Business Process Security Maturity

- A Paradigm Convergence

by

Debra Box

DISSERTATION

Submitted in fulfilment of the requirements for the degree in

MAGISTER TECHNOLOGIAE
in
INFORMATION TECHNOLOGY

at the

School of Information and Communication Technology

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

at the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Dr Dalenca Pottas

January, 2008

Acknowledgements

My sincerest gratitude and appreciation are extended to:

- My dear husband, Norman, for all his support;
- My promoter, Dr. Dalenca Pottas, for all her advice, guidance and encouragement.

And finally,

- Alan P Alchin who ignited, in a young person, this passion for IT.

ABSTRACT

Business Process Security Maturity - A Paradigm Convergence

Information technology developments in software and hardware have enabled radical changes in information systems, culminating in the paradigm Business Process Management. There has been a concomitant rise in the importance of information security and security engineering due to the increased reliance by society on information. Information is seen as a critical success factor which needs protection. Information security is the response to increased hazards created through recent innovations in Web technology and the advent of intra and inter enterprise-wide systems. Security engineering is based on a variety of codes of practice and security metrics which aim at ameliorating these increased security hazards. Its aim is to produce a balanced set of security needs which are integrated into the system activities to establish confidence in the effectiveness of the security counter-measures.

It is generally accepted that security should be applied in an integrated approach, for example, in Information Systems development. This has proved to be a noble thought but is the exception to the rule. Security, historically, is generally applied as an after-thought in an Information Technology implementation. This motivated the concept of formulating a model of integrating security inherently within the paradigm of BPM. The overarching requirements of the model are to align the overall organisational security initiatives and ensure continuous improvement through constant evaluation and adaptation of the security processes. It is the intention of this research to show that these requirements are achievable through aligning the process management methodology of BPM, with the security paradigms of Information Security Management (using the ISO 17799 standard) and security engineering (using the Systems Security Engineering Capability Maturity Model – SSE-CMM).

The aim of the Business Process Security Maturity model as the output of this research, is to link the SSE-CMM, as the security metric and appraisal method, to the ISO 17799 security standard, which provides the guidance for the information security management framework and security control selection, within the Business Process Management environment. The SSE-CMM, as the security

version of the Capability Maturity Model, provides the necessary strategy to control the security engineering processes that support the information systems and it maintains that as processes mature they become more predictable, effective and manageable. The aim of the model is to provide an integrated, mature security strategy within the business process and monitor and correct the security posture of the implemented counter-measures.

DEPARTMENT OF ACADEMIC ADMINISTRATION

EXAMINATION SECTION – NORTH CAMPUS

PO Box 77000
Nelson Mandela Metropolitan University
Port Elizabeth 6013

Nelson Mandela Metropolitan University
for tomorrow

DECLARATION BY STUDENT

NAME: ……Debra Box……

STUDENT NUMBER: ……20315813……

QUALIFICATION: MAGISTER TECHNOLOGIE: Information Technology

TITLE: ……Business Process Security Maturity……..
……- A Paradigm Convergence……..……
…….
…….

DECLARATION:

In accordance with Rule G4.6.3, I hereby declare that the above-mentioned treatise/dissertation/thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

SIGNATURE: ……..

DATE: ……..

ACRONYMS

A2A	Application to Application
ACID	Atomicity, Consistence, Isolation, Durability
ASD	Adaptive Software Development
B_2B	Business-to-Business
B_2Bi	Business-to-Business Integration
BAM	Business Activity Monitoring
BI	Business Intelligence
BPA	Business Process Analysis
BPA/M	Business Process Analysis and Modeling
BPI	Business Process Improvement
BPM	Business Process Management
BPMI	Business Process Management Initiative
BPMM	Business Process Maturity Model
BPMS	Business Process Management System
BPR	Business Process Re-engineering
BPSM	Business Process Security Maturity Model
BS 7799	British Standards Institute – BS 7799 - Information Technology – Code of Practice for Information Security Management
BS 7799-2:2002	British Standards Institute – BS 7799 - Information Security Management Systems Part 2: Specification with guidance for use
BSI	British Standards Institute
CCSC	Commercial Computer Security Center
CMM	Capability Maturity Model
CoBiT	Control Objectives for Information and related Technologies
CPI	Continuous Process Improvement
CRACK	Collaborative, Representative, Authorised, Committed and Knowledgeable
CRM	Customer Relationship Management
DBMS	Database Management System
DoD	Department of Defense
DTI	Department of Trade and Industry
EAI	Enterprise Application Integration

EII	Enterprise Information Integration
EPM	Enterprise Performance Management
ERP	Enterprise Resource Planning
FDD	Feature Driven Development
IDE	Integrated Development Environment
IDEAL	Initiating, Diagnosing, Establishing, Acting and Learning approach
IDEFO	Integrated Definition Function Modeling
IEC	International Electrotechnical Commission
INS	International Network Services
IS	Information Systems
ISBS	Information Security Breaches Survey
ISD	Internet Speed Development
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISO/IEC 17799:2000	ISO 17799: 2000. Information Technology – Code of Practice for Information Security Management
ISO/IEC 17799:2005	ISO 17799:2005. Information Technology – Code of Practice for Information Security Management
ISO/IEC 17799-2:2003	ISO 17799-2:2003. Information Security Management Systems Part 2: Specification with guidance for use
ISSO	Information System Security Officer
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
KPIs	Key Performance Indicators
NCC	National Computing Center
NIST	National Institute of Standards and Technology
OO	Object Oriented
PA	Process Area
PDCA	Deming Wheel - Plan-Do-Check-Act Model
PP	Protection Profile
QM	Quality Management
ROI	Return on Investment
ROSI	Return on Security Investments
RUP	Rational Unified Approach
SAM	Security Assessment Model

SANS	SysAdmin, Audit, Network, Security
SDLC	System Development Life Cycle
SEI	Software Engineering Institute
SoA	Statement of Applicability
SoC	Statement of Controls
SPC	Statistical Process Control
SSAM	SSE-CMM Appraisal Method
SSE-CMM	Systems Security Engineering Capability Maturity Model
TCSEC	Trusted Computer System Evaluation Criteria
TDD	Test-Driven Development
TQM	Total Quality Management
UML	Unified Modeling Language
WfM	Workflow Management
WfMC	Workflow Management Coalition
WfMS	Workflow Management Systems
XP	Extreme Programming

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 - CHAPTER ONE - INTRODUCTION

There is a widespread belief that the current trend of sustained and unpredictable change in the business world will continue. Its ingredients - namely marketplace changes, tailored products and services, changing social and demographic patterns - are relentless (Moreton and Chester, 1996). Globalisation, with its attendant effects of increased competition and the shift from producer-controlled markets (supply push) to customer-controlled markets (demand pull), has necessitated organisations to review the way they operate (Smith and Fingar, 2002). These changes in the business world have required that the Information Technology (IT) industry responds to this dynamic operating environment which obliges the business community to continually adapt its structures, strategies and policies (Abrahamsson, Warsta, Siponen and Ronkainen, 2003, Nerur, Mahapatra and Mangalaraj, 2005). The Agile Enterprise is the result of these developments (Baskerville and Siponen, 2002). These organisational transformations are aided by various business methodologies and advances in technology.

Information Technology is perceived as potentially the most pervasive enabler in these transformations. The field has moved from the mainframe to the stand-alone personal computer and on to enterprise-wide systems linking organisations globally. Information has evolved from functional silos to shared data models. IT, from an industry perspective, has changed significantly from its conception. It was originally seen, from the business standpoint, as a substitute for repetitive clerical work. Consequently, office work was arranged utilising the computer as a transaction processing system. The design of computer-based systems as operational systems was justified by the 'Scientific Management' principles as refined by Frederick Taylor over the previous fifty years (Thompson, 2003, Pruijt, 2002, Moreton and Chester, 1996).

These 'Scientific Management' principles or Taylorism comprise time and motion studies. Routine tasks are separated from planning and control and machines replace manpower. This concept was originally intended for the factory floor but was extended to material flow and management systems. A major premise is that work products are stable and predictable. This is inappropriate in the prevailing milieu where businesses are required to be proactive. The IT infrastructure installed using the rigid Taylorism approach delivered little return-on-investment

(ROI) nor provided businesses with any degree of competitive advantage (Thompson, 2003, Pruijt, 2002).

Radical developments in IT and its infrastructure in the last two decades have enabled its omnipresence and strengthened its role as a business enabler. Eatock, Giaglis, Paul and Serrano (2000) conclude, from a simulation case study, that changes to the IT infrastructure has a corresponding influence on organisational business performance and there is a clear dependence between business process performance and IT capability.

The emergence of new software and hardware facilitated the evolution of businesses towards enterprise-wide systems using intra and internets through the use of Internet Web technology. These new systems required an original way of thinking in their design and implementation. A variety of strategies were realised and refined, culminating currently in Business Process Management (BPM). A BPM deployment is characterised by agile development methods and it requires security to ensure its efficient and reliable operation. The value that an IT infrastructure brings to an enterprise is a factor of this security. Inadequate security renders any IT installation untrustworthy and diminishes user confidence. The implementation of any automated system imposes increased security risks. Information is communicated between enterprises through the partnerships built via BPM and Business-2-Business (B_2B) installations and is vulnerable. The development of security standards has ameliorated these hazards to a varying degree.

There are a variety of standard security metrics and security management systems in existence. These include:

- The Trusted Computer System Evaluation Criteria (TCSEC);
    - Information Technology Security Evaluation Criteria (ITSEC);
    - Common Criteria;
    - Control Objectives for Information and related Technologies (CoBiT);
    - ISO 17799 Code of Practice for Information Security Management.

The international security standard, ISO 17799, for example, provides a set of guidelines for the design of an Information Security Management System (ISMS).

It aids the enterprise in constructing its security policy which is the core of its information security management process.

The increased focus on information security has raised the importance of the quality of the security processes themselves. Quality is seen as a Twenty-First Century business driver. The industrial revolution stressed high quality and high cost, while the mass production era, which extended past the Second World War, heralded moderate quality and low cost. Currently, quality is increasing and costs are being reduced. This third era focuses on quality, the product process and the uses of information (DeFeo and Janssen, 2001). The application and technological efficacy of an IT infrastructure are imperative. There is dissatisfaction with the ROI and quality previously achieved. It was acknowledged that the chief drawback was the failure to control the software process. Projects were late and over budget (SEI-CMM, 1993). These failings led to the development of the Capability Maturity Model (CMM). It provides the enterprise with the necessary strategy to control the processes that support their Information Systems (IS) (SEI-CMM, 1993, Bardoloi, 2004). A Systems Security Engineering Capability Maturity Model (SSE-CMM) was developed that particularly addresses the security engineering process. It holds that as a process matures, its results become more stable, predictable and controllable and effective in terms of costs, productivity and quality (SSE-CMM, 2003, Barton, Hery and Liu, 2000).

The three paradigms that are relevant to this research have been introduced into the discussion; namely business process management, information security management and (security) maturity measurement. An overview of these paradigms is subsequently presented to introduce the three pillars of this research and highlight their significant role in the IT, security and IS environments.

1.1 Business Process Management

The business paradigm, BPM, is not new and has evolved from the related fields of business process improvement, Business Process Re-engineering (BPR), Business Intelligence (BI) and business process innovation. BPM efforts exist

under a variety of names, for example, Six Sigma (Harmon, 2003). The business process is the embodiment of BPM.

