation facilitated more rigorous controls, thus ensuring better accuracy. These rigorous controls allowed the research to reduce non-sampling errors such as interviewer bias and mistakes, non-response problems, questionnaire design flaws, and data processing and analysis errors.

These non-sampling errors were reduced through pretesting to allow careful testing of the survey questionnaire and procedures. The detail of information that could be asked in a sample was greater than that in a census due to the cost and time constraint. A relatively long and comprehensive questionnaire was administered to the sample more easily.

A simple random sampling was used since an exhaustive list (sampling frame) of all manufacturing setups in Kenya could easily be determined. From the list, the sample was drawn such that each manufacturing establishment had an equal chance of being drawn during each selection round without replacement. Manufacturing companies selected for sampling were removed from the population for all subsequent selections. At any draw, the process for a simple random sample without replacement provided an equal chance of inclusion of any member of the population not already drawn. To draw a simple random sample without introducing research bias, SPSS or PASW software was used to impartially select the members of the population to be sampled.

4 RESEARCH FINDINGS AND DISCUSSIONS

4.1 Population Sample

There are 615 manufacturing companies in Kenya as per Kenya Association of Manufacturers Directory (2009). The companies are of variable sizes and are engaged in different economic activities. The core business activities of these manufacturing companies can be classified into the following major categories:

- a) Building and construction
- b) Chemicals and allied
- c) Consultant and industrial services
- d) Energy, electrical and electronics
- e) Food, beverages and tobacco
- f) Leather products and footwear
- g) Metal and allied
- h) Motor vehicle assembly and accessories
- i) Paper and paperboard
- j) Pharmaceutical and medical equipment
- k) Plastics and rubber
- l) Textiles and apparels
- m) Timber, wood products and furniture

A study of a number of these organizations' information security implementation gave an insight of practical status and established a base for recommendation of an appropriate security model. From the research findings, most medium to large enterprises, have attempted to put in place security implementations of their information resources. Some organizations have manual implementations whereas others have intranets and electronic information security implementations.

Information Security Policy Framework for a Manufacturing Firm

The study focused on these manufacturing firms to find out how they have implemented Information and Communication Technology to support their core businesses. It was found that ICT had necessitated information security implementation to safeguard valued organization resources. The implementation of a suitable information security model, organizations would achieve a more cost effective way of optimizing performance or operations by ensuring availability, integrity and confidentiality of their ICT Infrastructure.

Beside manufacturing establishments, the study also considered a small number of other industries like the service industry, academic institutions, and telecommunications among others mainly to establish common aspects of information security implementations for recommendation of a more generalized approach.

It was desirable to undertake a comprehensive study of almost all manufacturing establishments, but due to the limitation of time and resources, a representative sample was considered. The study considered the maximum possible number of companies within the limited time to come up with more objective findings for representation of the entire population. Also to ensure good response time, different research methods were deployed for different organizations. The research findings were tabulated and carefully analyzed for elaborate reporting.

The research sample was randomly taken from the entire population using statistical sampling methods. During the sampling, caution was taken for better representation of organizations by size and core business activities engaged in among other factors.

From the possible 615 Manufacturing companies in Kenya (Kenya Association of Manufacturers' Directory, 2009), only about 250 companies are of medium to large in size based on annual turnover. The research mainly considered companies of this magnitude because of their organized company structures, and better communication infrastructures to facilitate the study. 150 questionnaires were distributed to prospective respondents, of which 96 gave effective

Information Security Policy Framework for a Manufacturing Firm

responses whose findings were considered for analysis. The data was considered sufficient in designing a suitable Information Security model for a manufacturing setup.

4.2 Research Data Analysis

In the data analysis, *Statistical Package for Social Sciences* (SPSS) software which in 2009 was re-branded as *Predictive Analytics SoftWare* (PASW) and Microsoft Excel statistical tools were used because they were the most appropriate in analyzing and presenting the data collected. These tools were used mainly in descriptive data analysis and in measuring correlations or relations. Statistical frequency charts, cross tabulations and correlations which were used in the presentation of the findings were accurately and easily computed using these tools. The statistical analysis tools were further used in testing the findings using standard testing methods.

Frequency charts gave a quick pictorial view of the proportions of respondents on specific information security topics. They showed responses on a nominal scale of whether an organization had implemented an information security aspect being asked by responding "Yes" in affirmative or "No" otherwise. Other responses to the questionnaire were "Don't know" and "N/A" for ensuring that respondents get an appropriate alternative response in cases where an information security aspect response was neither "Yes" nor "No".

The responses were further assigned proportionate values or weighted appropriately for better analysis as follows:

1) Yes	100
2) No	0
3) Don't Know	20
4) N/A	10

"Yes" response was given the highest score of 100 because it was the expected positive response.

"No" on the other hand had the lowest score of 0 (zero) which was the least expected response in

Information Security Policy Framework for a Manufacturing Firm

circumstances where an Information Security aspect was confirmed to be lacking. “Don’t know” and “N/A”, however got some minimal score because of benefit of doubt. These two mainly catered for respondent’s inability to give factual information either deliberately or due to incompetence about the information security status of the topic.

Crosstabs or otherwise called cross tabulations were deployed to measure Information security associations or relationships among various components. In almost all cases information security components were found to be strongly related. For instance for information security policy to be effectively implemented, there must be senior management commitment to the process. In cross tabulations, bar charts were plotted for better interpretation of the results.

Correlation analysis (also called “Least Squares” analysis) was used in this research to help examine relationships among variables as well. Pearson’s correlation coefficient and Spearman’s rho correlations, with their significance levels were computed from the statistical data analysis using PASW or SPSS.

From the research findings, it was established that there is a strong relationship among the various Information Security components because the correlations were quite significant.

4.2.1 Bar Charts Showing Respective Frequency Responses

Bar charts were considered for some key information security topics to give a quick graphical representation of responses from the data collected. These represented proportions or frequencies and hence could be effectively projected for the entire population. As an example, approximately 67% of the population has a published information security policy as in figure 4-1 below.

Information Security Policy Framework for a Manufacturing Firm

Published approved Information Security Policy

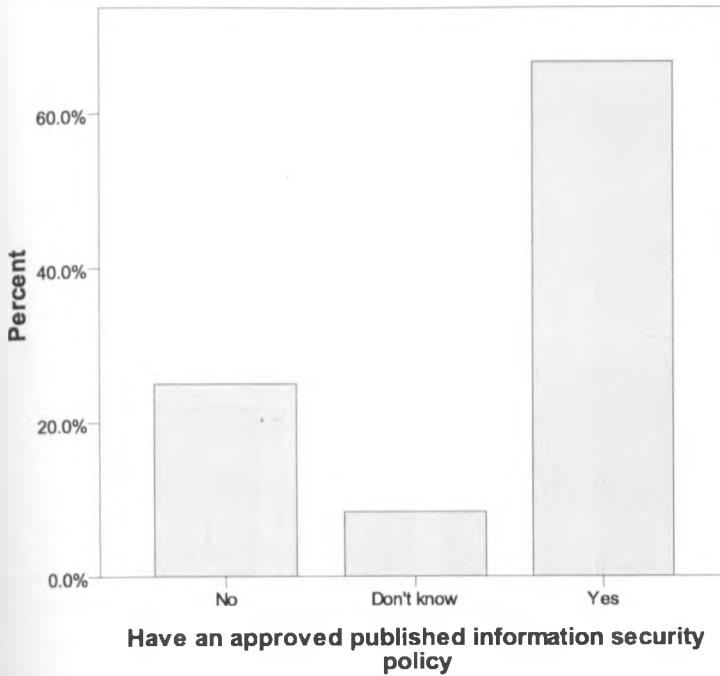


Figure 4-1: Bar chart of Approved Information Security Policy

From the findings, information security policy implementation is an acknowledged concept in most organizations. Most organizations are now working on the modalities to get the information security policy effectively implemented, for efficiency, compliance and business continuity among other reasons.

Information Security Policy Framework for a Manufacturing Firm

Information Security Communication to All Employees

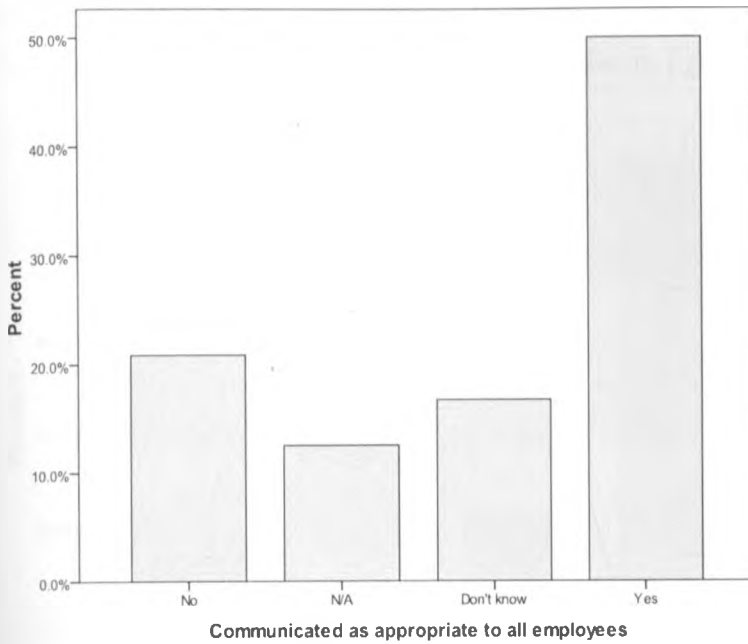


Figure 4-2: Information Security communication to all employees

Information Security study also reveals that only 48% of the population as indicated in figure 4-2 has communicated the availability and function of the Information Security policy. It is only after effective communication that users can enforce the requirements of Information Security policy. An excellent policy without good communication channels to users will not be of any benefit to the organization. Communication should be in form of intranets, training, newsletters etc.

Security Policy Management Commitment

It is evident from the study that for an Information Security Policy to be effectively implemented, senior management must fully participate in the process. With senior management involvement, it will be easier to align organizational strategies with Information and

Information Security Policy Framework for a Manufacturing Firm

Communication Technology strategies. The process will ensure maximum utilization of emerging technologies for increased productivity and hence competitive advantaged against other players. 58% of the organizations researched have senior management actively committed to Information Security implementation as illustrated in figure 4.3.

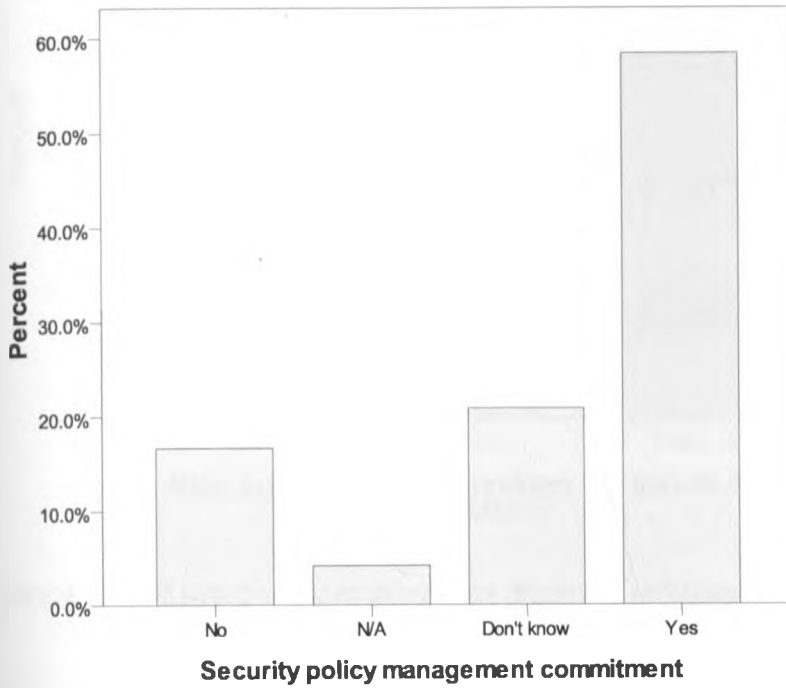


Figure 4-3: Security Policy management commitment

Information Security Policy Framework for a Manufacturing Firm

Risk assessment to Determine Impact of Interruptions

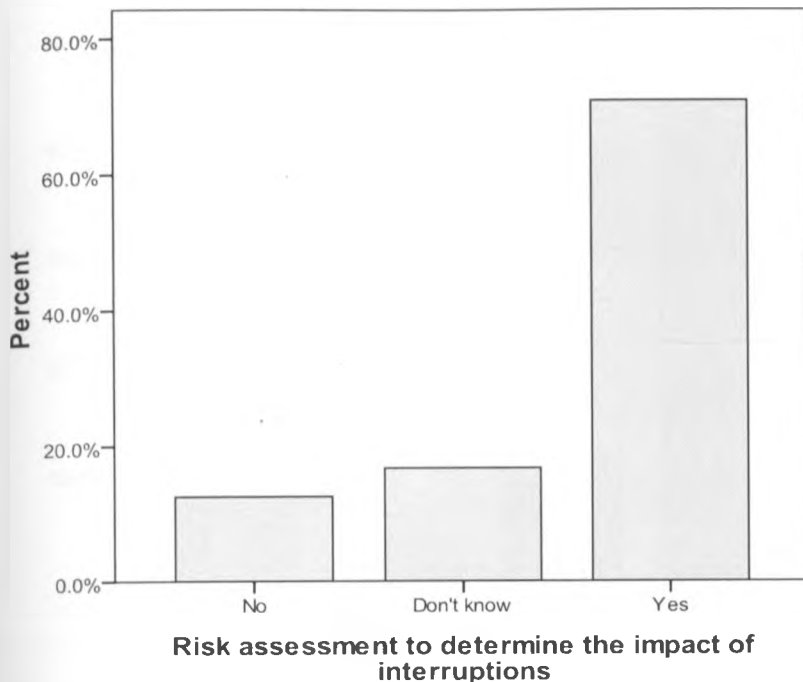


Figure 4-4: Risk assessment to determine impact of interruptions

From the study, 72% of the population undertakes Risk Assessment to determine the impact of disruptions as illustrated in figure 4-4 above. Disruptions would lead to an organization losing a lot of money in lost productivity and hence the need for Risk Assessment and for corrective action.

Information Security Policy Framework for a Manufacturing Firm

Regular Updates in Organizational Security Policies and Procedures

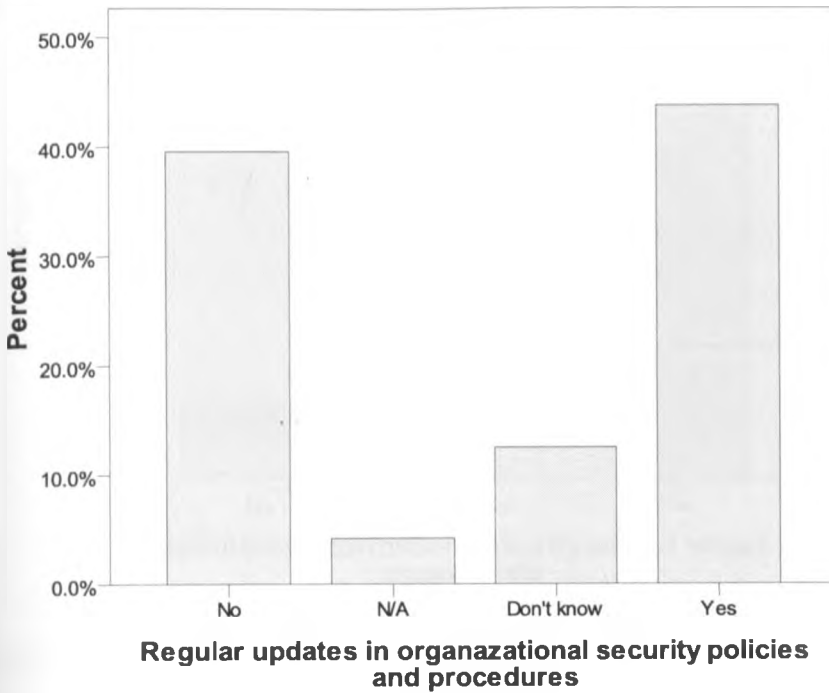


Figure 4-5: Regular updates in organizational security policies and procedures

Only about 45% of the population conducts regular updates of organizational security policies and procedures as depicted in figure 4-5. Reviews and updates are important in adjusting the policies to changing organizational needs and integrating security policies to change management processes.

Specialist Information Security Advice

Information Security Management reviews and updates calls for specialist advice. Majority of organizations at 75% of the population have specialist information security advice as shown in figure 4-6 below. Many of these organizations either have their security operations managed or administered by an Information Security Manager and/or a security consultant firm or security specialist to review and advice on information security implementations.

Information Security Policy Framework for a Manufacturing Firm

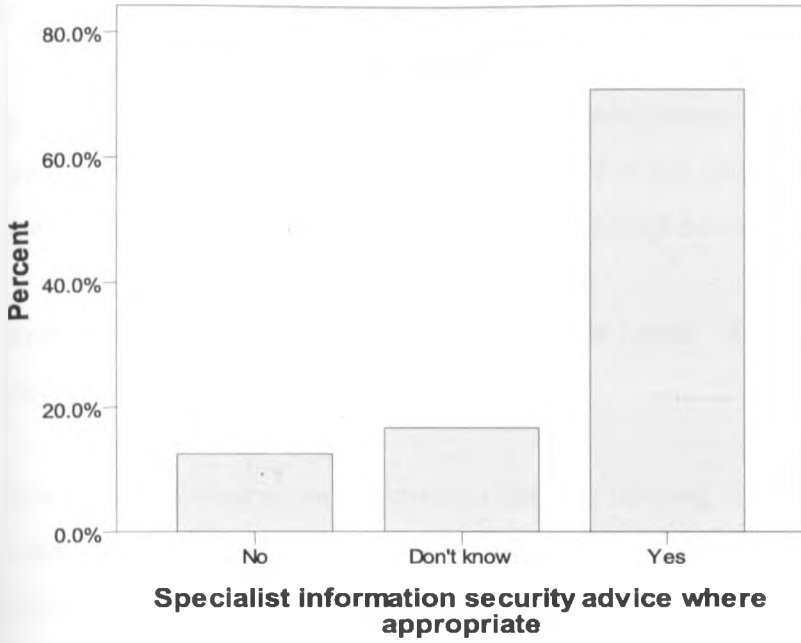


Figure 4-6: Specialist information security advice

Employees and Third Party Users' Reception of Appropriate Security Training

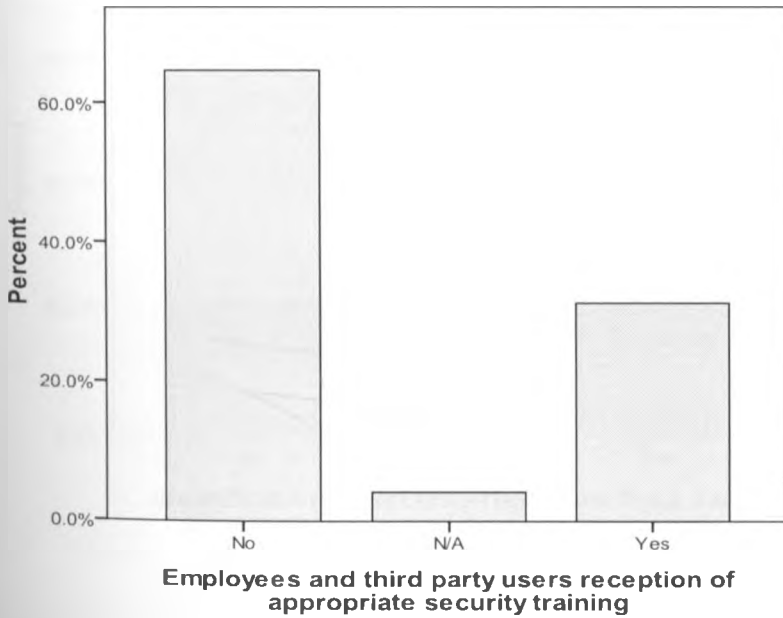


Figure 4-7: Employees and third party users' reception of appropriate security training

Information Security Policy Framework for a Manufacturing Firm

Most organizations do not have an Information Security Training strategy for their employees and other third party users. Only about 30% have implemented appropriate security training programs as shown in figure 4-7. Information Security information will be important in knowing the implications of exposing organization resources at risk and hence taking corrective measures. Training should be emphasized for effective Information Security implementations.

Security Risks from Third Party Access and Appropriate Security Controls Implementation

Despite poor performance on Information Security training, a majority of the organizations have in place measures of identifying security risks from third party access and implementing appropriate controls. 75% of the population has implemented these measures to safeguard organizational information resources from unauthorized access. This is clearly depicted in figure 4-9 below. Authorized users have different access control levels for enhanced security.

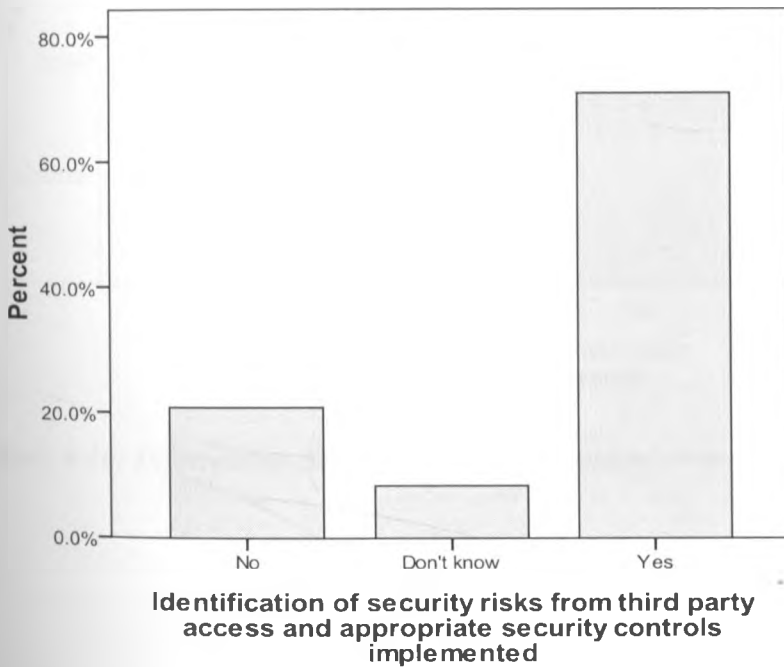


Figure 4-9: Security risks from third party access and appropriate security controls implementation

Information Security Policy Framework for a Manufacturing Firm

Information Security Policy Independent Review for Assurance

Organizations have now started to realize the importance of implementing independent review of security policies for assurance. Most of them are engaging Security Audit firms which have standard minimum security requirements to be implemented and can also advice on implementation of industry best practices. About 47% of the population has these assurance reviews conducted as illustrated in figure 4-10 below.

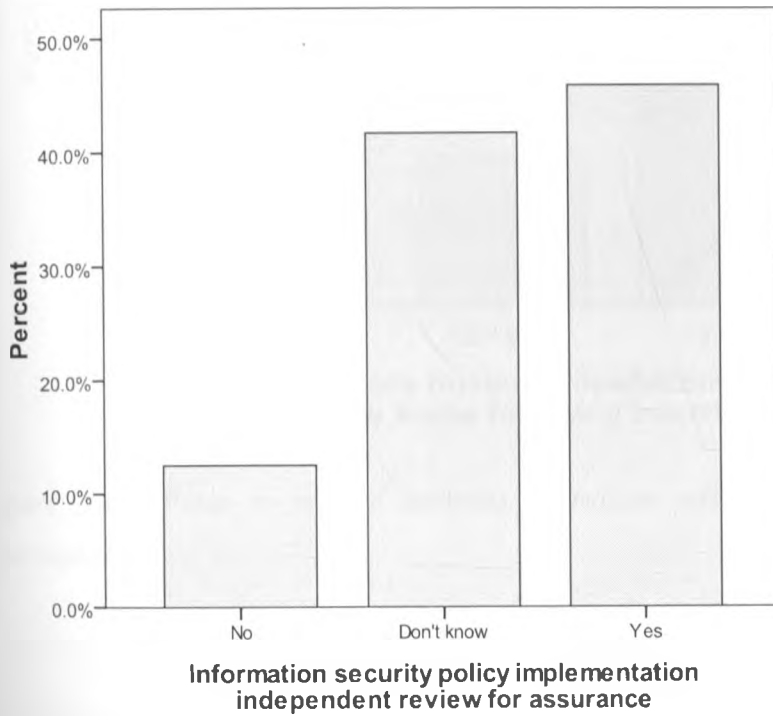
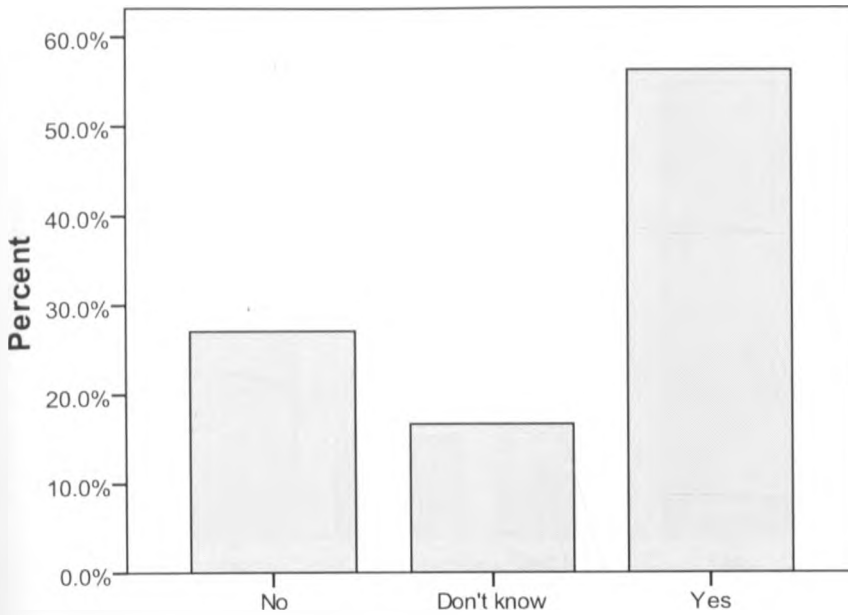


Figure 4-10: Information Security policy independent review for assurance

Information Security Policy Framework for a Manufacturing Firm

Plans to Restore Business Operations within Required Time Frame Following Interruptions



Plans to restore business operations within required time frame following interruptions

Figure 4-11: Plans to restore business operations within required time frame following interruptions

55% of the organizations have implemented plans to restore business operations within required time frames following interruptions as shown in figure 4-11. Such organizations have elaborate business continuity plans to ensure minimum business interruptions.