1.1.1 Business Process Defined

The business process, as a concept, was first defined, in the Twenties by Frederick Taylor, in terms of "methods and procedures". Smith and Fingar (2002) define the business process as a dynamically coordinated set of collaborative and transactional activities that deliver value to clients. It is, according to McGovern (2004), seen as an interdependent set of business activities and decisions. An essential feature is its coordination across a value chain. A *Value Chain* includes all the core and support processes needed to convert the raw resources into the finished product that is sold to the customer. Business processes are constantly evolving in size and complexity and are generally not engineered from their outset. BPM is seen as a vital tool which has emerged to both manage and improve these evolving business processes (Pyke and Whitehead, 2003).

1.1.2 Business Process Management Development

Business Process Management, initially, entailed processes being manually re-engineered and placed in automated Enterprise Resource Planning (ERP) systems. These ERP systems, based on Total Quality Management (TQM) principles, provided little management control over the processes. This led to a dearth in the realisation of benefits from investments in IT. It is only recently that a practical means of accomplishing the management and implementation of business process design and execution has been established. These enabling technologies include Workflow, Enterprise Application Integration (EAI) and Web services which have been converging from different perspectives over time to create BPM (Hollingsworth, 2004).

Process management is an activity most companies perform and is core to any process-driven strategy (PPI Research Report, 2004, Harmon, 2004, Smith and Fingar, 2004b, Rosemann and de Bruin, 2005, Lee and Dale, 1998). Its prominence as a business activity increased after the advent of the IT motivator, Business Process Re-engineering (BPR), which is a business performance improvement strategy based on Quality Management (QM) principles. Other predecessors of BPM include ERP applications and EAI. ERP applications provide

greater visibility into business processes, EAI links intra- and inter-enterprise applications and data while BPR is viewed as the radical re-structuring of the business process (Smith and Fingar, 2002, McGovern, 2004). BPM is the latest shift in the process management paradigm.

1.1.3 Business Process Management Defined

Business Process Management is a tool to manage and improve the business process (Pyke and Whitehead, 2003). It views the business process as uniquely identifiable with specific objectives whose degree of success can be measured both qualitatively or quantitatively (McGovern, 2004). It is seen as both a solution to and consequence of a changing business environment. It satisfies the business goal of improving efficiency by reducing operating and capital costs. It addresses business agility by improving the delivery cycle and market reaction gap and finally, it addresses customer retention and satisfaction (McGovern, 2004, Smith and Fingar, 2002). The components that characterise BPM are divided into six groups (McGovern, 2004):

- Users facilities;
- Business Process activity and Modelling facilities;
- Run-time components;
- Business Activity Monitoring;
- Business Performance Monitoring;
- Infrastructure and system management.

A BPM deployment enables an organisation to meet its corporate goals through its potential to provide opportunities to respond to changes and challenges. BPM aids businesses in facing two distinct but related pressures; the need to eliminate unproductive costs through improved efficiency and the need to provide flexible processes that respond to changing markets and client requirements. These needs are met through the capacity of a BPM deployment to advance Continuous Process Improvement (CPI) efforts.

However, a BPM environment needs to be secure to ensure its efficient, reliable operation, therefore, information system security is an important issue.

1.2 Information Security development - Changing Security Needs

There has been a continuous change in the need for security in the last few decades. Security concerns, in early computing environments, were chiefly focused on physical theft or destruction of the computer equipment. Computer systems, from the early Seventies onwards, have been transformed by network technology. This greater interconnectedness made computer systems more vulnerable to poor system design. The Eighties saw the introduction of the personal computer and their widespread introduction into the general population. The Nineties onwards have seen an exponential growth in the Internet, Intranets and the personal computer market, raising security issues to an even higher level of urgency (Ferraiolo and Thompson, 1997).

Computer systems security is increasingly important due to the pervasiveness of the Internet which potentially links computer-based systems, enterprises and organisations globally. It is, currently, thought to be the era of 'systems of systems'. These comprise components which are systems in their own right and are characterised by the operational and managerial independence of their components. The global, public Internet is a prominent example of computer-based system of systems (Sheard and Moini, 2003).

A survey conducted by Information Security Breaches Survey (ISBS) illustrates some notable trends in the United Kingdom. The extensive business use of the Internet incurs greater exposure to security incidents with 94% of local businesses experiencing a security incident in 2004 (ISBS, 2004). Security, whilst remaining a management priority, is seen as an overhead and does not receive the commensurate financial investment (ISBS, 2002, ISBS, 2004, Dhillon, 2005). Information security, according to Siponen (2002), Fiedler (2003) and Margaritis, Kolokotronis, Papadopoulou, Kanellis and Martakos (2001), is generally not treated as an IS priority but as a technological issue and an afterthought to the system implementation. However, technical security solutions are limited in their effectiveness (Kahraman, 2005). Because security is not considered as an integral part of the business process, within an IS, the 'development duality' phenomenon is caused. This is a critical issue in secure systems development and results from the separate development of the system software and its security. This causes a conflict between the business analyst-designed functionality of the IS and its

security function as designed by the security analysts (Margaritis et al, 2001, Siponen and Baskerville, 2001, White and Dhillon, 2005).

The information of an organisation comprises its past experience and its potential future. It is a critical success factor and needs protection. Any threats to it or its mediating procedures are risks to quality, effectiveness and the existence of the organisation (Fiedler, 2003). Information security is the consequence of responding to these hazards and has risen in prominence. It covers many issues including security policy; risk analysis and management; contingency planning and disaster recovery. A system, as perceived by its users, is secure when it operates as expected (Hong, Chi, Chao and Tang, 2003). Security is addressed through the analysis of the potential threats to the system and engineering the system to reduce its vulnerability (Sheard and Moini, 2003). Security engineering has concurrently become important through the increasing reliance of society on information.

1.2.1 Addressing Security Issues

Organisations have, in response to their recognised security conditions, implemented security control programs. These require regular maintenance and governance otherwise '*security slippage'* occurs. This happens when the security program lacks governance as a result of a lack of focus, skilled resources or investment. Traditionally, security controls shift into maintenance mode without meaningful governance and the security solutions fall into apathy. This disrupts budgetary cycles and leads to management cynicism which prevents security becoming an active participant in meeting organisational objectives. The installation of a mechanism to monitor the quality and capability of the ISMS to contend with this '*security slippage'* is recommended (Tiller, 2005).

1.2.2 ISO 17799 Security Standard

The British Standards Institute developed and implemented the British Standard, BS 7799, in 1995, which provides guidelines and controls devoted to the design of an ISMS. The standard was internationally accepted and published as ISO 17799 (Fiedler, 2003). ISO 17799 is broad in scope and conceptual in nature. It defines information as an enterprise asset which needs protection and information security as the protection of the information asset to ensure its continuity, to minimise

business harm and to maximise ROI (Carlson, 2001, Spears, Barton and Hery, 2004).

The ISO 17799 is an international standard which constitutes the code of practice for information security management and it provides the necessary guidelines and controls (ISO 17799:2000, Carlson, 2001, Spears et al, 2004) It provides a non-technical view to organisational security needs (Kahraman, 2005). It is neither technically-driven, nor product or technology-aligned (Carlson, 2001, Spears et al, 2004). The ISO 17799:2000 contains 127 controls in 10 areas or domains which can be designated at an organisational or application level. The control or counter-measures selection is determined by conducting a risk analysis and considering the unique security needs of the organisation implementing it (ISO 17799:2000).

The BS 7799 / ISO 17799 standards are continually evolving and being superseded. The BS 7799: Part 1, as a code of practice for an ISMS, was accepted as the ISO 17799 in 2000. It was revised and republished in 2005 as ISO 17799:2005. There are plans to change its numbering in 2008 and republish it as ISO 27002. The BS 7799: Part 2. as the specification document to achieve formal accreditation against the BS 7799: Part 1 was adopted by a variety of countries, for example, South Africa and Australia, but did not become an ISO standard in 2000. The review of the ISO 17799 in 2005 caused the BS 7799: Part 2 to be submitted to the ISO and it was accepted as the ISO 27001 (von Solms and von Solms, 2007).

The development of the ISO 17799:2:2003 specifically addresses the lack of an audit or certification facility in the ISO 17799:2000. It provides the activities required by an organisation and the auditing party to ensure certification.

The increased need for effective information security has advanced its importance as a discipline. The evaluation of security features implemented through the application of the ISO 17799 highlighted the reality that the processes themselves were deficient and proved to be costly and time-consuming to render secure. Secure systems were either delivered late or without being evaluated. The secure system and its documentation are the focus of evaluation and certification with almost no emphasis on the creating processes. Attempts to provide secure system development, using various security testing processes and procedures, proved

unrealisable in an undisciplined environment. These prompted the development of the SSE-CMM, the security version of CMM (Ferraiolo and Thompson, 1997). The CMM was initially developed to address issues of dissatisfaction with quality and the ROI on IT technology and infrastructure.

1.3 Capability Maturity Model

The CMM was developed by the Software Engineering Institute (SEI) at Carnegie-Mellon University in 1986, originally funded by the Department of Defence (DoD) in the United States of America. It was developed following two decades of dissatisfaction with the productivity and quality gained from the software applications and technology methodologies in place. It was realised that the fundamental problem was the inability to manage the software process. Projects were late and outside the planned budget (SEI-CMM, 1993). CMM provides organisations with the guidance to gain control of the processes that support their IS. The software industry deems quality as important and an aid to cost-reduction and competitiveness. It enhances the quality of processes through improving their maturity (Bardoloi, 2004).

1.3.1 Capability Maturity Model Defined

The CMM comprises five increasing levels of process maturity. Its five-stage structure focuses on various principles, notably TQM (Bardoloi, 2004). These have been adapted into a maturity framework which establishes a project management and engineering foundation for the quantitative control of the software process (SEI-CMM, 1993). It is described as a normative model which describes the state of an organisation at each maturity level (Tse, 2005).

The CMM provides the structure for organising the improvement steps of CPI into five maturity levels. A maturity level is an ordinal scale which measures the maturity of the software processes and process capability of an organisation. It assists in the prioritisation of improvement efforts. Each maturity level emphasises the primary process changes made at each stage as illustrated in Table 1.1 (SEI-CMM, 1993).

There are a variety of advantages gained from evolving through the maturity levels of CMM. Each upgrade is accompanied by an improvement in the overall performance and core competency of an organisation. Its benefits include a shift

from re-active to pro-active management, improved decision-making and shortened delivery cycles. There is improved software product quality together with a reduction in development and support systems costs and finally, greater customer satisfaction (Bardoloi, 2004).

Maturity Level	**Software Process Character**	
Maturity Level 1 (Initial)	Ad hoc	
Maturity Level 2 (Repeatable)	Disciplined	Process management polices and controls are established and project successes are repeatable
Maturity Level 3 (Defined).	Formally defined and integrated	Both management and engineering processes are documented within a stable environment
Maturity Level 4 (Managed).	Predictable	Process quality is quantitatively controlled within a management program
Maturity Level 5 (Optimising).	Continuously improving	CPI is facilitated through quantitative process feedback and from piloting innovative ideas and technologies

Table 1.1 - Maturity Level Characteristics

The increased need for security was previously highlighted together with the concomitant increase in the focus on security engineering. This leads to a discussion on the CMM which was developed specifically for security and security engineering by the SEI, namely its security version, the SSE-CMM model.