Policy to Account for Risks of Working with Mobile Computing Facilities

With an increase of mobile computing, many organizations are integrating in their Security Policies, measures to account for risks of working with mobile computing facilities like laptops, palmtops, notebooks etc. 45% of the population has implemented such measures to give access

Information Security Policy Framework for a Manufacturing Firm

to authorized mobile workers at the same time protecting information resources illustrated in figure 4-12 below.

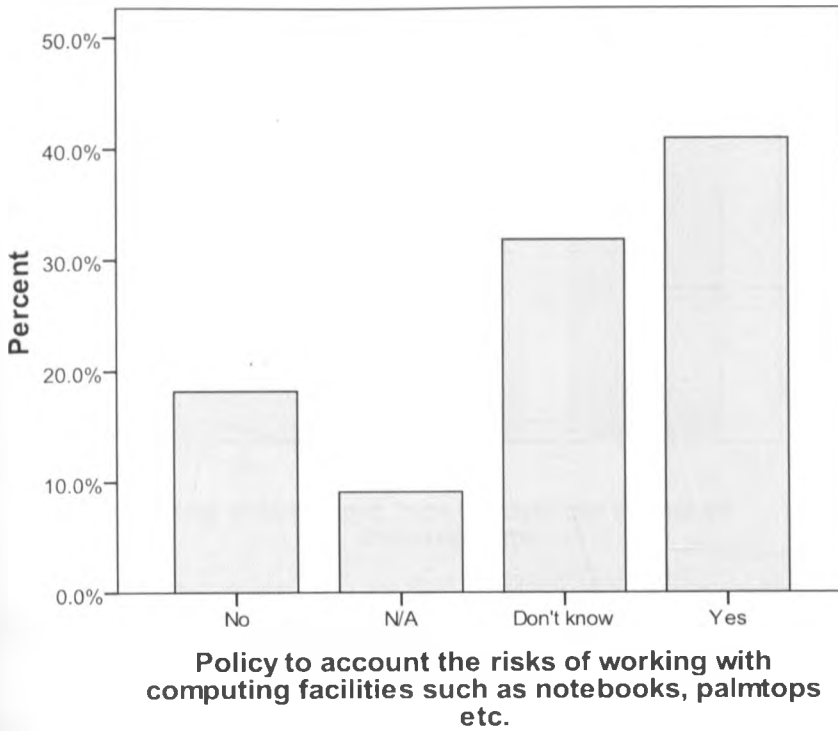


Figure 4-12: Policy to account for risks of working with mobile computing facilities

Risk Assessment to Determine the Impact of Interruptions

78% of the organizations undertake risk assessment to determine the impact of interruptions which is clearly illustrated in figure 4-12. Many organizations have realized the importance of business continuity planning to minimize interruptions on business operations. A majority of the organizations appreciate the fact that business interruptions can lead to massive losses and hence have invested in Information Security for minimal interruptions.

Information Security Policy Framework for a Manufacturing Firm

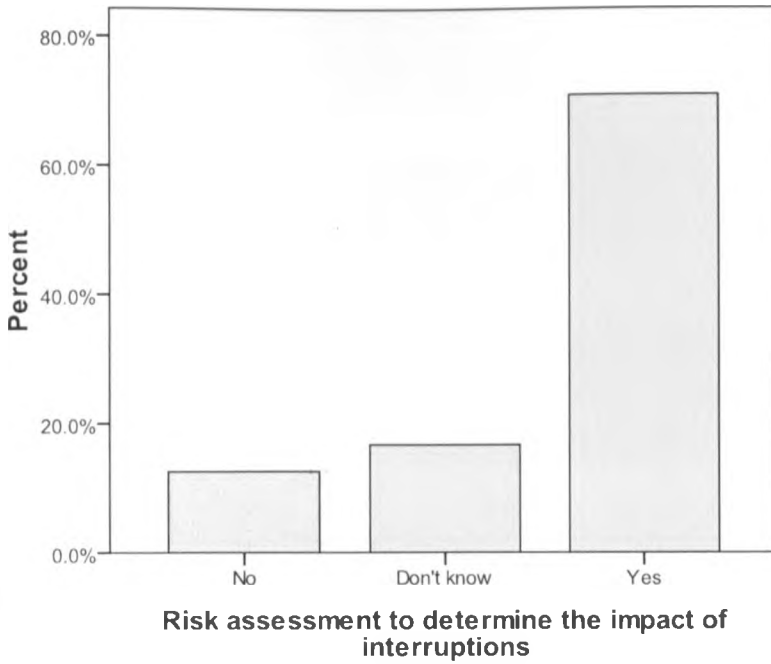


Figure 4-13: Risk assessment to determine the impact of interruptions

Regular Checking for Compliance with Security Implementation Standards

Only 43% of the population has put in place measures to regularly check their security policies for compliance with security implementation standards as illustrated in figure 4-13. Most organizations have already implemented Information Security policies and have now started enforcing industry best practices.

Information Security Policy Framework for a Manufacturing Firm

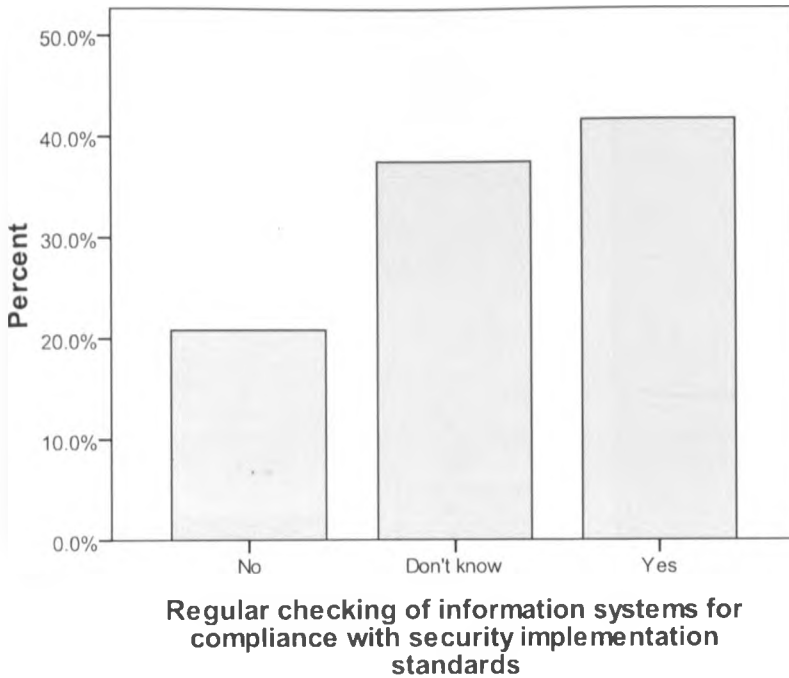


Figure 4-14: Regular checking for compliance with security implementation standards

48% of the organizations have considered all organizational areas to ensure compliance with security policy standards and procedures as illustrated in figure 4-14. All business units have a measurably high degree of business continuity planning competency. Complex business protection strategies are formulated and tested successfully.

Access to System Audit Tools Such as Software Protected to Prevent Possible Misuse or Compromise

72% of the companies have reinforced their security systems with system audit tools which are software protected and controlled to prevent possible misuse or compromise as shown in figure 4-15. Such systems have audit trails or logs that log all events performed for later review and enforcing appropriate action.

Information Security Policy Framework for a Manufacturing Firm

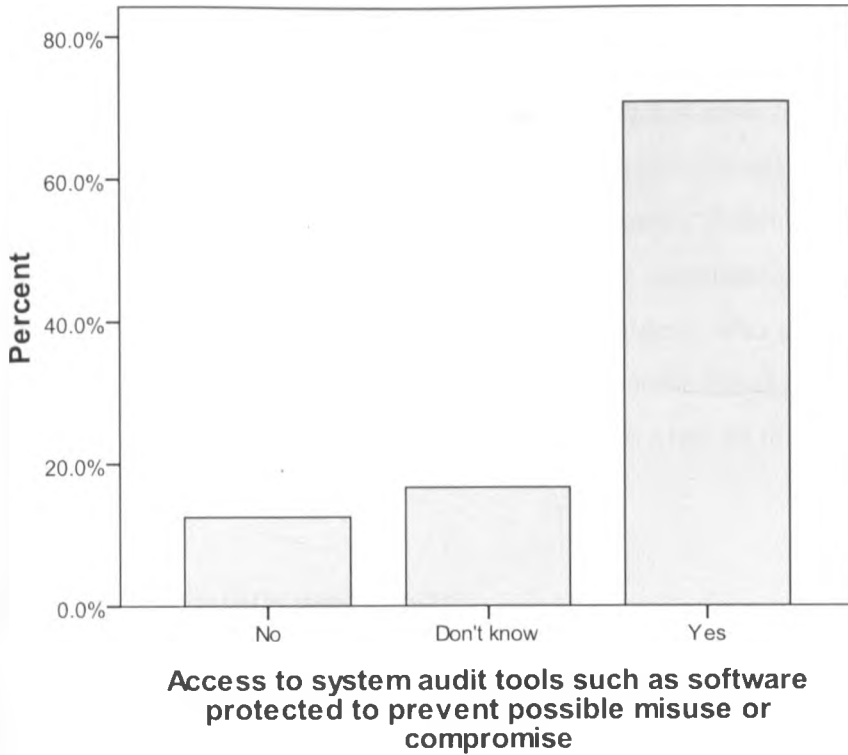


Figure 4-15: Access to system audit tools such as software protected to prevent possible misuse or compromise

From the frequency representation of the selected information security topics, it can be seen that many organizations have or are in the process of implementing security policies. The scenario has been facilitated by technological advancements, recognition of ICT by senior management as a necessary tool in realizing business goals and objectives, and a mandatory audit and legal requirement for information security implementations.

4.2.2 Cross Tabulation Analysis

A **cross tabulation** (often abbreviated as **cross tab**) in this analysis has been used to display the joint distribution of two or more variables. Cross tabulations are usually presented as a contingency table in a matrix format. Whereas a frequency distribution provides the distribution of one variable, a contingency table describes the distribution of two or more variables simultaneously. Each cell shows the number of respondents who gave a specific combination of responses, that is, each cell contains single cross tabulation. Cross tabulation analysis can also be accompanied with corresponding bar chart for a quick view of the findings as illustrated in the figures 4-21 to 4-27 below.

Cross tabs are frequently used because:

1. They are easy to understand. They appeal to people who do not want to use more sophisticated measures.
2. They can be used with any level of data: nominal, ordinal, interval, or ratio. Cross tabs treats all data as if it is nominal.
3. A table can provide greater insight than single statistics.
4. It solves the problem of empty or sparse cells.
5. Cross tabs are simple to conduct.

Information Security Policy Framework for a Manufacturing Firm
Crosstabs Analysis Supported by Bar Charts

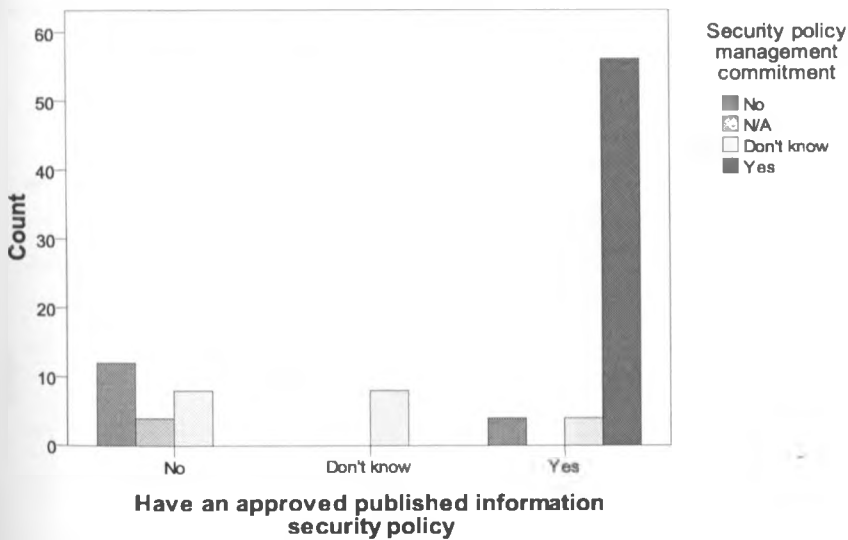
*Table 4-1: Have an approved published information security policy * Security policy management commitment*

Cross tabulation

Count

	Security policy management commitment				Total
	No	N/A	Don't know	Yes	
Have an approved published information security policy					
No	12	4	8	0	24
Don't know	0	0	8	0	8
Yes	4	0	4	56	64
Total	16	4	20	56	96

*Figure 4-16: Have an approved published information security policy * Security policy management commitment*



Information Security Policy Framework for a Manufacturing Firm

Cross tabulation of having an approved published information security policy and Security policy management commitment shows a total count of 56 out of 96 positive responses (Yes) which indicate a strong relationship.

*Table 4-2: Security policy management commitment * Reviews in response to changes affecting original assessment*

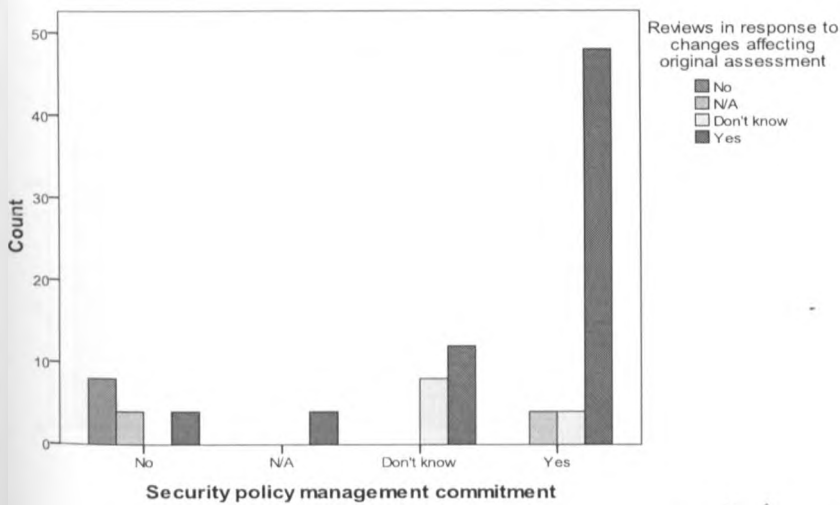
Cross tabulation

Count

		Reviews in response to changes affecting original assessment				Total
		No	N/A	Don't know	Yes	
Security policy management commitment	No	8	4	0	4	16
	N/A	0	0	0	4	4
	Don't know	0	0	8	12	20
	Yes	0	4	4	48	56
Total		8	8	12	68	96

*Figure 4-17: Security policy management commitment * Reviews in response to changes affecting original assessment*

Bar Chart



Information Security Policy Framework for a Manufacturing Firm

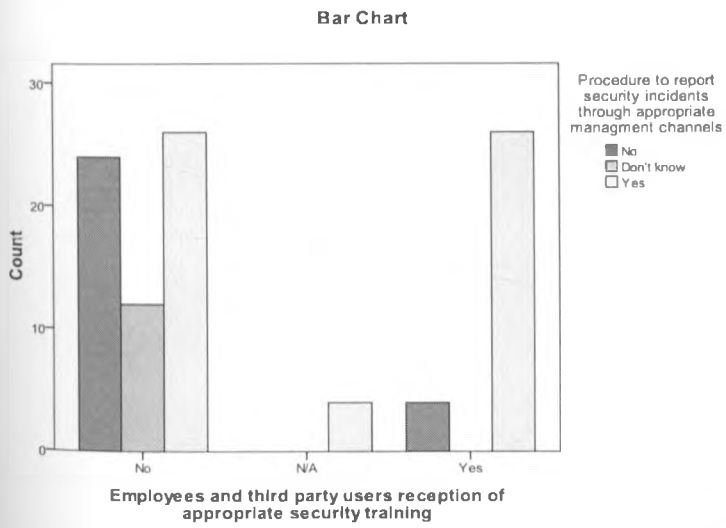
Cross tabulation of having security policy management commitment and reviews in response to changes affecting original assessment shows a total count of 48 out of 96 positive responses (Yes) which indicate a moderate relationship.

*Table 4-3: Employees and third party users reception of appropriate security training * Procedure to report security incidents through appropriate management channels*

Cross tabulation

Count	Procedure to report security incidents through appropriate management channels			Total	
	No	Don't know	Yes		
Employees and third party users reception of appropriate security training	No	24	12	26	62
	N/A	0	0	4	4
	Yes	4	0	26	30
Total		28	12	56	96

*Figure 4-18: Employees and third party users' reception of appropriate security training * Procedure to report security incidents through appropriate management channels*



Information Security Policy Framework for a Manufacturing Firm

Cross tabulation of employees and third party users' reception of appropriate security training and procedure to report security incidents through appropriate management channels gives 26 positive counts out of possible 96 that indicate moderate association of these information security items.

Information Security Policy Framework for a Manufacturing Firm

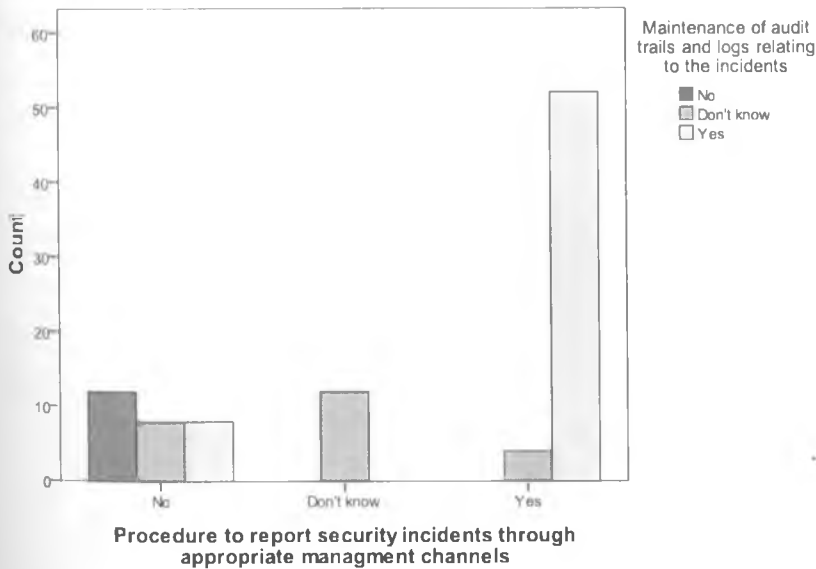
**Table 4-4: Procedure to report security incidents through appropriate management channels *
Maintenance of audit trails and logs relating to the incidents**

Cross tabulation

Count		Maintenance of audit trails and logs relating to the incidents			Total
		No	Don't know	Yes	
Procedure to report security incidents through appropriate management channels	No	12	8	8	28
	Don't know	0	12	0	12
	Yes	0	4	52	56
Total		12	24	60	96

**Figure 4-19: Procedure to report security incidents through appropriate management channels *
Maintenance of audit trails and logs relating to the incidents**

Bar Chart



Information Security Policy Framework for a Manufacturing Firm

Cross tabulation of procedure to report security incidents through appropriate management channels and maintenance of audit trails and logs relating to the incidents give 52 positive counts out of possible 96 which indicate a strong association of these information security items.

*Table 4-5: Maintenance of audit trails and logs relating to the incidents * Procedure to report security weakness and malfunctions, or threats to systems or services*

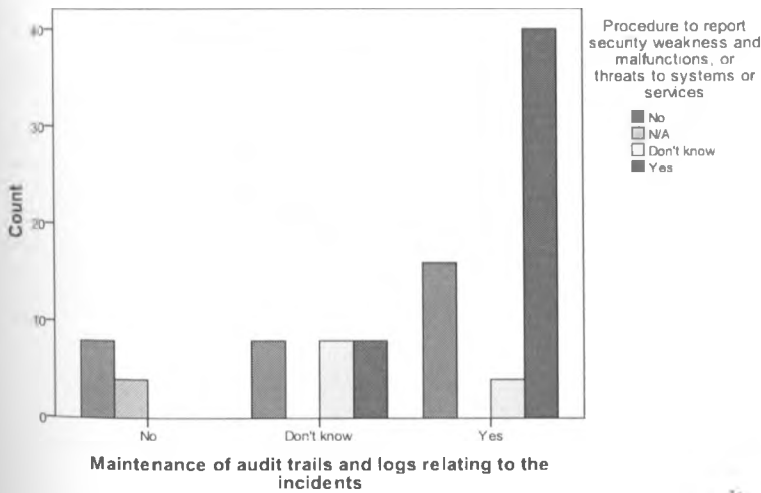
Cross tabulation

Count

	Procedure to report security weakness and malfunctions, or threats to systems or services				Total
	No	N/A	Don't know	Yes	
Maintenance of audit trails No and logs relating to the incidents	8	4	0	0	12
Don't know	8	0	8	8	24
Yes	16	0	4	40	60
Total	32	4	12	48	96

*Figure 4-20: Maintenance of audit trails and logs relating to the incidents * Procedure to report security weakness and malfunctions, or threats to systems or services*

Bar Chart



Information Security Policy Framework for a Manufacturing Firm

Cross tabulation of maintenance of audit trails and logs relating to the incidents and procedure to report security weakness and malfunctions, or threats to systems or services 40 positive counts out of 96 which is a moderate association of the respective security components.

Information Security Policy Framework for a Manufacturing Firm

Table 4-6: Management committee to set direction and support organizational security initiatives * Advice and contacts with law enforcement authorities, regulatory bodies, I.S. providers

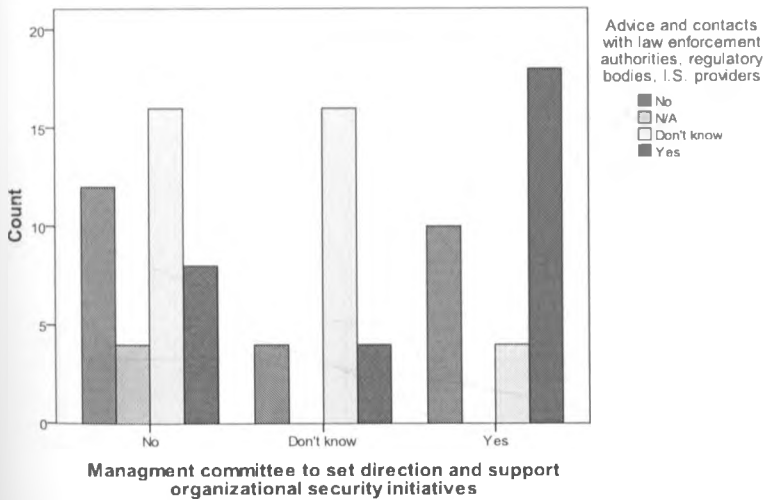
Cross tabulation

Count

	Advice and contacts with law enforcement authorities, regulatory bodies, I.S. providers				Total
	No	N/A	Don't know	Yes	
Management committee to No	12	4	16	8	40
set direction and support Don't know	4	0	16	4	24
organizational security Yes	10	0	4	18	32
initiatives					
Total	26	4	36	30	96

Figure 4-21: Management committee to set direction and support organizational security initiatives * Advice and contacts with law enforcement authorities, regulatory bodies, I.S. providers

Bar Chart



Cross tabulation of Maintenance of audit trails and logs relating to the incidents * Procedure to report security weakness and malfunctions, or threats to systems or services gives 18 positive counts of the 96 possible counts. The relationship between the security components is not strong.

Information Security Policy Framework for a Manufacturing Firm

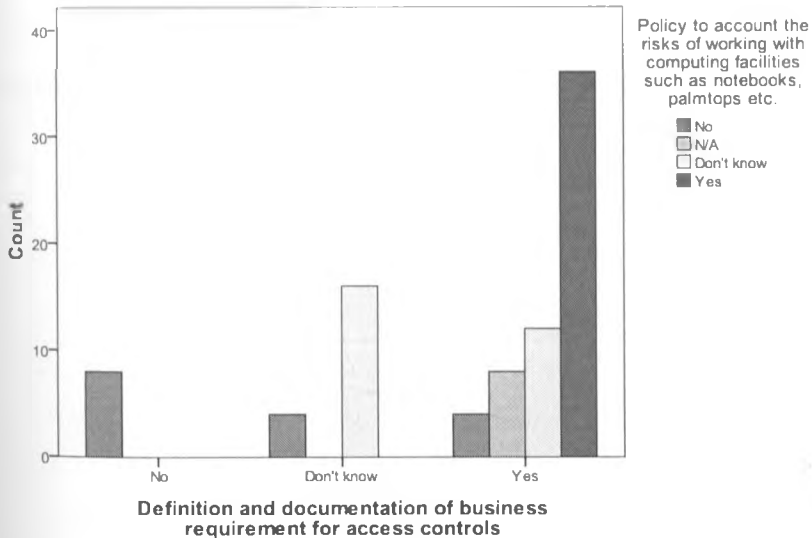
Table 4-7: Definition and documentation of business requirement for access controls * Policy to account the risks of working with computing facilities such as notebooks, palmtops etc.

Cross tabulation

Count		Policy to account the risks of working with computing facilities such as notebooks, palmtops etc.				Total
		No	N/A	Don't know	Yes	
	Definition and documentation No of business requirement for access controls	8	0	0	0	8
	Don't know	4	0	16	0	20
	Yes	4	8	12	36	60
	Total	16	8	28	36	88

Figure 4-22: Definition and documentation of business requirement for access controls * Policy to account the risks of working with computing facilities such as notebooks, palmtops etc.

Bar Chart



Information Security Policy Framework for a Manufacturing Firm

Cross tabulation of definition and documentation of business requirement for access controls and policy to account the risks of working with computing facilities gives a strong association of 36 counts out of 96.

4.2.3 Correlation Analysis

Correlation is one of the most common and most useful statistics. A correlation is a single number that describes the degree of relationship between two variables. In statistics, correlation (often measured as a correlation coefficient, ρ) indicates the strength and direction of a linear relationship between two random variables.