1.3.2 Systems Security Engineering Capability Maturity Model

The SSE-CMM describes the essential characteristics of a high-quality security engineering process. It is a framework for developing a mature, security engineering process which is characterised as formally defined, documented and which practices CPI (SSE-CMM, 2003, Spears et al, 2004). It portrays general industry practices and covers, as a standard metric (SSE-CMM, 2003):

- The entire system life cycle;

- The entire organisation including management, organisational and engineering activities;
- Concurrent activities with other disciplines and interactions with other organisations.

The SSE-CMM intends that security becomes an integral part of engineering efforts for an ISMS and IT infrastructure and is pervasive throughout the organisation. The security engineering process is defined, measured, controlled and thus effective (SSE-CMM, 2003). It comprises two parts, a model for security engineering, project and organisational processes and an appraisal method to assess their maturity. It is used to achieve process improvement through advancing through the maturity levels. The capability evaluation establishes the process capability levels of the organisation and its business partners and finally, establishes security assurance by providing evidence of the process maturity (Spears et al, 2004). Therefore, an organisation can evaluate its security engineering practices and identify areas for improvement (Barton et al, 2000).

The practices of the SSE-CMM concentrate on the security needs of the customer. It focuses on implementing security within an IS and its IT infrastructure. Its purpose is to assess and improve the security engineering capability and promote its integration to ensure that security engineering becomes persistent across the organisation (SSE-CMM, 2003). It provides a generic framework for the design and development of a secured system and the method to improve, manage and control security and its awareness within an organisation (Tse, 2005, Chan and Kwok, 2001). Security practices and technology are more business-appropriate as the security engineering process matures (Tiller, 2005).

This concludes the overview of the three pillars of this research which now enables the formulation of a problem statement.

1.4 Problem Statement

Recent and significant developments in IT infrastructure, software, hardware and technology have culminated, currently, in the business paradigm, BPM, which is characterised by a dynamic environment and the so-called agile enterprise. BPM enables an organization to achieve its corporate goals of reducing costs, improving quality and efficiency, and meeting customer satisfaction. This requires

flexible business processes. These changes in business environments have raised the importance of information security. A BPM deployment requires security to ensure its safe and efficient operation but its emergent and turbulent nature poses particular security problems.

Information security and security engineering have, concurrently, become increasingly important because of the progressive reliance of modern society and the business community on information contained in the various IS and IT infrastructures. Both the advent and pervasiveness of the Internet and related technologies have resulted in an increase in security hazards to the information assets of an enterprise.

The following realisations are motivated by these afore-mentioned developments and are stated as follows:

- Security is not treated as an integral part of BPM at the business process level. It is generally not integrated in the design of the business process and therefore, is not treated as an IS priority but is approached in a piecemeal fashion by addressing issues such as authentication, authorisation and network-security as add-ons to the IT environment (Margaritis et al, 2001, Siponen and Baskerville, 2001, White and Dhillon, 2005);
- Technical approaches to information security are seen as limited in their effectiveness (Kahraman, 2005);
- An IS system is only as reliable and trusted as it is secure (Wynes, 2001, Neubauer, Klemen and Biffl, 2005, Fiedler, 2003, White and Dhillon, 2005).

The following needs are identified from these realizations:

- There is a need to integrate security into the business process itself to render the business process secure;
- Its security position or status needs to be evaluated to ensure it is both satisfactory and current and meeting the needs of the organisation and the security posture within the business process must be continuously monitored, managed and improved as necessary;
- Any security system that is implemented needs to be based on an internationally recognized security standard which provides the guidelines

to select the security controls uniquely tailored to the individual situation. The use of an internationally recognized security standard provides the means for an organization to be certified which creates both confidence and business trust.

The BPM environment presents unique security problems due to its dynamic nature which continually changes its security needs. This further highlights the need to continually evaluate and amend the security position of the business process.

The problem that is addressed in this research can, therefore, be summarized as originating from the 'development duality' phenomenon, which implies that security is not integrated into IS design at the business process level. This highlights the need for a cogent model that links the methodologies of the CMM and its security version, the SSE-CMM, to the international security standard, the ISO 17799 within the business paradigm, BPM. These methodologies (individually) contend that process improvement is dynamic and essential to their function and is a vital part of their operation. The coupling of these methodologies will allow the security posture within the business process to be established, continuously monitored, managed and improved as necessary. The development of the Business Process Security Maturity model will address this omission.

1.5 Research Aim and Objectives

The aim of this research is to align the concepts of the ISO 17799 security standard and the SSE-CMM framework, with the corporate methodology of BPM. The objective is to develop a Business Process Security Maturity (BPSM) model. Its development is motivated by the perceived omission of a cogent model linking these methodologies to provide a mature and effective security posture that is integrated into the business process. Its goal is to provide an integrated and holistic security strategy for BPM. A security-integrated mature business process is seen as a function of an information security management framework, being the ISO 17799 security standard and a security metric, being the SSE-CMM, within the business methodology, BPM. The SSE-CMM will provide a framework which evaluates the maturity of the security engineering process. The ISO 17799 security standard will provide the necessary security controls to populate a

security framework. It provides the basis for the security policy of the organisation and it provides the guidelines for implementing and maintaining an ISMS.

It will be demonstrated in subsequent chapters that there are apparent convergences in the defining characteristics of the three pillars of this research which contends that they can be combined into an information security management framework to integrate security into a business process. These convergences will be uncovered, defined and developed into a rational model, the BPSM model. The output of the BPSM model is a secure mature business process which integrates security into the business process itself.

1.6 Research Paradigm

There are two categories of research, quantitative and qualitative. Quantitative methods are appropriate for testing and refining a well-developed theory and they tend to produce convincing scientific evidence (Moody, 2002). Their methods include the laboratory experiments, survey methods, formal methods such as econometrics and mathematical modelling (Myers, 1997).

Qualitative methods are seen as more appropriate in the early stages of research (exploratory research) and for theory building (Moody, 2002, Myers, 1997). The researcher attempts to draw a reasonable connection between what is observed and the conclusions that are argued from these observations (Hoepfl, 1997). It is usually necessary to present some argument to explain the selection of a particular solution or alternative. This argumentation can range from the statement of obvious facts to detailed reasoning which highlight and combine a variety of subtle issues (Olivier, 2004).

Myers (1997) notes that there has been a general shift in IS research from technological to managerial and organisational issues which has promoted the interest in qualitative research methods. Information systems are seen to be a social activity which combines social systems together with technology to benefit society as a whole (Goede, 2003). This places an emphasis on a more phenomenological approach to the research (Lester, 1999). This means that there is greater importance placed on the meaning of what is being researched rather than on the measurement thereof. This research adopts the underlying epistemology of interpretivism of the qualitative paradigm, with the philosophical

foundation of interpretivism being phenomenology, hermeneutics and language. The researcher, with interpretivist research, gathers information and filters it, while involving themselves in the study. Subjectivity, in this kind of research, plays a role, with the researchers having to argue towards the interpretation of the research area and the proposed solution.

The research aim of this work is to investigate and develop a model which incorporates security engineering and information security management approaches in the Business Process Management paradigm. A model is constructed due to its ease of comprehension and manipulation. Models are used to propose an idea because it is more practical than constructing or implementing the complete modelled system (Olivier, 2004). The BPSM model is constructed due to the practical challenges involved in constructing and implementing an operational system.

1.7 Methodology

A research method is a strategy of inquiry which moves from its underlying philosophy to the research design and data collection. All research methods use various techniques to collect data or material. These range from interviews to archival research. Written data sources include unpublished works, for example, case notes and experimental data, as primary sources and published documents, such as journal articles, as secondary resources (Myers, 1997). Since this research is predominantly of a phenomenological nature, the execution of a proper literature study was employed as a suitable research method.

A comprehensive literature survey is conducted, using secondary sources, which are collected on the three research topics or domains under investigation, namely BPM, the ISO 17799 security standard and the CMM and its security version, the SSE-CMM. The literature survey is reviewed and the BPSM model is developed through reasoned argumentation. The BPSM model is used to illustrate the proposed research aims which, due to resource constraints, are impractical to demonstrate through constructing an operational system.

The results of the study are reported in the form of a dissertation.

1.8 Preliminary Layout of Dissertation

The proposed outline of the dissertation is presented in Figure 1.1. It is divided into three parts. The first part acquaints the reader with the research area and is split into four chapters. The chapters in Part One provide an in-depth examination of the three pillars of this research, the ISO 17799 security standard, the CMM and its security descendent, the SSE-CMM and the business paradigm, BPM.

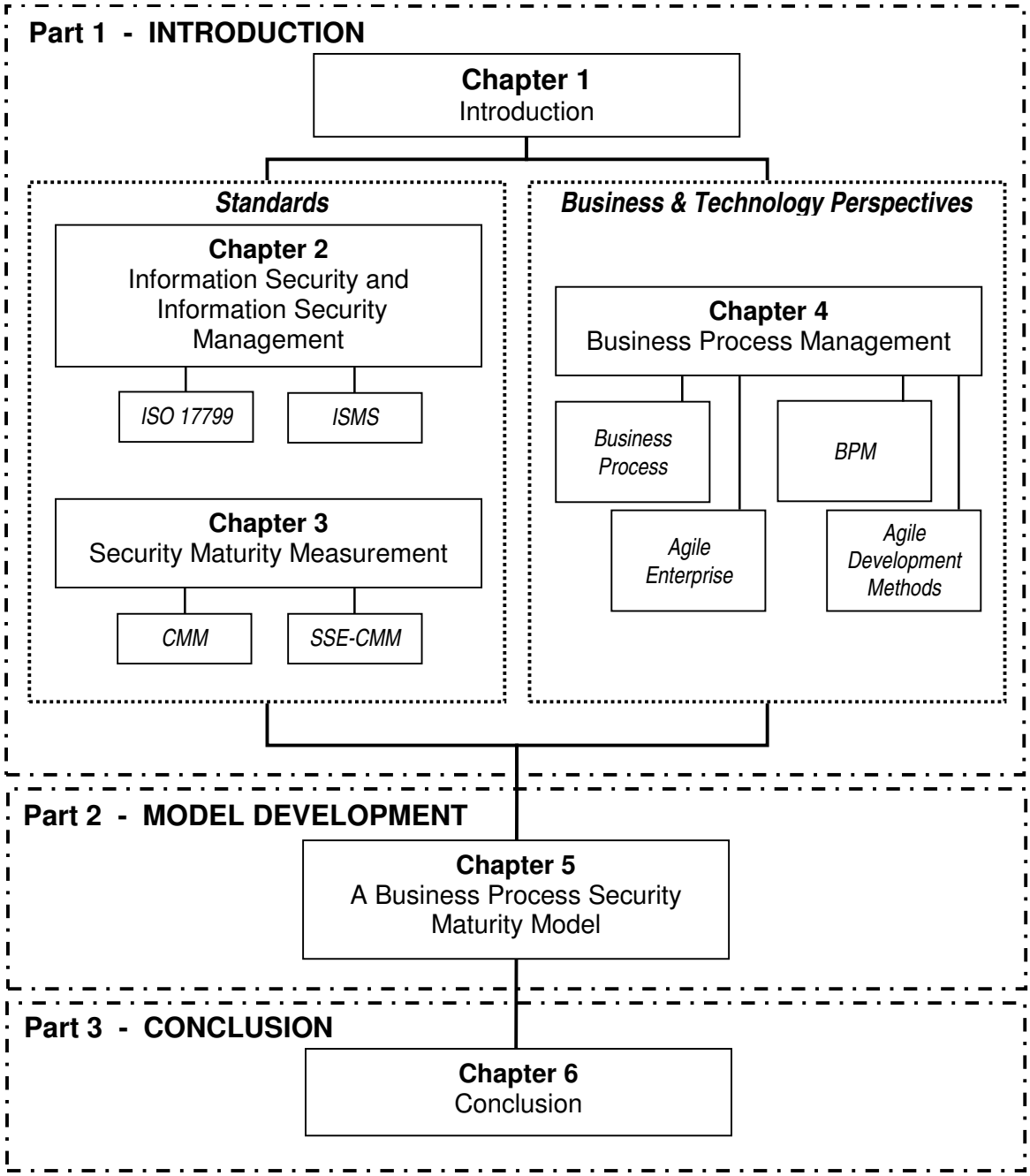


Figure 1.1.- Proposed layout of Dissertation

Chapter One provides the overall background information on the research area and presents the problem statement, aim, objectives and research methodology pertaining to this research.