Further analysis of the degree of relationship between various information security components can be seen in the measure of correlations as illustrated below. From the findings, it is shown that **correlations are significant** in almost all cases. The significance in correlations, show that the various Information Security components are strongly interdependent.

This study used Pearson correlation coefficient and Spearman's rho tests to analyze and present correlations.

Information Security Policy Framework for a Manufacturing Firm

Table 4-8: Have an approved published information security policy & Security policy management commitment

Correlations

	Have an approved published information security policy	Security policy management commitment
Have an approved published information security policy	1	.827**
Pearson Correlation		.000
Sig. (2-tailed)		
N	96	96
Security policy management commitment	.827**	1
Pearson Correlation		.000
Sig. (2-tailed)		
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Have an approved published information security policy	Security policy management commitment
Spearman's rho	1.000	.809**
Have an approved published information security policy		.000
Correlation Coefficient		
Sig. (2-tailed)		
N	96	96
Security policy management commitment	.809	1.000
Correlation Coefficient		.000
Sig (2-tailed)		
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlation analysis of Having an approved published information security policy & Security policy management commitment is significant at 0.01 level with 0.827 and 0.809 using Pearson correlation coefficient and Spearman's rho test respectively.

Information Security Policy Framework for a Manufacturing Firm

Table 4-9: Communicated as appropriate to all employees & Management committee to set direction and support organizational security initiatives

Correlations

	Communicated as appropriate to all employees	Management committee to set direction and support organizational security initiatives
Communicated as appropriate to all employees	1	.726**
as Pearson Correlation Sig (2-tailed)		.000
N	96	96
Management committee to set direction and support organizational security initiatives	.726**	1
as Pearson Correlation Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Communicated as appropriate to all employees	Management committee to set direction and support organizational security initiatives
Spearman's rho	1.000	.753**
Communicated as appropriate to all employees		.000
as Correlation Coefficient Sig (2-tailed)		
N	96	96
Management committee to set direction and support organizational security initiatives	.753**	1.000
as Correlation Coefficient Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed)

Communication as appropriate to all employees & Management committee to set direction and support organizational security initiatives have significant correlations at 0.01 level of 0.726 using Pearson Correlation Coefficient and 0.753 using Spearman's rho test.

Information Security Policy Framework for a Manufacturing Firm

Table 4-10: Specialist information security advice where appropriate & Information security policy implementation independent review for assurance

Correlations

	Specialist information security advice where appropriate	Information security policy implementation independent review for assurance
Specialist information security advice where appropriate	1	.491**
Pearson Correlation		.000
Sig (2-tailed)		
N	96	96
Information security policy implementation independent review for assurance	.491**	1
Pearson Correlation		
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Specialist information security advice where appropriate	Information security policy implementation independent review for assurance
Spearman's rho	1.000	.568**
Specialist information security advice where appropriate		.000
Correlation Coefficient		
Sig (2-tailed)		
N	96	96
Information security policy implementation independent review for assurance	.568**	1.000
Correlation Coefficient		
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlation of Specialist information security advice where appropriate & Information security policy implementation independent review for assurance is significant at the 0.01 level using Pearson Correlation Coefficient and Spearman's rho test of 0.491 and 0.568 respectively.

Information Security Policy Framework for a Manufacturing Firm

Table 4-11: Identification of security risks from third party access and appropriate security controls implemented & A formal contract with third parties with all security requirements to ensure compliance

Correlations

	Identification of security risks from third party access and appropriate security controls implemented	A formal contract with third parties with all security requirements to ensure compliance
Identification of security risks from third party access and appropriate security controls implemented	1	.597**
Sig (2-tailed)		.000
N	96	96
A formal contract with third parties with all security requirements to ensure compliance	.597**	1
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Identification of security risks from third party access and appropriate security controls implemented	A formal contract with third parties with all security requirements to ensure compliance
Spearman's rho	1.000	.534**
Identification of security risks from third party access and appropriate security controls implemented		.000
Sig. (2-tailed)		
N	96	96
A formal contract with third parties with all security requirements to ensure compliance	.534**	1.000
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

There is a significant correlation between Identification of security risks from third party access and appropriate security controls implemented & A formal contract with third parties with all security requirements to ensure compliance at the 0.01 level of 0.597 and 0.534 using Pearson Correlation Coefficient and Spearman's rho test respectively.

Information Security Policy Framework for a Manufacturing Firm

Table 4-12: Effective operational controls established where necessary & Controls to safeguard confidentiality and integrity of data processing over the public networks

Correlations

	Effective operational controls established where necessary	Controls to safeguard confidentiality and integrity of data processing over the public networks
Effective operational controls established where necessary	1	.585**
Sig (2-tailed)		.000
N	96	96
Controls to safeguard confidentiality and integrity of data processing over the public networks	.585**	1
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Effective operational controls established where necessary	Controls to safeguard confidentiality and integrity of data processing over the public networks
Spearman's rho	1.000	.515**
Effective operational controls established where necessary		.000
Sig (2-tailed)		
N	96	96
Controls to safeguard confidentiality and integrity of data processing over the public networks	.515**	1.000
Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

There is a significant correlation between Effective operational controls-established where necessary & Controls to safeguard confidentiality and integrity of data processing over the public networks at 0.01 level of 0.585 and 0.515 using Pearson Correlation Coefficient and Spearman's rho test respectively.

Information Security Policy Framework for a Manufacturing Firm

Table 4-13: Management of information processing facilities by an external party & Identification of risks associated with such management hence appropriate controls

Correlations

	Management of information processing facilities by an external party	Identification of risks associated with such management hence appropriate controls
Management of information processing facilities by an external party	1	.774
Pearson Correlation Sig (2-tailed)		.000
N	96	96
Identification of risks associated with such management hence appropriate controls	.774	1
Pearson Correlation Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Management of information processing facilities by an external party	Identification of risks associated with such management hence appropriate controls
Spearman's rho	1.000	.722
Management of information processing facilities by an external party		.000
Correlation Coefficient Sig (2-tailed)		
N	96	96
Identification of risks associated with such management hence appropriate controls	.722	1.000
Correlation Coefficient Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

There is a significant correlation between Management of information processing facilities by an external party & Identification of risks associated with such management hence appropriate controls at 0.01 level of 0.774 and 0.722 using Pearson Correlation Coefficient and Spearman's rho test respectively.

Information Security Policy Framework for a Manufacturing Firm

Table 4-14: Regular checking of information systems for compliance with security implementation standards & Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions

Correlations

	Regular checking of information systems for compliance with security implementation standards	Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions
Regular checking of information systems for compliance with security implementation standards	1	.640**
Pearson Correlation Sig (2-tailed)		.000
N	96	96
Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions	.640**	1
Pearson Correlation Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

Correlations

	Regular checking of information systems for compliance with security implementation standards	Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions
Spearman's rho	1.000	.601**
Regular checking of information systems for compliance with security implementation standards	1	
Correlation Coefficient Sig (2-tailed)		.000
N	96	96
Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions	.601**	1.000
Correlation Coefficient Sig (2-tailed)	.000	
N	96	96

** Correlation is significant at the 0.01 level (2-tailed).

There is a significant correlation between Regular checking of information systems for compliance with security implementation standards & Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions at 0.01 level of 0.640 and 0.601 using Pearson Correlation Coefficient and Spearman's rho test respectively.

*Information Security Policy Framework for a Manufacturing Firm***4.3 Critic of the Current Information Security Models**

There are models that have been recommended universally, but may not be practical in all situations due to differences in industrial and technological developments. Most models have been developed in the developed world which is an ideal environment for the practical implementation of the security frameworks. In other developing economies there are challenges of infrastructure, telecommunications among other things that may limit similar security implementations.

Based on the inherent strengths and weaknesses of an organization, risk handling strategies have to be modified to enable managers to make their programs and projects successful. The concepts and skills need to be woven into day-to-day business decision making. They must be self correcting and self sustaining for continuous improvement of products and services. Policies must therefore be customized for them to be practical and effective.

Information security legal and statutory requirements may vary from country to country. Legislative requirements may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow). The compliance implementations therefore will vary from one country to another. This limits the ability to standardize and apply a universal information security policy.

Most of these developed and acknowledged security policy models are base models with constituents for most situations; they do not provide solutions for all situations all the time. They need to be adapted, customized and extended based on the risk trends in the organizational and business needs.

Risk models have generally been reactive, silo-based and have resolved risks in a project's immediate context. There has never been a focus on learning from the mistakes or experiences of others in the organization. Organizations have avoided risky projects and have even ignored

Information Security Policy Framework for a Manufacturing Firm

possible opportunities due to their conservative approach. A holistic or enterprise outlook can change the mindset of organizations. They may explore and venture into new opportunities to reduce time-to-market, exploit new product lines and enable participants to deal with risks in a mature way.

Kenya like most of the other developing countries is still in the process of developing an ICT governance policy which will determine the requirement and compliance of an appropriate information security policy. It is hoped that after formulation of an ICT policy, standards and procedures of Kenyan ICT infrastructure will be well defined.

Management of most business operations especially in the emerging economies focuses more on the business operations profitability and legal and statutory requirements other than Information and Communication Technology. This approach limits their participation in information security arrangements and hence limiting the benefits that would have been derived from well developed and implemented information security policies.

The approach to information security implementation has been reactive more than proactive. The majority of Kenyan organizations have not prioritized information security implementations until business operations are adversely affected by security threats. This causes organizations to lose business opportunities in an effort to handle the incidences. Their businesses are also at risk due to lack of confidentiality, integrity and availability.

Information Security Policy Framework for a Manufacturing Firm

5 Information Security Policy Framework for a Manufacturing Firm

In developing security policies, it was most effective to use an established template. Developing a policy from scratch may have omitted certain areas inadvertently. A wealth of sources can be tapped for input into a security policy from established standards and organizations like:

- a) American Institute of Certified Public Accountants (AICPA)
- b) BS 7799
- c) Consultant firms (e.g. KPMG, PricewaterhouseCoopers, Ernest and Young)
- d) Institute of Certified Public Accountants of Kenya (ICPAK)
- e) Internet Engineering Task Force (IETF) security handbooks
- f) ISO/IEC 27002:2005
- g) Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
- h) The SANS Institute
- i) System security Engineering, Capability Maturity Model
- j) US General Accounting Office (GAO), Federal Information Systems Control Audit Manual (FISCAM)
- k) US National Security Agency (NSA)
- l) US NIST

In establishing and maintaining security policies the following steps should be considered (ISACA, CISM Review Manual, 2009);

- a) Implementing a policy and process of development and maintenance
- b) Identifying the personnel responsible for various aspects of the security policy and approval
- c) Researching existing organizational policies, such as personnel
- d) Implementing a review of the security policy, into the organizations change management process
- e) Developing awareness program to educate the organizations employees

Information Security Policy Framework for a Manufacturing Firm

The information security manager should understand how to ensure that security policies align with the enterprise business objectives. Methods to ensure this happens include;

- a) Determining whether or not information security investment is proportionate with organization's risk profile and business objectives
- b) Determining the information/data classification required of the organization, so that security policies can be implemented to protect them
- c) Determining whether or not the security policies are appropriately designed, implemented and enforced to protect the organization's information

5.1 Functions and content of essential elements of an Information Security program

Essential elements of an information security program must be well understood for proper management and administration. Security program essential elements are; policies, standards, procedures and guidelines.

Policies – High-level statements of concepts and expectations. A policy can be considered the “constitution” of governance. Policies in most cases remain fairly static.

Standards – Definition of metrics used to determine the correctness of a thing or process; a set of rules or specifications when taken together define a software or hardware. A standard is also an acknowledged basis for comparing or measuring something. Standards must change as requirements and technologies change.

Procedures – Procedures must include detailed steps needed to accomplish specific tasks. They should include expected outcomes and displays and required conditions towards execution of the procedure.

Information Security Policy Framework for a Manufacturing Firm

Guidelines – A suggested action or recommendation related to an area of information security policy that is intended to supplement a procedure. The implementation of guidelines is encouraged but not enforced.

To be effective, security must address the entire processes from end to end, both physical and technical. It is of little benefit to an organization if a secure IT system is used to process fraudulent orders. To ensure that all relevant elements of security are addressed in an organizational security strategy, all the major areas of an accepted standard like ISO/IEC 27002:2005 on which this document is based, can provide a useful framework to gauge comprehensiveness.

5.2 Information Security Policy Implementation

Information security policy implementation will provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Establishing and maintaining information security policies that support business goals and objectives is the responsibility of the Information Security Manager. A process will be in place for the development and maintenance of security policies. An organization need to ensure that these policies become an integral part of its overall governance.

Standards must then be reviewed and modified as needed to address the changes of the policies. Information security policies that support business goals and objectives are normally approved by the board of directors. Security procedures and guidelines are derived from security policies.

Information Security Policy Framework for a Manufacturing Firm

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
- b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - 1) compliance with legislative, regulatory, and contractual requirements;
 - 2) security education, training, and awareness requirements;
 - 3) business continuity management;
 - 4) consequences of information security policy violations;
- e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

Information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable.

The information security policy might be part of a general policy document. If the information security policy is distributed outside the organization care should be taken not to disclose sensitive information.

5.3 Recommended Information Security Policy Model

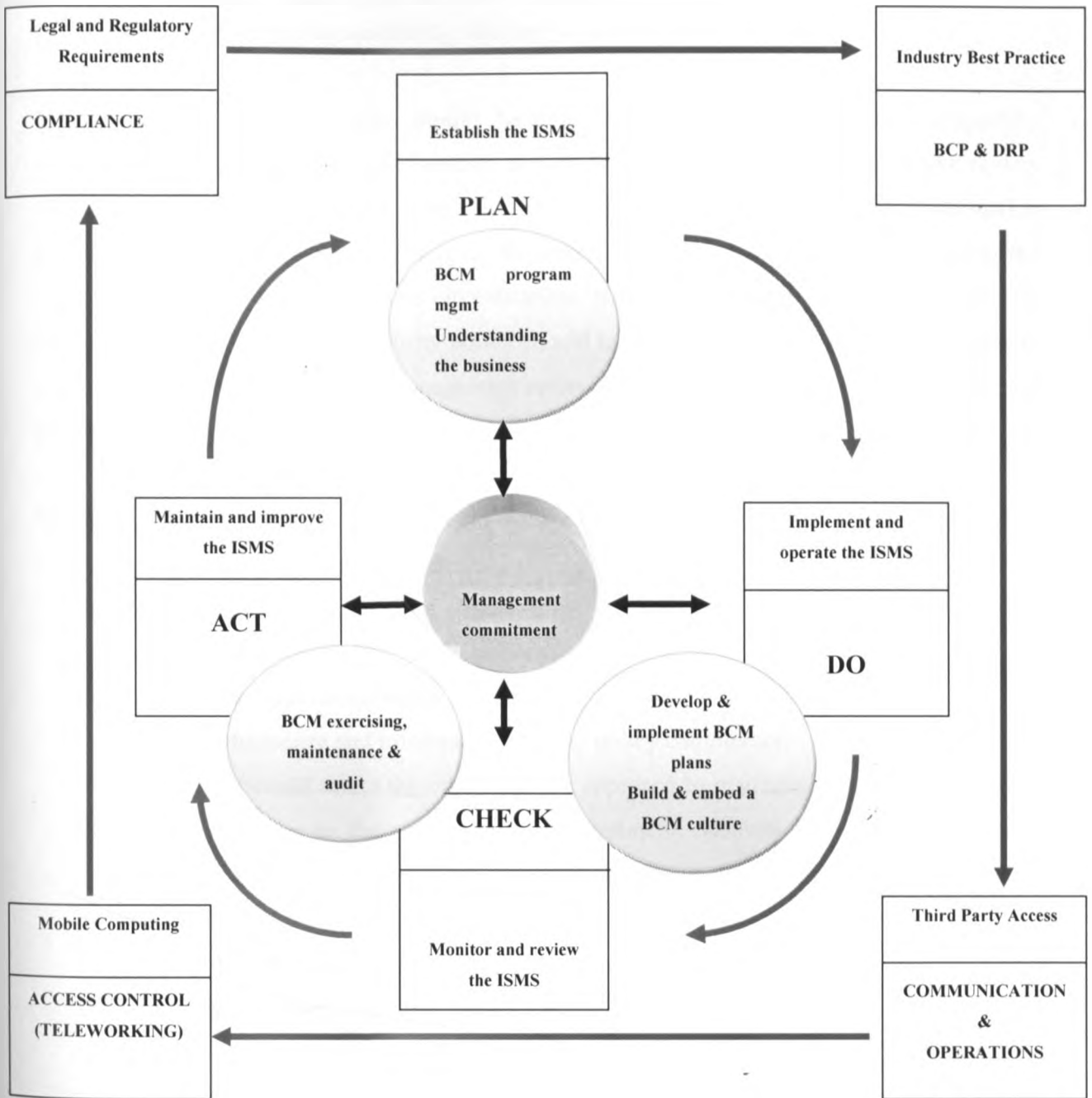


Figure 5-1: Recommended Information Security Policy Model

Information Security Policy Framework for a Manufacturing Firm

Information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment. The review of the information security policy should take account of the results of management reviews. There should be defined management review procedures, including a schedule or period of the review.

The input to the management review should include information on:

- a) feedback from interested parties;
- b) results of independent reviews;
- c) status of preventive and corrective actions;
- d) results of previous management reviews;
- e) process performance and information security policy compliance;
- f) changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;
- g) trends related to threats and vulnerabilities;
- h) reported information security incidents;
- i) recommendations provided by relevant authorities.

The output from the management review should include any decisions and actions related to:

- a) improvement of the organization's approach to managing information security and its processes;
- b) improvement of control objectives and controls;

Information Security Policy Framework for a Manufacturing Firm

- c) improvement in the allocation of resources and/or responsibilities.

A record of the management review should be maintained. Management approval for the revised policy should also be obtained.

6 CONCLUSION AND RECOMMENDATIONS

In Kenya most organizations have acknowledged the importance of implementation of a suitable information security policy. Although only a few organizations have effectively implemented an appropriate information security policy and are constantly reviewing and auditing it. They are further adjusting the policy to industry best practices and standards with direct involvement and support of senior management. They have also gone further to ensure that the information security policy is compliant with legal and statutory requirements. These organizations are deriving the benefits of having an effective information security policy implementation. They are able to make timely and informed decisions because of information availability, integrity and confidentiality.

The majority of Kenyan organizations have not implemented practical information security policies. They are yet to come up with an information security policy that is effective for the organization. A number of companies have information security policy documents that are never reviewed to establish whether they are practical in their setup. Similarly statutory compliance of these policies may not be adequate. However, a number of organizations are now attempting to come up with more practical and compliant information security policies.

Boards and management alike are now ensuring that IT is aligned with organizational strategies and that these strategies take proper advantage of IT opportunities. An important facet of IT governance is information security governance. Information security governance provides assurance that information assets are given a level of protection commensurate with their value or with the risk their compromise poses to the organization. Therefore executive management committees are now ensuring that the definition of roles and responsibilities throughout the organization include information security.

For practical implementation, Management should fully be involved in the implementation process. They should also support information security efforts and allocate enough resources for

Information Security Policy Framework for a Manufacturing Firm

such projects. They must be involved in the evaluation and review of the information security policy implementations to check compliance and recommend appropriate improvements.

Information security management is, to an increasing extent, a business issue and a legal requirement, and not only a technology issue. On the basis of identified and prioritized information resources that need protection, security policies and baselines are now being developed and implemented. Information security baselines represent the minimum acceptable security implemented to protect information resources. Baselines are normally set using commonly accepted, industrial wide standards, such as ISO/IEC 27002:2005, legal and regulatory requirements, and decisions by the business owners on what level of risk the organization may be willing to accept.

Information Technology is now widely recognized as a valued organizational resource. IT is now being acknowledged and used by most organizations for information processing, analysis and storage for effective decision making. This is also making organizations have a competitive advantage in the evolving business world. This calls for implementation of a practical information security policy to guard and protect this valued resource.

It is recommended that for effective implementation of an information security policy, there should be specialist support. Either an information security specialist(s) must be charged with information security responsibility or such services can be outsourced to specialist information security firms.

For information security policy implementation to be effective there should be well documented review procedures. The reviews should be carried out periodically by a respected and acknowledged independent party. This will ensure information security best practices and the necessary compliance procedures. With these properties the security policy will be more responsive and resilient to changing environments.

Information Security Policy Framework for a Manufacturing Firm

This information Security Policy Framework can be developed further and generalized for any kind of business establishment.

7 REFERENCES AND BIBLIOGRAPHY

1. 360 Degree Risk Management Model, www.infosys.com
2. British Standards Institute (BSI), Publicly Available Specification PAS 56:2003, "Guide to Business Continuity Management" ISBN 0-580-41370-5 (<http://www.standardsdirect.org/pas56.htm>)
3. ISACA, 2009, Certified Information Security Manager Review Manual 2009
4. ISACA, IS Standards, Guidelines and Procedures for Auditing and Control Professionals
5. ISO/IEC 27002: 2005 Information Technology – Security Techniques – Code of Practice for Information Security Management
6. ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards
7. ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
8. ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security
9. ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model
10. ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services
11. ISO/IEC TR 18044 Information technology – Security techniques – Information security incident
12. IT Governance Institute, Control Objectives for Information and related Technology (COBIT), www.isaca.org/cobit
13. IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, www.itgi.org
14. <http://www.pas56.com/contents.htm>
15. <http://virtual-corp.net/html>

8 Appendices

Appendix A

Information Security Policy Questionnaire

How to complete the Questionnaire

Kindly answer these questions to assist in compiling an Information Security Report.

The questionnaire is divided into **seven** sections. Each section focuses on a specific area of security, based on the requirements included in the Data Security Standard. For any questions where **N/A** is marked, a **brief explanation** should be given.

TIPS

Be honest.

There is no right or wrong answer. Ask for help and if you don't know you may guess.

A		Information Security Policy	YES	NO	Don't Know	N/A
1	Information security policy document	Do you have an approved published Information security policy?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is the policy communicated to all employees?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Does the security policy state management commitment?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Review and evaluation	Do you have someone responsible for Information Security maintenance and review according to a defined review process?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		How often do you review your information security policy in a year	<input checked="" type="checkbox"/>			

Information Security Policy Framework for a Manufacturing Firm

		Does the review take place in response to changes affecting original assessment, example: significant security incidents, changes to organizational or technical infrastructure?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B		Organizational Security				
1		Information Security Infrastructure				
	Management Information Security forum	Do you have a management committee to set the direction and support organizational security initiatives?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Information security coordination	Does the security committee represent all organizational units for a well coordinated implementation of controls?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Allocation of information security responsibilities	Are the security responsibilities well defined in a document?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Specialist information security advise	Do you obtain specialist information security advice where appropriate?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Co-operation between organizations	Do you have contacts with law enforcement authorities, regulatory bodies, information service providers to ensure appropriate action is quickly taken and advice obtained, in the event of a security incident?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Independent review of Information security	Is information security policy implementation reviewed independently on regular basis to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		Security of third party access				
	Identification of risks from third party access	Are security risks from third party access identified and appropriate security controls implemented?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

		Are the types of accesses identified, classified and reasons for access justified?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Security requirements in third party contracts	Is there a formal contract with third parties containing all security requirements to ensure compliance with the organization's security policies and standards?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is there a procedure to highlight and address third party information security compromises or weaknesses?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3		Accountability of assets				
	Inventory of assets	Do you maintain an inventory or register with important assets associated with each information system?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is each asset identified associated to an owner?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4		Information classification				
	Classification guidelines	Is there an Information classification scheme or guideline in place that can assist in determining how the information is to be handled and protected?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Information labeling and handling	Do you have a set of procedures defined for information labeling and handling in accordance with the classification scheme?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
C		Personnel security				
1		Security in job definition and Resourcing				
	Including security in job responsibilities	Are security roles and responsibilities as laid in organization's information security policy incorporated in job descriptions?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Confidentiality agreements	Are employees asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

	Terms and conditions of employment	Do the terms and conditions of the employment cover the employee's responsibility for information security?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		User training				
	Information security education and training	Do all employees in your organization and third party users (where relevant) receive periodic Information Security training?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		How often is the Information Security training conducted? Monthly, Quarterly, etc				
		Do they receive regular updates in organizational policies and procedures?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3		Responding to security incidents and malfunctions				
	Reporting security incidents	Is there a formal reporting procedure to report security incidents through management channels as quickly as possible?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Reporting security weaknesses	Does a formal reporting procedure or guideline exist for users, to report security weakness in, sw malfunctions, or threats to, systems or services?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Disciplinary process	Is there a formal disciplinary process in place for employees who have violated organizational security policies and procedures?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are audit trails and logs relating to the incidents maintained?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D		Physical and Environmental Security				
1		Secure Area				
	Physical Security Perimeter	Is there a physical security border facility implemented to protect the Information processing service?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

	Physical entry Controls	Do you have entry controls in place to allow only authorized personnel into various areas within organization?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Securing offices, rooms and facilities	Are rooms with Information processing services locked?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are the Information processing services protected from natural and man-made disruptions?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is your company information given only when absolutely required?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		General Controls				
	Clear Desk and clear screen policy	Is there a mechanism to protect a computer that is left unattended and is not in use?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are employees advised to leave confidential material in the form of paper documents, media etc., in a locked manner while unattended?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E		Communications and Operations Management				
1		Operational Procedure and responsibilities				
	Documented Operating procedures	Does the Security Policy have identified, documented operating procedures such as Back-up, Equipment maintenance etc?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Operational Change Control	Are all programs running on production systems subject to strict change control?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are audit logs maintained for changes made to the production programs?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Segregation of duties	Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

	Separation of Development and Operational facilities	Are the development and testing facilities isolated from operational facilities?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	External facilities management	Do you have any of the Information processing facility managed by an external company or contractor (third party)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are risks associated with such management identified in advance, discussed and appropriate controls incorporated into the contract?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		Network Management				
	Network Controls	Are effective operational controls such as separate network and system administration facilities established where necessary?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are responsibilities and procedures for management of remote equipment, including equipment in user areas established?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are there any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3		Business Requirements for Access Control				
	Access Control Policy	Have the business requirements for access control been defined and documented?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Does the Access control policy address the rules and rights for each user or a group of users?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are users and service providers given a clear statement of business requirements to be met by access controls?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