Chapter Two presents an overview of the increased need for information security. The history of the ISO 17799 is presented. The code of practice of the ISO 17799 security standard is discussed. The stages of developing an ISO 17799-based ISMS are examined.

Chapter Three examines the motivation for a CMM. An overview of the architecture and concepts of the CMM and SSE-CMM is presented. The maturity levels are analysed in depth. Security engineering, as a discipline, is examined. The uses of the SSE-CMM and its appraisal method, to provide and prioritise process improvement efforts are examined.

Chapter Four presents and discusses the methodology of BPM. The history of BPM and its business drivers are examined. A generic BPM model and its supporting standards are examined. The development of the agile enterprise, its characteristics and a variety of agile software development methods are presented.

Part Two presents the development of the proposed model. The converging characteristics of the CMM, ISO 17799 standard and BPM are identified and evaluated in Chapter Five which deals with the development of the conceptual Business Process Security Maturity Model. Two business process (management) maturity models are examined to establish the efficacy of evaluating BP(M) maturity using a CMM-based approach. Various assessment models which combine the ISO 17799 and the SSE-CMM are examined to ascertain whether their combination is viable. A method for integrating security within an agile environment is presented. The aim of the chapter is to demonstrate the viability of combining the security metric, the SSE-CMM with the security standard, ISO 17799 and whether the integration of security into the business process as the fundamental element of the agile enterprise can be successfully achieved. Finally, the BPSM model is described.

Part Three of the research presents the conclusions in Chapter Six. The problem statement and research objectives are re-examined with relevance to the literature study and to the BPSM model.

1.9 Conclusion

Chapter One presented an overview of the three pillars of this research, namely the BPM business paradigm, a CMM and its security version, the SSE-CMM and the security standard, ISO 17799. They were discussed at a high-degree of abstraction to provide an introduction into the subject matter. The problem statement and research objectives were presented and the proposed BPSM model broadly motivated.

Chapter Two introduces the ISO 17799 security standard as the starting point for the discussion on the three research pillars. The ISO 17799 is one of the three prime foci of this research as an element of the BPSM model and it provides the necessary security controls and guidance for implementing an ISMS. It acts as the standard which allows the security metric, the SSE-CMM, as part of the information security framework, to evaluate the security within a business process which originates from the BPM environment.

2 - CHAPTER TWO – INFORMATION AND INFORMATION SECURITY MANAGEMENT

Chapter Two introduces and defines the concepts of Information Security and its management. It examines the need for information security and its drivers. The ISO 17799 security standard is examined and its security topics are discussed. The process of implementing a security management system is examined. Finally a critique of the standard is presented.

2.1 Information Security as an Enterprise Aspect

There is a growing realisation that the information of an enterprise is an important asset (Hong et al, 2003, von Solms, 2005). Data security migrated from computer security into information security due to an extended understanding of its business threats (von Solms, 2005). Perfect security is only achievable in a network-less environment located within an isolated and locked room. Information security is a compromise, based on sound best practices. Its goal is to prevent, detect and contain security breaches (Carlson, 2001).

2.1.1 The Need for Information Security

The ISBS, conducted bi-annually by Price Waterhouse Coopers and the United Kingdom Department of Trade and Industry (DTI), illustrates some notable trends in the United Kingdom (UK). The ISBS 2004 is the seventh such survey. The Internet is pervasive with some 99% of businesses in the UK embracing its use. This increased connectivity brings greater exposure to security incidents. It notes that over half of businesses electronically store highly confidential data and 87% of business are dependent on electronic information and their processing systems. The number of businesses which experienced a security incident rose from 32% in 1998 to 94% in 2004. The proportion of these which were malicious incidents rose from 18% in 1998 to 32% in 2004. Malicious incidents include viruses, unauthorised access, system misuse, fraud and theft (ISBS, 2004). Security is identified as a management priority but lacks the necessary funding (ISBS, 2002, ISBS, 2004, Dhillon, 2005). This results in a disconnect between the emphasis placed on the security policy and its controls (ISBS, 2002, ISBS, 2004).

The scope of information security is broader than the IT department, as technical solutions alone are limited in their effectiveness. A system is not adequately

secured until all its interconnecting parts, organisational, technical and operational facets, are protected (Kahraman, 2005). Information security therefore covers many issues including the security policy; risk analysis and management; contingency planning and disaster recovery.

An ISMS is defined as a management system used to establish and maintain a secure information environment (Eloff and Eloff, 2003). It is fundamental in engaging the effective and appropriate controls to protect the information assets. It is underpinned by a security policy and includes risk analysis and treatment activities. It needs to be current and maintain its focus. The Deming Wheel model (PDCA – Plan, Do, Check, Act cycle) is introduced in the BS 7799 Part 2 / ISO 17799:2:2003 as a de facto methodology which ensures the ISMS is engaged, monitored and improved on a continual basis (Theobald, 2003). The ISMS needs to be based on best-practices and guidelines and the ISO 17799 security standard offers both the benchmark against which to build information security and the mechanisms to manage the information security process (Carlson, 2001).

2.2 ISO 17799 Security Standard

There are a variety of security metrics, guidelines, standards and Codes of Practice; for example, Control Objectives for Information and related Technologies (CoBiT), BS 7799: Part 1, c:cure and the Pentana Checker Audit System (Eloff and von Solms, 2000a). The ISO 17799 standard, as the international rendition of the British Standard BS 7799, appears to have gained great acceptance. The standard was internationally accepted and published as ISO 17799 in 2000 (Fiedler, 2003).

2.2.1 The History of the ISO 17799

The concept of an international, IT security standard was initiated, in the UK, by the DTI Commercial Computer Security Centre (CCSC). Its major tasks were to, firstly, assist IT security product vendors by establishing a set of internationally recognised evaluation criteria and an associated evaluation and certification scheme which produced the Information Technology Security Evaluation Criteria (ITSEC) and the United Kingdom ITSEC Schemes and secondly, to assist users in developing a code of good security practice which resulted in a “Users Code of Practice” which was published in 1989. These were further extended by the British

Standards Institute (BSI), the National Computing Centre (NCC) and a consortium of users drawn from the British Industry, including Marks and Spencer, Midland Bank, Shell and Unilever, who ensured that the Code was both significant and practical. It was published, after various refinements, by the BSI, in 1995, as the British Standard BS 7799:1995 (Spears et al, 2004, Wynes, 2001, Carlson, 2001).

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) form a particular system for global standardisation. International Standards are proposed in accordance with conventions set down in the ISO/IEC Directives, Part 3. There was extensive revision and public consultation and Part 1 of the British Standard BS 7799 was proposed as an ISO Standard via the "Fast Track" mechanism in 1999 by the Joint Technical Committee ISO/IEC JTC 1 (ISO 17799:2000). It was published as ISO/IEC 17799:2000 in December 2000. ISO 17799 provides a non-technical viewpoint to organisational security needs (Kahraman, 2005).

The ISO 17799:2000 was not considered to be auditable and certifiable because it suggests the security control selection (Spears et al, 2004). This problem was resolved through the creation of the BS 7799 Part 2 / ISO 17799:2:2003 which specifically formulates the required activities needed by both an organisation and assessor to ensure certification. It acts as the standards specification for an ISMS which allows managers to monitor and control their security, from a top-down perspective, while applying and certifying it against ISO 17799 (Wynes, 2001).

2.2.2 An Overview of ISO 17799:2000

The ISO 17799 is high level, broad in scope and conceptual in nature. It defines information as an enterprise asset that exists in many forms which require protection. It defines the goal of information security as the protection of the information asset to ensure business continuity, minimise business damage and maximise return on investments. It is not technically-driven nor product or technology-aligned (Carlson, 2001, Spears et al, 2004).

ISO 17799:2000 contains 127 controls from 10 domains which can be designated at an organisation or application-level. It recommends that control selection is determined by a risk analysis; legal, statutory and contractual requirements and the particular set of information processing principles, objectives and requirements

unique to the organisation (ISO 17799:2000, Spears et al, 2004). The ISO 17799:2000 was replaced by ISO 17799:2005 in November 2005 and it is conceivable that the differences between the two editions may have implications for this research. The timing of the revision and release of the ISO 17799:2005 was not propitious during this research and posed the dilemma of accuracy and currency. The ISO 17799:2005 is reviewed to highlight any implications that its differences may pose on the outcome of this work.

2.2.3 Implications of the introduction of ISO 17799:2005

The differences between the ISO 17799:2000 and ISO 17799:2005, according to ISO, 'are not challenging' and 'backwards compatibility, consistency and easy transition' were foremost during the revision process. The significant changes are the inclusion of 17 new controls, the deletion and merger of others which results in a total of 134 controls. There are changes in every section ranging from numbering to the wording of clauses. The requirements of risk assessment and management commitment are clarified while the concepts of metrics and continuous improvement are expanded (IT Governance Ltd, 2005). Table 2.1 illustrates the differences in chapter structure between the two versions.

ISO 17799:2000	**ISO 17799:2005**
1. Scope	1. Scope
2. Terms and definitions	2. Terms and definition
	3. Structure of the standard
	4. Risk assessment and treatment
3. Security policy.	5. security policy
4. Organisational security	6. Organising information security
5. Asset classification and control	7. Asset management
6. Personnel security	8. Human resources security
7. Physical and environmental security	9. Physical and environmental security
8. Communications and operations management	10. Communications and operations management
9. Access control	11. Access control
10. Systems development and maintenance	12. Information systems acquisition, development and maintenance
	13. Information security incident management
11. Business continuity management	14. Business continuity management
12. Compliance	15. Compliance

Table 2.1 - ISO 17799:2000 compared to ISO 17799:2005 structure

The significant changes in the ISO 17799:2005 and their implication to this research are examined. There are three new chapters, namely the structure of the standard, risk assessment and treatment and information security incident management. The author, during the literature review, noted the importance attributed to the security policy, management commitment, risk assessment and treatment and audit processes (Carlson, 2001, ISO 17799-2:2000, ISBS, 2002, ISBS, 2004, Margaritis et al, 2001, Wynes, 2001). These appeared under-addressed in ISO 17799:2000 but are dealt with as part of an ISMS in the ISO 17799–2:2000.