4		Mobile computing and teleworking				
	Mobile computing	Is there a formal policy adopted that takes into account the risks of working with computing facilities such as notebooks, palmtops etc., especially in unprotected environments?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Teleworking	Is there a policy, procedure and/ or standard to control teleworking activities, consistent with organization's security policy?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is there suitable protection of teleworking sites in place against threats such as theft of equipment, unauthorized disclosure of information etc.?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F		Business Continuity Management				
1		Aspects of Business Continuity Management				
	Business continuity Management process	Do you have a documented Business Continuity Plan?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is there a managed process in place for developing and maintaining business continuity throughout the organization?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Business continuity and impact analysis	Are events that can cause interruptions to business process identified, example: equipment failure, flood and fire?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is a risk assessment conducted to determine impact of such interruptions?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Have you developed a strategy plan based on the risk assessment results to determine an overall approach to business continuity?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

	Writing and implementing continuity plan	Are plans developed to restore business operations within the required time frame following an interruption or failure to business process?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Testing, maintaining and re-assessing business continuity plan	Are Business continuity plans tested regularly to ensure that they are up to date and effective?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are Business continuity plans maintained by regular reviews and updates to ensure their continuing effectiveness?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are procedures included within the organizations change management program to ensure that Business continuity matters are appropriately addressed?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G		Compliance				
1		Compliance with legal requirements				
	Identification of applicable legislation	Are you or anyone in your organization aware of information security legal/compliance requirements?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Are specific controls and individual responsibilities to meet these requirements defined and documented?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Intellectual property rights (IPR)	Are there procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights such as copyright, design rights, trade marks?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

		Are proprietary software products supplied under a license agreement that limits the use of the products to specified machines?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Safeguarding of Organizational records	Are important records of the organization protected from loss, destruction and falsification?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Data protection and privacy of personal information	Is there a management structure and control in place to protect data and privacy of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Prevention of misuse of Information processing facility	Is the use of information processing facilities for any non-business or unauthorized purpose, without management approval treated as improper use of the facility?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		At the log-on, is there a warning message presented on the computer screen indicating that the system being entered is private and that unauthorized access is not permitted?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Collection of evidence	Is the process of collecting evidence in accordance with legal and industry best practice?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		Reviews of Security Policy and technical compliance				
	Compliance with security policy	Do you conduct periodic reviews for your information security requirements?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		How often are the reviews conducted?				
		Who conducts the periodic reviews				
		Are all areas within the organization considered for regular review to ensure compliance with security policy, standards and procedures?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm

	Technical compliance checking	Are information systems regularly checked for compliance with security implementation standards?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Is technical compliance check carried out by, or under the supervision of, competent, authorized persons?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3		System audit considerations				
	System audit controls	Are audit requirements and activities involving checks on operational systems carefully planned and agreed to minimize the risk of disruptions to business process?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Protection of system audit tools	Is access to system audit tools such as software or data files protected to prevent any possible misuse or compromise?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Security Policy Framework for a Manufacturing Firm
Appendix B

Information Security Policy PASW or SPSS Editor

NAME	TYPE	WIDTH	DEC	LABEL	VALUES	MISSING	COLUMNS	ALIGN	MEASURE
ID	String	8	0	Name of Company	None	None	8	Left	Nominal
INFOSEC	Numeric	8	0	Have an approved published information security policy	{0, No}...	None	8	Left	Nominal
Communicate	Numeric	8	0	Communicated as appropriate to all employees	{0, No}...	None	8	Left	Nominal
MGTCOMIT	Numeric	8	0	Security policy management commitment	{0, No}...	None	8	Left	Nominal
Responsibility	Numeric	8	0	Responsibility for information security maintenance	{0, No}...	None	8	Left	Nominal
Review	Numeric	8	0	Reviews in response to changes affecting original assessment	{0, No}...	None	8	Left	Nominal
COMMITTE	Numeric	8	0	Management committee to set direction and support organizational security initiatives	{0, No}...	None	8	Left	Nominal
COMMREPR	Numeric	8	0	Security committee representation of all organizational units for a coordinated implementation of controls	{0, No}...	None	8	Left	Nominal
DEFRESPO	Numeric	8	0	Security responsibilities definition in a document	{0, No}...	None	8	Left	Nominal
SPECLIST	Numeric	8	0	Specialist information security advice where appropriate	{0, No}...	None	8	Left	Nominal
Contacts	Numeric	8	0	Advice and contacts with law enforcement authorities, regulatory bodies, I.S. providers	{0, No}...	None	8	Left	Nominal
INDEPREV	Numeric	8	0	Information security policy implementation independent review for assurance	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

THIRDPAR	Numeric	8	0	Identification of security risks from third party access and appropriate security controls implemented	{0, No}...	None	8	Left	Nominal
ACCTYPES	Numeric	8	0	Identification of types of access and appropriate security controls implemented	{0, No}...	None	8	Left	Nominal
Contract	Numeric	8	0	A formal contract with third parties with all security requirements to ensure compliance	{0, No}...	None	8	Left	Nominal
HIGHLIGHT	Numeric	8	0	A procedure to highlight and address third party information security compromises or weaknesses	{0, No}...	None	8	Left	Nominal
Inventory	Numeric	8	0	An inventory with important assets associated with each information system	{0, No}...	None	8	Left	Nominal
ASSETID	Numeric	8	0	Asset identification and association to an owner	{0, No}...	None	8	Left	Nominal
CLASSIFI	Numeric	8	0	Information classification scheme that can assist determine how information is handled and protected	{0, No}...	None	8	Left	Nominal
INFLABEL	Numeric	8	0	Appropriate set of procedures for information labeling and handling in accordance with classification scheme	{0, No}...	None	8	Left	Nominal
JOBDESCR	Numeric	8	0	Incorporation of security roles and responsibilities in JD as laid in org's security policy	{0, No}...	None	8	Left	Nominal
Confidentiality	Numeric	8	0	Employee confidentiality or non-disclosure agreement as part of terms and conditions of employment	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

EMPTERMS	Numeric	8	0	Terms and conditions of the employment cover employee's responsibility for information security	{0, No}...	None	8	Left	Nominal
TRAINING	Numeric	8	0	Employees and third party users reception of appropriate security training	{0, No}...	None	8	Left	Nominal
POLUPDAT	Numeric	8	0	Regular updates in organizational security policies and procedures	{0, No}...	None	8	Left	Nominal
INCIDENT	Numeric	8	0	Procedure to report security incidents through appropriate management channels	{0, No}...	None	8	Left	Nominal
SECUWEAK	Numeric	8	0	Procedure to report security weakness and malfunctions, or threats to systems or services	{0, No}...	None	8	Left	Nominal
Disiplinary	Numeric	8	0	Disciplinary process for employees who violate organizational security policies and procedures	{0, No}...	None	8	Left	Nominal
AUDTRAIL	Numeric	8	0	Maintenance of audit trails and logs relating to the incidents	{0, No}...	None	8	Left	Nominal
SECPERIM	Numeric	8	0	Physical security border facility to protect the information processing services	{0, No}...	None	8	Left	Nominal
ENTRYCON	Numeric	8	0	Entry controls in place to allow only authorized personnel into various areas	{0, No}...	None	8	Left	Nominal
ROOMLOCK	Numeric	8	0	Locking of rooms with information processing services	{0, No}...	None	8	Left	Nominal
Disaster	Numeric	8	0	Information processing services protection from natural and man-made disasters	{0, No}...	None	8	Left	Nominal
Needtoknow	Numeric	8	0	Information on need to know basis	{0, No}...	None	8	Left	Nominal
UNATTEND	Numeric	8	0	Mechanism to protect unattended computer not in use	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

CONFSEC	Numeric	8	0	Employees to lock unattended confidential material or documents	{0, No}...	None	8	Left	Nominal
Procedures	Numeric	8	0	Security policy incorporation of operating procedures e.g back-up	{0, No}...	None	8	Left	Nominal
CHANGECO	Numeric	8	0	Programs running on production systems subjected to strict change control	{0, No}...	None	8	Left	Nominal
LOGAUDIT	Numeric	8	0	Maintenance of audit logs for changes to the production programs	{0, No}...	None	8	Left	Nominal
DUTYSEGR	Numeric	8	0	Separation of duties and responsibility to reduce opportunities for unauthorized modification	{0, No}...	None	8	Left	Nominal
SEPARATE	Numeric	8	0	Separation of development and testing facilities from operational facilities	{0, No}...	None	8	Left	Nominal
ExternalC	Numeric	8	0	Management of information processing facilities by an external party	{0, No}...	None	8	Left	Nominal
Risksassociated	Numeric	8	0	Identification of risks associated with such management hence appropriate controls	{0, No}...	None	8	Left	Nominal
OPCONTRO	Numeric	8	0	Effective operational controls established where necessary	{0, No}...	None	8	Left	Nominal
REMOT EQU	Numeric	8	0	Responsibilities and procedures for management of remote equipment	{0, No}...	None	8	Left	Nominal
Specialcontrols	Numeric	8	0	Controls to safeguard confidentiality and integrity of data processing over the public networks	{0, No}...	None	8	Left	Nominal
Requirements	Numeric	8	0	Definition and documentation of business requirement for access controls	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

Controlpolicy	Numeric	8	0	Access control policy to address rights of each user or user groups	{0, No}...	None	8	Left	Nominal
Users	Numeric	8	0	Access control business requirement statement to users and service providers	{0, No}...	None	8	Left	Nominal
MOBILE	Numeric	8	0	Policy to account the risks of working with computing facilities such as notebooks, palmtops etc.	{0, No}...	None	8	Left	Nominal
Teleworking	Numeric	8	0	A policy, procedure and/or standard to control teleworking consistent with the org's security policy	{0, No}...	None	8	Left	Nominal
TELWSITE	Numeric	8	0	Suitable protection of teleworking sites against threats	{0, No}...	None	8	Left	Nominal
Businessvalue	Numeric	8	0	A documented Business Continuity Plan	{0, No}...	None	8	Left	Nominal
BCPMGT	Numeric	8	0	A managed process for developing and maintaining BCP	{0, No}...	None	8	Left	Nominal
BCPIMPAC	Numeric	8	0	Identification of events that can cause interruptions to business processes	{0, No}...	None	8	Left	Nominal
RISKASSE	Numeric	8	0	Risk assessment to determine the impact of interruptions	{0, No}...	None	8	Left	Nominal
STRPLAN	Numeric	8	0	A strategy plan based on risk assessment results to determine BCP approach	{0, No}...	None	8	Left	Nominal
TIMEFRAM	Numeric	8	0	Plans to restore business operations within required time frame following interruptions	{0, No}...	None	8	Left	Nominal
BCPTEST	Numeric	8	0	Regular testing of BCP to ensure that they are up to date and effective	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

BCPMAINT	Numeric	8	0	BCP maintenance by regular reviews and updates to ensure their continuing effectiveness	{0, No}..	None	8	Left	Nominal
PCPPROCE	Numeric	8	0	Procedures within org'l change management program to ensure business continuity matters are addressed	{0, No}..	None	8	Left	Nominal
LEGISLAT	Numeric	8	0	Organizational awareness of information security legal or compliance requirements	{0, No}..	None	8	Left	Nominal
COMPLIAN	Numeric	8	0	Definition and documentation of all statutory, regulatory and contractual requirements for each information system	{0, No}..	None	8	Left	Nominal
COMPREQU	Numeric	8	0	Specific controls and individual responsibilities to meet these requirements	{0, No}..	None	8	Left	Nominal
IPRIGHTS	Numeric	8	0	Procedures to ensure compliance with legal restrictions on use of material in respect to IPR	{0, No}..	None	8	Left	Nominal
LICENSE	Numeric	8	0	Supply of proprietary software products under a license agreement that limits use of the products	{0, No}..	None	8	Left	Nominal
RECORDS	Numeric	8	0	Adequate protection from loss, destruction and falsification of important organization records	{0, No}..	None	8	Left	Nominal
PERSINFO	Numeric	8	0	Management structure and control to protect data and privacy of personal information	{0, No}..	None	8	Left	Nominal
FACUSE	Numeric	8	0	Use of information processing facilities for non-business or unauthorized purpose treated as improper use	{0, No}..	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

LOGON	Numeric	8	0	A warning message at log on indicating that the system is private and unauthorized access is not permitted	{0, No}...	None	8	Left	Nominal
EVIDENCE	Numeric	8	0	Collecting evidence in accordance with legal and industry best practice	{0, No}...	None	8	Left	Nominal
Periodic	Numeric	8	0	Periodic reviews for information security requirements	{0, No}...	None	8	Left	Nominal
POLCOMPL	Numeric	8	0	All org'l areas considered for regular review to ensure compliance with security policy, standards and procedures	{0, No}...	None	8	Left	Nominal
CHECKS	Numeric	8	0	Regular checking of information systems for compliance with security implementation standards	{0, No}...	None	8	Left	Nominal
COMPETEN	Numeric	8	0	Technical compliance checking by competent authorized person	{0, No}...	None	8	Left	Nominal
SYSAUDIT	Numeric	8	0	Audit requirements involving checks on systems carefully planned and agreed to minimize business disruptions	{0, No}...	None	8	Left	Nominal
AUDITPRO	Numeric	8	0	Access to system audit tools such as software protected to prevent possible misuse or compromise	{0, No}...	None	8	Left	Nominal
ifscpo	Numeric	8	0	Information security policy	{0, No}...	None	8	Left	Nominal
secinfra	Numeric	8	0	Information security infrastructure	{0, No}...	None	8	Left	Nominal
thirdpac	Numeric	8	0	Third party access	{0, No}...	None	8	Left	Nominal
account	Numeric	8	0	Accountability of assets	{0, No}...	None	8	Left	Nominal
infoclas	Numeric	8	0	Information classification	{0, No}...	None	8	Left	Nominal
jobdefn	Numeric	8	0	Security in job definition and resourcing	{0, No}...	None	8	Left	Nominal
usrtrain	Numeric	8	0	User training	{0, No}...	None	8	Left	Nominal