The scope of information security, in ISO 17799:2005, is extended to include the monitoring, review and improvement of suitable controls to achieve the specific security and business objectives of an organisation in conjunction with other business management processes. The concept that technical security solutions are limited is addressed and the use of supporting management processes is advocated. The risk assessment and treatment chapter extends the previous security risk assessment section. It covers the periodic identification and prioritisation of risks which address the changing security and business environment. The treatment of risks, through the unique selection of controls, includes the risk acceptance criteria of an organisation and its business objectives.

The use of a management program, to monitor, evaluate and improve the effectiveness of the security controls, is advocated. The security policy and its review receive greater attention with the intent of maintaining and improving its relevance in a changing security and business environment. Management commitment was identified as a prominent issue in a security program and its ISMS. The ISO 17799:2005 acknowledges this prominence by instituting a specific control covering management support issues within the “Organising information security” chapter. The “Information security incident management” chapter aims to ensure security events and weaknesses are effectively managed and corrected. It advocates an enterprise-wide process of continual improvement to monitor, evaluate and manage information security incidents. This is akin to the PDCA cycle postulated in an ISMS (ISO 17799-2:2000, ISO 17799:2005).

The issue of metrics is significant and security metrics are discussed in this research. The ISO 17799:2005 perspective on metrics reflects the view that

measurements are part of the control mechanisms used during continuous improvement. It uses concepts from the CMM world to motivate the use of metrics to measure system effectiveness which enables the planning and execution of specific, measurable improvements. It is noted that measurements and metrics within an ISMS are still in their infancy and organisations need to develop their own appropriate solutions (IT Governance Ltd, 2005).

The ISO 17799:2005 addresses the integration of information security into business goals and notes that security is not a stand-alone issue but interacts and supports the entire organisation. It is the opinion of the author that the ISO 17799:2005 moves closer to the stated premise of this research and is in accordance with trends identified during this literature review. It appears to facilitate the goal of this research that security is treated as an integral part of the organisation and that the security posture, within a business process, can be constantly managed and improved as proposed by the BPSM model.

2.2.4 Benefits of the ISO 17799

The implementation of the ISO 17799, according to ISBS 2004, will yield concrete business benefits. The Data Protection Act of 1998 in the UK, together with similar acts in other countries, requires that businesses have a legal obligation to secure any personal information entrusted to them (Wynes, 2001). ISO 17799 provides a benchmark to build and manage the organisational security process and provides the following benefits (Wynes, 2001, Carlson, 2001):

- An internationally recognised, structured methodology;
- A set of defined processes to evaluate, implement, maintain and manage information security;
- A set of tailored policies, standards, procedures and guidelines;
- Certification demonstrates the security status of an organisation;
- Certification illustrates “due diligence”.

There are internal benefits accrued from implementing an ISO 17799-based ISMS. It provides security measurement; a set of controls; a method to set targets and suggest improvements and acts as a basis for internal information security

standards (Wynes, 2001). The ISO 17799:2000 code of practice, security domains and controls are examined in the following sections.

2.3 Information Security – ISO 17799:2000 View-point

Information security as viewed by the ISO 17799:2000 is examined together with the necessity for security. Various organisational sources of security, security risk assessment and security control selection are discussed.

The ISO 17799 defines information as a business asset which is valuable to the organisation. It is presented, stored and transmitted in various electronic, paper or graphic formats. It needs appropriate protection whatever its configuration. The goal of information security is portrayed as the safeguarding of the following (ISO 17799:2000, Carlson, 2001, Spears et al, 2004, Wynes, 2001):

1. Confidentiality. The assurance that information is only accessible to those authorised with access;
2. Integrity. The assurance of the accuracy and completeness of the information and its processing and mediating methods;
3. Availability. The assurance that legitimate users have access to the information and its associated assets when required.

Information security and specific organisational security objectives are achieved through implementing a suitable set of controls from the ISO 17799 (ISO 17799:2000, Spears et al, 2004). Organisations face threats to their information assets whilst simultaneously becoming increasingly dependent upon them (Carlson, 2001).

2.3.1 Information Security Threats

The security of organisational information and its supporting processes is essential to maintain a competitive edge, profitability, legal compliance, commercial image and organisational existence (Fiedler, 2003, ISO 17799:2000). There exists an escalating variety of security threats and vulnerabilities which include among others (ISO 17799: 2000):

- Computer-assisted fraud and sabotage;
- Computer hacking and malicious software;

- Denial of service and weakened access control;
- Dependence on IT and networks promotes security vulnerabilities;
- Environmental hazards such as floods or fires.

The achievement of effective access control has been complicated by additional complexities, such as the trend towards distributed computing and the interconnectedness of public and private networks. The security domains contained in the ISO 17799 are discussed in the next section. The ISO 17799:2000 standard is used as the main reference source.

2.4 Code of Practice for Information Security Management

The ISO 17799 standard provides the recommendations for information security management for those persons accountable for its introduction, operation and continuance. Its intention is to develop organisational security standards and effective security management practices (Spears et al, 2004, ISO 17799:2000, Carlson, 2001). It defines the following basis concepts:

i) Information security. As previously discussed, the preservation of confidentiality, integrity and information availability;

ii) Risk assessment. The assessment of threats, potential impacts and vulnerabilities to the information and its mediating facilities;

iii) Risk management. The process of identification, control, elimination or management of the acknowledged security risks.

The ISO 17799 comprises ten security domains (Spears et al, 2004, ISO 17799:2000). These and the controls within each security domain are discussed briefly.

2.4.1 Security Policy

The first security domain is the security policy. Its objective is "*To provide management direction and support for Information Security."* Management is required to provide clear policy direction and demonstrate commitment for its goals through the circulation and maintenance of the security policy (Wynes, 2001, Spears et al, 2004, ISO 17799:2000). It provides the benefit of setting the target for an effective security system from the outset (Wynes, 2001).

The security policy document requires management approval and distributing to all stake-holders. It should contain, at a minimum:

a) Information security definition comprising overall objectives and scope;

b) Management intent statement supporting the information security goals and principles;

c) Explanation of security policies, principles, standards and compliance requirements;

d) Definition of the responsibilities of information security management;

e) Documentation policy references to more detailed security procedures.

An example of the information security policy document control as detailed in ISO 17799 is provided in Table 2.2.

3 Security policy
3.1 Information Security policy
3.1.1 Information security policy document
b) a statement of management intent, supporting the goals and principles of information security;

Table 2.2 – Security Policy Document Control Example

The security policy is distributed in a format that is relevant, accessible and comprehensible for its intended audience. It is an implementation-independent, conceptual document which helps enforce policy statements (Carlson, 2001).

The security policy is an evolving document which requires reassessment at regular, defined intervals. New threats and vulnerabilities can emerge or the organisational or technical infrastructure can change. The following must be reviewed:

a) Security policy effectiveness as verified by the number of security incidents;

b) Business cost effectiveness of security controls;

c) Effects of technological changes.

It establishes ongoing, management commitment through a schedule of reviews and by assigning ownership (Carlson, 2001). The security policy and its

documentation constitute the core of the information security management strategy.

2.4.2 Organisational Security

The second security domain is Organisational Security. Its objective is "*To manage Information Security within the organisation."* A management framework is required which creates, sustains and manages the security infrastructure (Carlson, 2001)**.** A benefit is that internal and external security requirements are identified, monitored and controlled through clearly mapping the security structure of the organisation (Wynes, 2001).

Management establish a framework for introducing security and controlling its performance. It comprises a multi-disciplinary approach with broad consultation, collaboration and co-operation between the business stakeholders including management; end-users and security specialists. It contains the following controls (Carlson, 2001, ISO 17799:2000):

- Information System Security Officer (ISSO) who acts as a central contact for all security issues;
- Information security co-ordination;
- Information security responsibilities are allocated and detailed within job descriptions;
- Specialist information security advice;
- Co-operation between organisations, outsourcing and the security of Third Party access;
- Independent review of information security.

An example of the Information Security Infrastructure control as detailed in ISO 17799 is provided in Table 2.3.

4 Organisational security
4.1 Information Security infrastructure
4.1.2 Information security co-ordination
d) ensures that security is part of the information planning process;

Table 2.3 - Organisational Security Control Example

These controls define the actions necessary to define, establish and manage the information security infrastructure.

2.4.3 Asset Classification and Control

The third security domain, Asset Classification and Control, involves the accountability and protection of the assets of an enterprise. Information is valued to reflect the impact its loss will have on the organisation (Wynes, 2001). Its objective is *"To maintain appropriate protection of organisational assets".* The information assets are audited and designated an owner (ISO 17799:2000). The benefit this accountability provides is that the protection of the assets is maintained (Wynes, 2001). It contains the following controls (Carlson, 2001, ISO 17799:2000):

- Accountability and inventory of assets uses mechanisms to maintain an accurate asset inventory and assign asset ownership;
- Information classification which ensures the enterprise assets are protected at an appropriate level. The classification indicates the needed protection based on business impact;
- Classification guidelines ensure asset protection whilst taking cognisance of the business needs and impacts;
- Information labelling and handling.

An example of the control is detailed in Table 2.4.

5 Asset classification and control
5.1 Accountability for assets
5.1.1 Inventory of assets
a) information assets: databases and data files, system documentation…archived information;

Table 2.4 – Asset Classification and Control Example

These controls define the correct handling of the security of the assets of the enterprise.

2.4.4 Personnel Security

The fourth security domain, Personnel Security, aims to reduce the human risks to an information security system. Its objective is "*To reduce the risks of human error,*

theft, fraud or misuse of facilities." It is ideally addressed during staff recruitment, job definition and through on-going performance reviews. Its aim is to mitigate the risks inherent in human interactions (Carlson, 2001). It includes the following controls (Carlson, 2001, ISO 17799:2000):

- Security is included in job description;
- Personnel screening and policy includes the vetting of prospective employees;
- Confidentiality agreements and conditions of employment;
- User training to ensure that the users support the security policy and are trained in the correct operation of the Information Processing facilities;
- Responding to security incidents and malfunctions involves the reporting, monitoring and improving of security incidents, and minimising their damage.

An example of a control is detailed in Table 2.5.

6 Personnel security
6.1 Security in job definition and resource-ing
6.1.2 Personnel security in job responsibilities
c) confirmation of claimed academic and profession qualifications;

Table 2.5 - Personnel Security Control Example

These controls define the correct handling of Personnel Security within the enterprise. They enable the checking of security, by all the stakeholders, on a regular basis (Wynes, 2001).

2.4.5 Physical and Environment Security

The fifth security domain, Physical and Environmental Security, aims to prevent harm or illegitimate access to the business premises and the information assets (Wynes, 2001, ISO 17799:2000). It addresses the risks inherent in the organisational premises (Carlson, 2001). Its objective is *"To prevent unauthorised access, damage and interference to business premises and information."* Critical business information processing facilities require housing in secure, physically protected, controlled areas. The information assets require protection which is

commensurate with their identified risk. It includes the following controls (ISO 17799:2000):

- Physical security perimeter. This is defined and physically sound with appropriate access control;
- Physical entry controls. Supervised and reviewed access rights;
- Securing offices, rooms and facilities.

The danger of a natural or man-made disaster is considered. Equipment security necessitates the prevention of information loss, compromise, damage or service interruption. The general controls protect the information and its processing facilities from unauthorised disclosure, modification and theft. An example of the control is detailed in Table 2.6.

7 Physical and environmental security
7.1 Secure areas
7.1.3 Securing offices, rooms and facilities
a) Key facilities should be sited to avoid access by the public;

Table 2.6 - Physical and Environmental Security Control Example

The surroundings are analysed for environmental hazards and policies are implemented which govern the operational security within the workspace, using such tactics as 'clean desk' principles (Carlson, 2001). These controls define the necessary measures to deliver physical and environmental security.

2.4.6 Communications and Operations Management

The sixth security domain, Communications and Operations Management, guarantees the accurate and secure functioning of the information processing services. Its objective is *"To ensure the correct and secure operation of the information processing facilities."* The responsibilities of management, operating manuals and incident response procedures for the IS facilities need establishing. It includes the following controls (Carlson, 2001, ISO 17799:2000):

- Operational procedures provides a set of procedures which support the organisational standards and policies;
- Change control entails managing changes to the information processing infrastructure and the ISMS;

- Incident management procedures provides mechanisms which ensure effective response to security incidents and include evidence collection for problem analysis;
- Segregation of duties minimises the potential for collusion and uncontrolled exposure;
- Separation of development and operational activities;
- System planning and acceptance ensures the reduction of system failures through capacity planning to ensure uninterrupted availability and methodologies which evaluate systems changes to ensure security;
- Protection against malicious software;
- Housekeeping which establishes routine procedures, such as backup schedules, to maintain the integrity and availability of the information processing and communication services;
- Network management ensures the secure operation of the enterprise network, its supporting infrastructure and information;
- Media handling and security which secures the information assets and prevents interruptions to business activities through appropriate protection procedures;
- Exchanges of information and software manages the secure exchange of information and software between organisations according to relevant legislation and includes end-user agreements and information transport mechanisms.

An example of a control is detailed in Table 2.7.

8 Communications an operations management
8.2 System planning and acceptance
8.2.2 System acceptance
a) performance and computer capacity requirements;

Table 2.7 - Communications and Operations Management Control Example

These controls define the necessary measures to deliver the essential communications and operations management security for the information

processing facilities. The documented procedures demonstrate that current and new information is secure from loss, corruption or disclosure (Wynes, 2001).

2.4.7 Access Control

The seventh security domain, Access Control, controls access to the information and its business processes. It is managed on a security and business requirements basis. The internal end-users and the access means are emphasised (Wynes, 2001). Its objective is *"To control access to information."* The information dissemination and authorisation policies are evaluated. It includes the following controls (Carlson, 2001, ISO 17799:2000):

- Access policy governs access to the information assets and is based on business requirements;
- User management involves preventing unauthorised access through formal procedures managing the allocation and control of access rights;
- Network access control involves the policies for protecting and controlling internal and external network usage;
- Operating system access control limits access based on user- or application-authorisation levels and includes controls such as password management;
- Application access control prevents unauthorised access to the information assets within the applications-based systems and restricts access within those systems;
- Monitoring system access detects unauthorised access and assesses the effectiveness of the security controls;
- Mobile computing and teleworking controls address security whilst using either mobile computing or teleworking. These environments have particular risks and require rigorous protection.

An example of a control is detailed in Table 2.8.

9 Access control
9.5 Operating system access control
9.5.4 Password management system
a) enforce the use of individual passwords to maintain accountability;

Table 2.8 - Access Control Example

These controls define the necessary measures to deliver access control security for the information asset, its processing infrastructure and its stakeholders.

2.4.8 Systems Development and Maintenance

The eighth security domain, Systems Development and Maintenance, ensures that the appropriate requirements for the security controls are identified, incorporated and maintained, as part of the business case, within an IS project (Carlson, 2001, ISO 17799:2000). Its objective is *"To ensure that security is built into information systems."* The security requirements are identified and agreed upon prior to IS development. Their design and implementation into the supporting business processes is vital to ensure security. It includes the following controls (Carlson, 2001, ISO 17799: 2000):

- Security requirements analysis and specifications incorporate the information security requirements. They are based on business requirements and reflect the business value of the information assets;
- Application security requirements prevent the loss or abuse of the information asset within the application systems. Their design includes the appropriate controls, audit trails and activity logs which are determined by the security needs, through risk assessments and by their business impact;
- Cryptographic controls provide a degree of protection for vulnerable information assets against which other controls are deemed inadequate and includes Usage Policies, Digital Signatures and Key management standards, procedures and methods;
- System integrity includes mechanisms that ensure the operational data and software are secure and includes access control, integrity verification and monitoring processes;
- Security in development and support processes ensures the project and support environments are strictly controlled to maintain application and information security.

An example of a control is detailed in Table 2.9.

10 System development and maintenance
10.5 Security in development and support processes
10.5.1 Change control procedures
a) maintaining a record of agreed authorisation levels;

Table 2.9 - System Development and Maintenance Control Example

These controls define the measures necessary to ensure security is integrated into the systems development and maintenance. Security is incorporated into the IS infrastructure, business applications, user-developed applications and the information assets. Controls applied at the design stage are appreciably more cost-effective and functional than security instituted at later stages.

2.4.9 Business Continuity Management

The ninth security domain, Business Continuity Management, ensures that any disruptions to the information processing facilities are reduced to a tolerable level by using precautionary and salvage controls. Its objective is *"To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters."* (Carlson, 2001, ISO 17799:2000). Risk analyses are completed and contingency plans are installed to protect and restore vulnerable business processes. Controls, which reduce and limit risk and ensure the prompt recommencement of essential operations, are identified. It includes the following controls (ISO 17799:2000):

- Business continuity management process is a development and management program, based on a business impact analysis, which includes:
  - Critical business process - risk analysis;
  - Business objectives of information processing facilities and the impact of their failure;
  - Business continuity strategy formulation;
  - Business continuity plans pertinent to this strategy;
  - Review and update of these plans and processes;

  - Incorporation of business continuity management into the organisational structure;

- Drafting and implementation of the continuity plans;
- Business continuity planning framework which comprises continuity plans, each with an owner responsible for the fallback procedures and resumption plans;
- Testing, maintaining and re-assessing business continuity plans. The recovery plans require review, cyclical re-evaluation and revision to guarantee their appropriateness and continuing efficacy.

An example of the control is detailed in Table 2.10.

11 Business continuity management
11.1 Aspects of business continuity management
11.1.1 Business continuity management process
a) understanding the risks the organisation is facing … of critical business processes;

Table 2.10 - Business Continuity Management Control Example

These controls define the necessary measures to ensure an effective business continuity management framework and process. It provides the benefit that potential security hazards can be recognised and controlled (Wynes, 2001). Disaster recovery teams are formed to test the efficacy of the business continuity plans (Carlson, 2001).

2.4.10 Compliance

The tenth security domain is Compliance which addresses the ability of the organisation to remain in compliance with various statutory, regulatory and contractual security requirements (Wynes, 2001, Carlson, 2001). Its objective is *"To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements."* Legislative requirements are location specific and trans-border data flow requires special consideration. The specific legal requirements can be ascertained from qualified professionals. It includes the following controls (Carlson, 2001, ISO 17799:2000):

- The relevant statutory, regulatory and contractual requirements are identified and the requisite security controls are defined and documented;
- Intellectual property rights (IPR) require compliance with the copyright, design right, trademark and software copyright laws;
- Safeguarding the organisational records protects them from loss, destruction and falsification and they must be securely retained to meet statutory requirements and support essential business activities;
- Prevention of the misuse of the information processing facilities requires management to institute a policy of authorised business usage;
- Collection of evidence. A business action requires adequate supporting evidence and the controls include the rules for evidence, admissibility, quality and completeness;
- Technical compliance involves mechanisms to review regularly and verify the security policy execution and implementation and ensure its compliance;
- System audits needs controls to safeguard the operational systems and audits tools during the system audits to maximise their effectiveness whilst minimising interference.

An example of the control is detailed in Table 2.11.

12 Compliance
12.1 Compliance with legal requirements
12.1.3 Safeguarding of organisational records
a) Guidelines should be issued on the retention, storage, handling…of records and information;

Table 2.11 - Compliance Control Example

These controls define the necessary measures to ensure effective compliance in the IS. The risk of prosecution from non-compliance is reduced through instituting a variety of compliance controls (Wynes, 2001).

The ten security domains that comprise the code of practice for the ISO 17799:2000 security standard were examined. Next their process of identification and selection is examined as part of implementing an ISMS.

2.5 ISO 17799 Information Security Management System

The ISO 17799 standard contains various annexure of which Annex B specifically deals with guidance on its use. The initiation and management of an ISMS, using the ISO 17799, uses a process management approach, exemplified in the PDCA model, which ensures best practices are documented, reinforced and continually improved (ISO 17799:2000, ISO 7799-2:2003).

A process ISMS is defined as a two-phase structure that establishes and maintains information security by planning and implementing management practices, procedures and processes. The controls or guidelines contained in a code-of-practice, such as ISO 17799, are, firstly, implemented and, secondly, assessed to determine their compliance against the specified standard. It is an iterative system using feedback and continuous improvement as illustrated in the PDCA model (Eloff and Eloff, 2003).

Carlson (2001), in Information Security Management: Understanding ISO 17799, describes the process for implementing an ISMS based on ISO 17799, which comprises the following phases:

Phase 1. Obtain upper management support;

Phase 2. Define security perimeter;

Phase 3. Create information security policy;

Phase 4. Create information security management system;

Phase 5. Perform a risk assessment;

Phase 6. Select and implement the control;

Phase 7. Document the statement of applicability;

Phase 8. Audit.

These steps are both supported and expanded upon by the ISO 17799:2000 and ISO 17799-2:2003 and are examined in detail.

2.5.1 Phase One - Obtain upper management support

A crucial component to the success of an ISO 17799 program is the support from upper management. The process of initiating a compliant infrastructure is arduous and requires long-term dedication which is promoted by obvious commitment from

management. Information security is a process rather than a program and security must be inculcated as an organisational lifestyle to ensure its success (Carlson, 2001). Management support is addressed in various sections in the ISO 17799.

The ISO 17799-2:2003 embraces management support under Section 5, Management responsibility. It specifically mentions that evidence of support management will promote commitment to all phases of the ISMS. It notes areas where management commitment is especially important and these include during establishing the information security policy and setting the security objectives, roles and responsibilities, resource provision, risk assessment and ISMS review (ISO 7799-2:2003).

2.5.2 Phase Two - Define security perimeter

The definition of the security perimeter is an early and difficult task. It is the security domain which, conceptually, is certifiable by the ISO 17799. It may not encompass the entire organisation, however, the security perimeter or domain is always under its control. An area that is outside the control of the organisation, cannot be effectively managed by it (Carlson, 2001).

The ISO 17799-2:2003 addresses the security perimeter under Annex B.2.3 Scope of the ISMS. An ISMS can cover all or portion of the organisation and clearly identify its dependencies, interfaces and any assumptions about its boundary to its environment. Its documentation includes the processes used to establish its scope; its strategic and organisational context; the organisational approach to risk management and the identification of the information assets within the ISMS scope. An ISMS that is within the control of a Quality Management System, another Management System or another ISMS, is only responsible for the management controls within its own scope (ISO 17799-2:2003).