Information Security Policy Framework for a Manufacturing Firm

				Responding to security					
secincident	Numeric	8	0	incidents and malfunctions	{0, No}...	None	8	Left	Nominal
secrea	Numeric	8	0	Secure area	{0, No}...	None	8	Left	Nominal
gencontrl	Numeric	8	0	General controls	{0, No}...	None	8	Left	Nominal
				Operational procedures and					
operaproc	Numeric	8	0	responsibilities	{0, No}...	None	8	Left	Nominal
nwmgmt	Numeric	8	0	Network management	{0, No}...	None	8	Left	Nominal
				Business requirement for					
busreqacc	Numeric	8	0	access control	{0, No}...	None	8	Left	Nominal
				Mobile computing and					
mobilecomp	Numeric	8	0	teleworking	{0, No}...	None	8	Left	Nominal
				Aspects of business continuity					
bcpaspects	Numeric	8	0	management	{0, No}...	None	8	Left	Nominal
				Compliance with legal					
legalreq	Numeric	8	0	requirements	{0, No}...	None	8	Left	Nominal
				Reviews of security policy and					
secpreview	Numeric	8	0	technical compliance	{0, No}...	None	8	Left	Nominal
auditsys	Numeric	8	0	System audit considerations	{0, No}...	None	8	Left	Nominal
orgsecurity	Numeric	8	0	Organizational security	{0, No}...	None	8	Left	Nominal
persecurity	Numeric	8	0	Personnel security	{0, No}...	None	8	Left	Nominal
				Physical and environmental					
physecurity	Numeric	8	0	security	{0, No}...	None	8	Left	Nominal
				Communications and operations					
commoperns	Numeric	8	0	management	{0, No}...	None	8	Left	Nominal
				Zscore: Have an approved					
ZINFOSEC	Numeric	11	5	published information security	None	None	13	Right	Scale
				Zscore: Communicated as					
ZCommunicate	Numeric	11	5	appropriate to all employees	None	None	14	Right	Scale

9 Glossary

Access Any exchange of a message between an interface, a repository or a service

Access Control The set formed by the User registration, Authentication, Authorization, Signing and Recording processes.

Access rights A class of access to a repository, a service or an interface that can be granted or revoked.

Accident A class of incident with non-human natural causes.

Activity A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans, and are documented in Procedures.

Agreement A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a Contract.

Alarm A set of events likely to be caused by an incident.

Alert A warning of a possible weakness or type of weakness, a new threat or a measured value of a metric going beyond defined thresholds.

Assessment Checking if an organization meets all the requirements specified in a standard or regulation to be accredited or audited.

Asset Any valuable property of the organization.

Attack A class of incident with an intentional human cause.

Audit Systematic, independent and documented process for obtaining Audit Evidence and evaluating it objectively to determine the extent to which the Audit Criteria are fulfilled.

Audit Criteria Set of policies, procedures or requirements. Audit criteria are used as a reference against which Audit Evidence is compared.

Audit Evidence Records, statements of fact or other information, which are relevant to the Audit Criteria and verifiable. Audit evidence may be qualitative or quantitative

Auditor Person external to the organization with the Skills to conduct an Audit on behalf of a Process Owner or a Customer.

Authentication Process that links the use of user accounts with their owner and manages the lifecycle of sessions.

Authority The technical person who implements approved access requests.

Information Security Policy Framework for a Manufacturing Firm

Authorization Process that grants the use of services and interfaces and access to repositories to Authorized and authenticated users and denies it to unauthorized users.

Authorizer A delegate of an Information System Owner who can approve or deny access requests to interfaces, repositories, channels and services of an information system.

Availability 1. The period of time when a process must performed as expected upon demand with minimal or no interruptions.

2. The period of time when a service, interface of channel must be accessible and usable upon demand with minimal or no interruptions.

Baseline The recorded state of an information system at a specific point in time.

Border A boundary between two environments.

Catastrophe Any incident that could result in an organization's demise.

Certificate 1. A credential based on Public Key Cryptography techniques.
2. A credential of being compliant with some standard or regulation.

Certification Body/Registration body A third party that assesses and certifies/ registers the ISMS of an organization with respect to published ISMS standards, and any supplementary documentation required under the system.

Certification Document/Registration Document Document indicating that an organization's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system.

Certification System/Registration System System having its own rules of procedure and management for carrying out the assessment leading to the issuance of a certification/ registration document and its subsequent maintenance.

Channel A channel is the medium used by services to exchange messages transparently, without explicit help from other lower level services. This collaboration is normally needed for creating and closing logical channels.

Client An information system that uses a service provided by another information system.

Configuration Item A service, repository, channel, interface or set of them.

Control Any kind of measure that can prevent, detect and correct undesired events.

Credential An item used for authentication of a user account in an access control system.

Information Security Policy Framework for a Manufacturing Firm

Critical A service is critical in a time span if the interruption of the service for that span of time cannot be replaced by alternative capabilities, and is highly likely to jeopardize business goals.

Customer The Customer of a process who provides the resources and sets the requirements for the process.

Device Instrument, software, measurement standard, reference material, auxiliary apparatus or combination thereof used to measure a process metric.

Digital Signature A type or record that includes the will and intent of a user about a repository. It might be hidden using watermarking techniques.

Disaster See Catastrophe

Effectiveness A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives.

Efficiency A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources.

Environment 1. All the physical, logical and organizational factors external to the organization.
2. A technical zone of the organization with a defined purpose, like the Server environment, User environment, Development environment, etc.

3. Any subdivision of a logical, technical or organizational partition under a single management.

Error A class of incident caused by a human because of a mismatch between the intended and the effective results of a task, or because of incorrect information or missing resources needed for the task.

Event Any fact that can lead to the detection of an incident.

Expectation Any hope for the future state of assets, organizational processes or information systems.

Exposure Any weakness that is visible to potential attackers.

Failure Loss of ability to operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, and Configuration Items etc. A Failure often causes an Incident.

Fault Synonym for Error.

Information Security Policy Framework for a Manufacturing Firm

Impact The direct and indirect cost of an incident including the cost of restoring the assets to the pre-incident state.

Incident A failure to meet a Information Technology objective resulting from accidents, errors or attacks.

Information System A human and technical infrastructure for the storage, processing, transmission, input and output of information.

Information System Owner The Customer [ITIL] of an information system, who has all the rights to the system, including discontinuation

Input specifications Procedures and policies that specify the requirements for the input of a process

Inputs The resource needed to generate the output of a process for which there are no possible alternatives.

Intellectual property Information which an organization has rights over under copyright, trade mark or patent law.

Interface A means of information input or output between a user and an information system.

Intrusion The theft of information about a target by an attacker.

Key Performance Indicator A metric of performance success of a process or

Knowledge Management The Process responsible for gathering, analyzing, storing and sharing knowledge information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge.

License An agreement that details the rights granted by an intellectual property owner to use certain information.

Lifecycle The set of states that make up a series of operational conditions of an information system.

Logging See Recording.

Login Beginning of a session, normally using a credential for authentication. Also called Logon.

Logout End of a session by the user account of by expiration. Also called Logoff.

Management To manage something is to define and achieve goals while optimizing the use of Resources.

Information Security Policy Framework for a Manufacturing Firm

Mark A legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification/ registration body indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard.

Mean Time Between Failures The average time between a two failures of an information system.

Mean Time To Repair The average time taken to restore an information system after a failure.

Measurement Considers the determination of a physical quantity, magnitude or dimension (using Measuring Equipment).

Measuring Equipment A Device that delivers quantitative information.

Message Meaningful data exchanged between services in a hierarchical or peer-to-peer fashion.

Metric A quantitative measurement that can be interpreted in the context of a series of previous or equivalent measurements.

Monitoring Implies observing, supervising, keeping under review (using monitoring devices); it can involve measuring or testing at intervals, especially for the purpose of regulation or control.

Network A set of physical or logical channels connecting repositories and interfaces.

Node An information system whose primary function is relay messages between channels

Non repudiation Ability to assert the authorship of a message or information authored by a second party, preventing the author to deny his own authorship.

Nonconformity The absence of, or the failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the business objectives of the organization.

Operational Level Agreement (OLA) SLA between a process provider and a Customer from the same organization who is a process provider to other Customers.

Opportunity The combination of an asset, a threat and an occasion that may give rise to an incident.

Information Security Policy Framework for a Manufacturing Firm

Organization A group of people that agree or accept responsibilities to act together with a common purpose. Associations, Companies and public institutions, for example, are organizations.

Output Results of a process.

Output specifications Procedures and policies that specify the requirements for the output of a process.

Performance Comparison between the outputs obtained and the set goals for outputs of a process.

Policy Documented rules to observe during implementation and maintenance that serve as governing principles when procedures are not detailed enough for a minority of cases.

Personal information Information that can identify a person.

Problem A cause of several non-simultaneous errors or accidents.

Process A organized set of tasks that uses resources and inputs to produce outputs.

Process Owner The person or team responsible for a process, including performance, prioritizing, planning for growth, and accounting for costs.

Process specification Procedures and policies that specify the requirements for a process.

Provider The process owner of a process that delivers its outputs.

Quality The meeting or surpassing of expectations.

Record An particular instance result of logging, including details like Interface ID and Location, User account or certificate ID, Signature, Type, Date and Time of Access attempt, Access attempt result, Repository, Interface, Service or Message accessed, etc.

Recording The process that registers the results of the user registration, authentication, authorization, use of systems and signing processes, so these can be investigated and will and intent or responsibilities determined.

Recovery Point Point in time when business processes or information systems can fall back in case of an incident.

Reliability The percentage of the Availability time a service, interface of channel must behave and produce results as intended.

Repository Any permanent or transient storage of information.

Information Security Policy Framework for a Manufacturing Firm

Resilience The ratio between the MTBF of a functionally equivalent redundancy free system and the MTBF of the system.

Resource A resource is anything needed to complete a task. Most resources stop being available to other tasks while they are being used. Some resources are exhausted after the task and cannot be reused.

Responsibility An assignment of a task, with power and resources, to a competent individual or a team accountable for the proper execution of the task.

Risk The loss expectancy as a function of a set of incidents' vulnerability and impact, measured in monetary units per year. The maximum risk the certainty of losing the total value of the organization within a year or less.

Role A set of responsibilities.

Scalability The ability of an IT Service, Process, Configuration Item etc. to perform its agreed Function when the Workload or Scope changes.

Secret Information shared in a controlled way between groups of people.

Security The repeated meeting of security objectives.

Security Objective A business expectation or requirement that is dependent on a security process.

Security Target A frequency and financial threshold for a metric derived from a security objective.

Service Any code or program that provides value for users, via messages exchanged with other services and access to repositories.

Service Level Agreement (SLA) Quality agreement between a process provider and a Customer specified using a set of metrics.

Session The set of successful and failed accesses to repositories and uses of services between the time a user account is authenticated and the time the authentication expires or the authentication is terminated.

Skills Demonstrated personal attributes and demonstrated ability to apply knowledge and competence

Information Security Policy Framework for a Manufacturing Firm

Signing Process that records the will and intent about a repository of the owner of the user account or certificate concerning a repository, such as agreeing, witnessing or claiming authorship of repositories and messages like original works, votes, contracts and agreements.

Special cause An assignable cause for a metric going beyond current thresholds

Specific Goal An objective of a set of specific practices.

Specific Practice A process.

Stakeholder A person, team or organization with interest in the success of a process, a management system or an organization.

Strategic Processes (SP) Processes that determine the objectives of lower level processes.

Target The information asset which may be the victim or potential victim of an attack.

Terminal An interface that is used directly by a User.

Threat Any potential cause of an Attack, an Accident or an Error.

Threshold Value against which a measurement is benchmarked or evaluated. In the context of Service Level Agreements is called a Service Level Objective.

Transaction A discrete Function performed by an IT Service. For example transferring money from one bank account to another. A single Transaction may involve numerous additions, deletions and modifications of data. Either all of these complete successfully or none of them is carried out.

User The person who uses an information system.

User account Representation of a user in an information system. A user account can be linked to a person or a group of persons.

User Registration Process that links user accounts and certificates to identifiable users, and manages the lifecycle of user accounts, certificates and access rights.

Visibility The degree to which information assets at a border present interfaces or provide services to information systems outside the organization.

Vulnerability The likelihood of an incident, measured as real instances against possible attacks, accidents and errors per year. These attacks, accidents and errors can be triggered by one or several threats.

Warning See Alert

Information Security Policy Framework for a Manufacturing Firm

Weakness Any fault in services, messages, channels, repositories, interfaces, organizational processes or responsibilities assignment that provides an opportunity for an error, attack or accident.