2.5.3 Phase Three - Create information security policy

Information security policies are tailored towards their particular audiences and take different formats within one or several documents. Their goal is the same – a high-level, implementation-independent statement displaying management direction and support of the ISMS (Wynes, 2001, Carlson, 2001, ISO 17799:2000, ISO 17799-2:2003). They define the ISMS strategy, objectives, intensions and

responsibilities (Fiedler, 2003). They are vital in information security management (Hong et al, 2003).

Information security policy enforcement is a development trend that influences the management of security. Information security management is not possible without a security policy providing guidelines about what must be managed. The security policy comprises the documented security decisions about the IT infrastructure and its information assets (von Solms and Eloff, 2001). Hong et al (2003) maintain that the security policy aims to plan the information security requirements whilst forming a consensus in the organisation which drafts, implements and reviews it, ensuring it remains current.

The ISO 17799:2001 Section 3, Annex B of the ISO 17799-2:2000 and ISO 17799-2:2003 Task B 2 address the information security policy (ISO 17799:2000, ISO 17799-2:2003). The security policy statement is similar to the mission statement of any organisation and is sufficiently non-specific to allow public disclosure (Carlson, 2001).

The ISBS 2002 identified the creation and implementation of a security policy as one of the top ten required actions for management (ISBS, 2002). The ISBS 2004 reveals that it does not receive the practical attention that its priority warrants (ISBS, 2004). This prompts a critique of the security policy itself.

2.5.3.1 Critique of information security policy

There appears to be agreement about the importance of the security policy as the foundation of good information security management, however, there is a paucity of research into its creation. There is a plethora of beliefs about the security policy. Some computer researchers use the term ‘policy’ to describe access control rules, whilst others distinguish various forms of policies. Examples include viewing the security policy objective as ‘ a statement ... to protect an identified resource from unauthorised use’ or as an organisational security policy which describes how to achieve these objectives or as an automated security policy which views how an IS protects its own resources. Other researchers differentiate between a corporate or upper-level management policy, an organisational or user-level policy and a technical or designers’ view security policy. There equally exists confusion

between the concepts of guidelines, standards and policies (Baskerville and Siponen, 2002).

It is, therefore, not without good reason that organisations, when confronted with this morass of definitions and similar, are unable to focus attention on a security policy. They are unable to find clarity on its role, relevance and position and this is an area where action needs to be taken. Baskerville and Siponen (2002) propose a three-level division for the security policy. At its high-level, it addresses general security goals and procedures using a high degree of abstraction. At its next lower level, its policies address the defined security methods while at its third level, it is a meta-policy which comprises an enterprise-wide plan for creating and operating its information system policies and includes the timing of its creation and its owners. The ISO 17799 demonstrates increased attention to the meta-policy (Baskerville and Siponen, 2002).

2.5.4 Phase Four - Create information security management system

Hong et al (2003), Carlson (2001) and ISO 17799-2:2003 advocate establishing and maintaining a documented ISMS, as a framework, to control the security process. The ISMS defines the security perimeter and sets its own ISMS policy, as a meta-policy. It develops a framework for setting the objectives and overall direction of the security actions. It considers the relevant business, legal and contractual security obligations and establishes the strategic, organisational and risk management context. It establishes risk evaluation criteria and the structure of the risk assessment process. These are used in information security strategies for each of the controls in the ISO 17799 (ISO 17799-2:2003).

These information security strategies often need the creation of policies, plans, committees and teams. The security policy will demonstrate management support. It is important to identify an Information System Security Officer (ISSO) to coordinate and take ownership of the ISMS (Carlson, 2001, ISO 17799-2:2003). The duties of the ISSO must be formally defined and include: leading the Management Security Forum and Incident Response Teams; ISMS maintenance, control selection and risk mitigation; documentation maintenance; external security contacts control and consulting on general information security issues (Carlson, 2001).

2.5.5 Phase Five - Perform security risk assessment

The ISO 17799 and particularly, the ISMS, deal with the management of risk (Carlson, 2001, ISO 17799-2:2003). Carlson (2001), ISO 17799-2:2003, Hong et al (2003) and Margaritis et al (2001) propose that the use of risk management theory, through risk analysis and threat and vulnerability evaluation, can plan the information security requirements and risk control measures. The goal is to reduce information security risk to an acceptable level within an organisation. A simpler viewpoint maintains that risk materialises through the incidence of an event or security failure and its consequences are the damage it causes through its adverse impact and during the recovery process (Brewer and List, 2004).

Risk assessment is defined as a systematic consideration of the business harm likely to arise from a security failure, considering any potential consequence from the loss of confidentiality, integrity or availability of the information or other assets. The realistic likelihood of such a failure occurring in the current situation is considered (ISO 17799:2000). There are discrete tasks within the security risk assessment activity which are examined.

First, the assets and their owners within the security perimeter are identified. An asset, to reiterate, can be tangible, such as hardware, or be intangible, such as an organisational database. They have organisational value which needs to be determined. This enables worth to be established for each asset when its risks are quantified (ISO 17799:2000, Carlson, 2001, Margaritis et al, 2001).

Second, the threats to the assets are identified. Threats exploit any vulnerabilities of the assets which creates risks. Each asset can have multiple vulnerabilities (Carlson, 2001). The business risks include unauthorised access, client service denial and loss of business. Those threats which have a significant probability or will cause extreme harm are considered (Margaritis et al, 2001, Carlson, 2001).

Third, the vulnerabilities to the assets are identified. Vulnerabilities are recognised deficiencies in the assets which can be exploited by the threats to create risk. Assets can have multiple vulnerabilities, for instance, an organisational database which has both weak access control and poor backup procedures (Carlson, 2001, Margaritis et al, 2001).

Fourth, the threats/vulnerabilities which can cause a security failure and the associated impacts are assessed. Threat/vulnerability combinations which are statistically insignificant may be ignored (ISO 17799-2:2003, Carlson, 2001).

Fifth, the risk is calculated. A goal of the ISO 17799 is the evaluation and mitigation of risk. Carlson (2001) views risk as a function of probability and harm. Hong et al (2003) calculates risk as a function of the impact of the failure as related to the value of the asset. This provides a numeric rating of asset-based risk for a given set of threats and vulnerabilities which allows for the prioritising of risk-mitigating resources (ISO 17799-2:2003, Carlson, 2001).

Margaritis et al (2001) propose a process of risk quantification which evaluates the cost of preventing the security failure in terms of time, expense and resources required. This is to be undertaken in conjunction with a cost assessment of the possible damage associated with each threat. The identified risks are graded according to their probability, the severity of impact and the cost of protection. Information assets are of critical business importance and need protection proportionate to their value against defined business goals (Margaritis et al, 2001). ISO 17799-2:2003 Section 4 and Annex B.2.3 address the ISMS specifically and details the risk assessment activities (ISO 17799-2:2003). The effectiveness of the ISO 17799 process is reliant on the accuracy of the security risk assessment because risks that are unidentified cannot be mitigated.

Security risk assessment provides management with guidelines and priorities to manage the security risks and to select the necessary controls to protect against those risks. Both the risk assessment and the selected controls require periodic review because changes occur to the business environment which results in threat/vulnerability changes and priority changes (ISO 17799:2000). Control selection is decided by the availability of resources and the decision to accept a degree of risk (Carlson, 2001). Security controls are more cost-effective and efficient when incorporated into the IT requirements and design stages. Security risk assessment provides a variety of organisational benefits.

2.5.5.1 Benefits of security risk assessment

There are a range of benefits accrued from performing a security risk assessment. It provides a cost justification because security controls involve expense which

requires financial justification. There is an increase in productivity through the security review forums which share knowledge and enhances security audit team productivity. Security is addressed between all the stakeholders and IT staff levels and business barriers are removed. Security development becomes part of the organisational culture and each business unit bears the responsibility for its security. There is greater security awareness because the broad application of the assessment places security at the focal point of the enterprise. Security is correctly targeted and relates to potential and existing impacts and threats. It establishes a baseline security. The assessment identifies both shortcomings and security observance (Wynes, 2001).

There are tangible internal benefits accrued from implementing an ISO 17799-based ISMS. These include measuring the current security status and introducing a set of security controls. A method of setting security targets and for motivating improvements is installed (Wynes, 2001). The security risk assessment guides the selection of the appropriate security controls which mitigate the previously identified risks (ISO 17799:2000).

2.5.6 Phase Six - Security control selection

The risk assessment process identifies the security requirements which guide the selection of the security controls. Controls are selected to reduce, avoid or transfer the security risk and rely on asset availability and the willingness of management to accept risk liability. The areas of highest risk are identified and used for priority setting (Carlson, 2001, ISO 17799-2:2003). Controls are either selected from the ISO 17799 or custom-designed. They need to be cost-effective whilst non-monetary factors, such as the loss of reputation, are recognised as intangible costs (ISO 17799:2000, ISO 17799-2:2003). There are three types of security controls (Brewer and List, 2004):

- Preventative which aim to ensure the event never occurs or, at least, detects the event and prevents any further damage;
- Detective which identify the incidence of an event and invoke appropriate remedial action;
- Reactive which identify the event has occurred and invoke appropriate recovery or mitigation actions.

A backup copy to external media, stored off-premises, is an example of a preventative type control because secure copies of the information exist, and a reactive type control because it is possible to recover the data into an uncorrupted state.

The ISO 17799 security controls are guiding principles for information security management and are broadly applicable. They are based on legislative requirements and information security best-practices. There are controls considered essential from the legislative and best-practice viewpoint which include (ISO 17799:2000):

1. Data protection and privacy of personal information – Section 12.1.4;
2. Safeguarding of organisational records – Section 12.1.3;
3. Intellectual property rights – Section 12.1.2;
4. Information Security Policy document – Section 3.1;
5. Allocation of Information Security responsibilities – Section 4.1.3;
6. Information Security education and training – Section 6.2.1;
7. Reporting Security incidents – Section 6.3.1;
8. Business continuity management – Section 11.1.

There are controls that are business process specific and are significant to this research and include (ISO 17799: 2000):

1. Accountability for Assets – Section 5.1;
2. Information Classification – Section 5.2;
3. Segregation of duties – Section 8.1.4;
4. Electronic commerce security – Section 8.7.3;
5. Media Handling and Security – 8.6;
6. User responsibilities – 9.3.

These controls are applicable to most organisations. Their importance is determined by the security challenges an organisation faces. They represent an appropriate starting point but do not replace the selection of controls based on a risk assessment (ISO 17799:2000).

2.5.7 Phase Seven - Create a Statement of Applicability

A Statement of Applicability (SoA) is created after the controls are selected. It formally documents the objectives of the controls, their selection and the reasons for their selection. The risk treatment plan and security risk assessment methods are documented together with the risk mitigation strategy. Excluded controls are documented together with the reasons for their exclusion (Hong et al, 2003, Carlson, 2001, ISO 17799-2:2003). It addresses the ISO 17799 control areas and tabulates the selection or absence of controls with their rationale. It documents the steps the organisation has taken to ensure its security (Carlson, 2001).

The ISO 17799 requires the preparation of an SoA and it is a working document required for ISMS certification. It recommends making available a Summary of Controls (SoC) which is relevant to the organisational ISMS. It facilitates inter and intra-business relationships by providing information about the installed security controls. These are sensitive documents which require the necessary care during their dissemination (ISO 17799-2:2003).

2.5.8 Phase Eight - Audit of ISO 17799

The audit allows the review of the information security infrastructure (Carlson, 2001, ISBS, 2002, ISBS, 2004). The ISMS is reviewed to determine whether its objectives, controls, processes and procedures conform to the ISO 17799 standard and any other relevant legislation. It is reviewed to ensure that it conforms to the identified security requirements which are effectively implemented, maintained and are performing to target (ISO 17799-2:2003, ISBS, 2002, ISBS, 2004).

Hong et al (2003) maintain an information audit should be undertaken regularly to assess control performance and information security is viewed as a function of the established control system, its implementation and the information audit. ISO 17799 advises scheduling the audit programme on the status of processes and areas under audit and on the previous audit results. The roles and responsibilities of the audits together with their planning, execution and reporting are documented. The results of the audit are used to continually improve the effectiveness of the ISMS through the analysis of monitored and audited events. These improvements are either corrective or preventative actions to eliminate the cause of non-

conformities or other undesirable conditions to prevent their repetition (ISO 17799-2:2003).

Audits are classified as First Party when performed by the organisation itself, Second Party when the customer or business partner conducts the audit and finally, as Third Party when an independent auditor performs the audit which is used for conformance certification (Carlson, 2001). Internal certification is done by the organisation as a first party audit but it receives no official recognition. External certification uses an independent and recognised third party to perform the assessment process which results in formal certification The implementation of the ISO 17799 controls does not imply their certification which is important to establish trust between intra- and inter-enterprise processes. The controls and guidelines in the ISO 17799 are implemented and assessed which determines their compliance (Eloff and Eloff, 2003).

The eight steps process proposed by Carlson (2001) to implement an ISMS based on ISO 17799 were discussed. There are other models which use the ISMS process. Wynes (2001) ISMS-based model, for example, derives its key factors from the ISO 17799 and labels its steps as: Define a security policy; Define the scope of the ISMS; Undertake a risk assessment; Manage the risk; Select the security controls and their objectives and Prepare an SoA. There are similarities between the various ISMS implementation models.

The ISO 17799:2000 standard, together with its ten domains and the process of implementing an ISMS based on the standard were described. There are certain limitations in the ISO 17799 standard and these merit examination.

2.6 Critique of ISO 17799 Security Standard

The following critique is based on the approach of ISO 17799 and not on its contents. It is based mainly on the research of Mikko T Siponen, a professor in the Department of Information Processing Science at the University of Oulu in Finland. His body of published research is extensive and covers a wide variety of information security topics within the arena of information standards, models, management approaches and methodologies. He is respected in the information security field and is an author who presents academic works of critique within this arena. It is not easy to critique this burgeoning field of information security

because it is a new and changing environment and works of critique are not plentiful. However, as a researcher in this field, the author agrees with the sentiments expressed.

Security aspects have historically been ignored in IS development methods and several IS security methods are proposed to overcome this omission. Security checklists and management standards are classified as normative management-oriented security standards and they are widely touted as pivotal to security management by various journals, for example Computers and Security, and by security practitioners and academics (Siponen, 2003). However, they are criticised as being mechanistic without sufficient emphasis on the social nature of organisational security or the security requirements needed. It is noted that the advocates of these standards/checklists have yet to reply to these criticisms which is contrary to the "self-corrective' approach of academic research (Siponen, 2002b, Siponen, 2003).

Tse (2005) describes the ISO 17799:2000 as a code of practice developed by computer security technologists addressing the possession, authenticity and utility of information. It does not, however, address major information threats and is vague about the concepts of auditing and reviewing. A major weakness is its inability to help an organisation to improve its processes because it is only possible to be "ISO 17799 certified" or "Not ISO 17799 certified" and the assessment merely involves ensuring there are sufficient controls in place (Tse, 2005).

Siponen (2003) in, Information Security Management Standards: Problems and Solutions, critiques various standards including the BS 7799/ISO 17799. It is described as a management standard and it provides guidance about countermeasures which guide development and, therefore, is a normative standard. However, Siponen believes that it is ambiguous to label it as a management standard because it presents a list of controls and procedures but does not provide help to overcome managerial problems that arise during its implementation (Siponen, 2003). It pays little attention to the conflicts that may arise between business needs and the security needs of an organisation. It is broadly-written, failing to consider that organisations and their security needs

differ, which compels the stakeholders to make ad hoc managerial decisions (Siponen, 2002b).

The ISO 17799 is also vulnerable to further criticisms. The “Is from Ought” problem implies that standards are built by prescribing the prevailing industrial practices as best-practices because they present an existing industry practice. The ISO 17799 yields to the “Is-from-Ought” myth because it does not address unique security needs but instead, prescribes universal procedures advocated by security practitioners. The irrationalist research process implies the standards have not been allowed the opportunity to prove the validity of their observations or the underlying research process. Irrationalism is evident in ISO 17799 because the standard is not sufficiently validated and reflects the experiences and partiality of its developers. It maintains its controls are widely accepted as best practice but the research methods used to obtain this result are unknown. Normative standards do not publish their observations nor test their work further and ignore related work or relevant objections (Siponen, 2003).

It is within the security community and the developers of the standards that the final critique is directed. Siponen (2002b) describes the practitioner community as comprising a set of practitioners working in the field of information security who may not have a serious academic research attitude and their research solutions are often based on intuition and personal experience rather than research problems and agendas put forth by colleagues and scientific journals and conferences. It is the practitioner community who promote normative standards and risk management. These problems require further quantitative and qualitative research, such as interpretive field studies, surveys, action and case studies, to achieve greater validity. This is beyond the scope of this research area.

It appears that normative standards are vulnerable to a varying degree of criticisms. Therefore, the limitations of the ISO 17799 are noted. However, because it is well-accepted and widely adopted within industry, is used globally and is well-advocated within the security practitioner community, it is used as the security standard in this research.

2.7 Conclusion

The concepts of information security and its management were examined together with the role of information as an organisational asset. The ISO 17799 security standard was examined, its history and its code of practice were detailed. The process of risk analysis and risk assessment and the benefits garnered from executing such processes were examined. The process of implementing an ISMS based on ISO 17799 was detailed, with a critique of the Information Security Policy. Finally, a critique of the standard was presented. The ISO 17799 security standard is proposed as the security standard that guides the selection of security controls or counter-measures and provides the framework for implementing an ISMS within the BPSM model. It acts as the standard which allows the security metric, the SSE-CMM, to evaluate the security within a business process as part of the BPSM model. The inclusion of ISO 17799 into an ISMS can be facilitated using a CMM to rate the security of the business processes. Chapter Three introduces and discusses the CMM and its security version, the SSE-CMM. The BPSM model proposes using the SSE-CMM to evaluate the security engineering process, provide the security metrics for the security posture within the business process and identify improvement opportunities.

3 - CHAPTER THREE – SECURITY MATURITY MEASUREMENT

Chapter Two introduced the need for security and discussed the ISO 17799 security standard. Information security management and an ISO 17799-based ISMS were examined. The importance of information was discussed and its threats which represent risks to the quality, effectiveness and existence of the organisation. Information security is the response to these threats.

Chapter Three introduces and discusses the CMM and its security version, SSE-CMM. The current increased need for integrated security is examined, together with security engineering concepts. The concept of maturity levels and their role in security improvement is considered. The SSE-CMM is the second pillar of this research and is proposed as the security metric, to evaluate the ISO 17799-based security controls, within the information security management framework of the BPSM model. It will be used to evaluate, monitor and improve the security position of the business process.

3.1 Motivation for a Capability Maturity Model

Quality is, according to Bardoloi (2004), judged to be a core organisational competency and an organisation is identified, within its market, by the level of quality it maintains. Its lack can cause a loss of reputation and competitive edge as customers become increasingly dissatisfied. This quest for quality has led to the development of a variety of maturity models of which the CMM is one example. These maturity models deal with process management and improvement to increase efficiency, control and quality. CMM uses the principles of statistical quality control in a maturity framework to establish project management. This is the basis for CPI (SEI-CMM, 1993). It is pertinent to introduce the concepts of quality and process management prior to discussing the CMM.

3.2 Statistical Process Control

The characteristics of the higher maturity levels within CMM are based on Statistical Process Control (SPC) concepts (SEI-CMM, 1993). These are exemplified in the Juran Trilogy Diagram, Figure 3.1, discussed next, which illustrates the primary goals of process management. Quality Management comprises Quality Planning, Control and Improvement. First, Quality Planning aims to provide the product/service producers with the resources to produce a

satisfactory product. Re-work and waste is inevitable because defects will occur. Waste is treated as chronic and is intentionally built into the process. Second, Quality Control is performed to prevent the waste from escalating. Sporadic spikes in the process, as illustrated, represent 'fire fighting' or crises management activities. The area of Chronic Waste provides the Quality Improvement opportunities as the final managerial process. It is necessary to manage a process so that it operates within a zone of quality control – this is process control. There are inevitably some chronic waste and sporadic spikes but the system is generally stable. CPI occurs when the process is changed to improve quality and the zone of quality control shifts creating a new performance baseline (SEI-CMM, 1993).

The Juran Trilogy Diagram

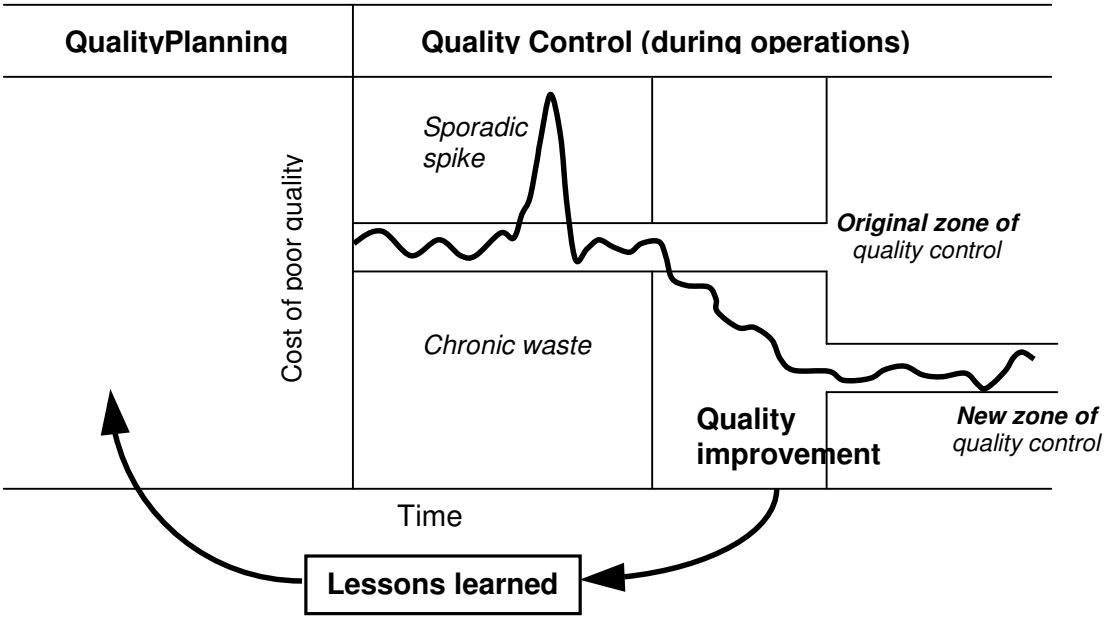
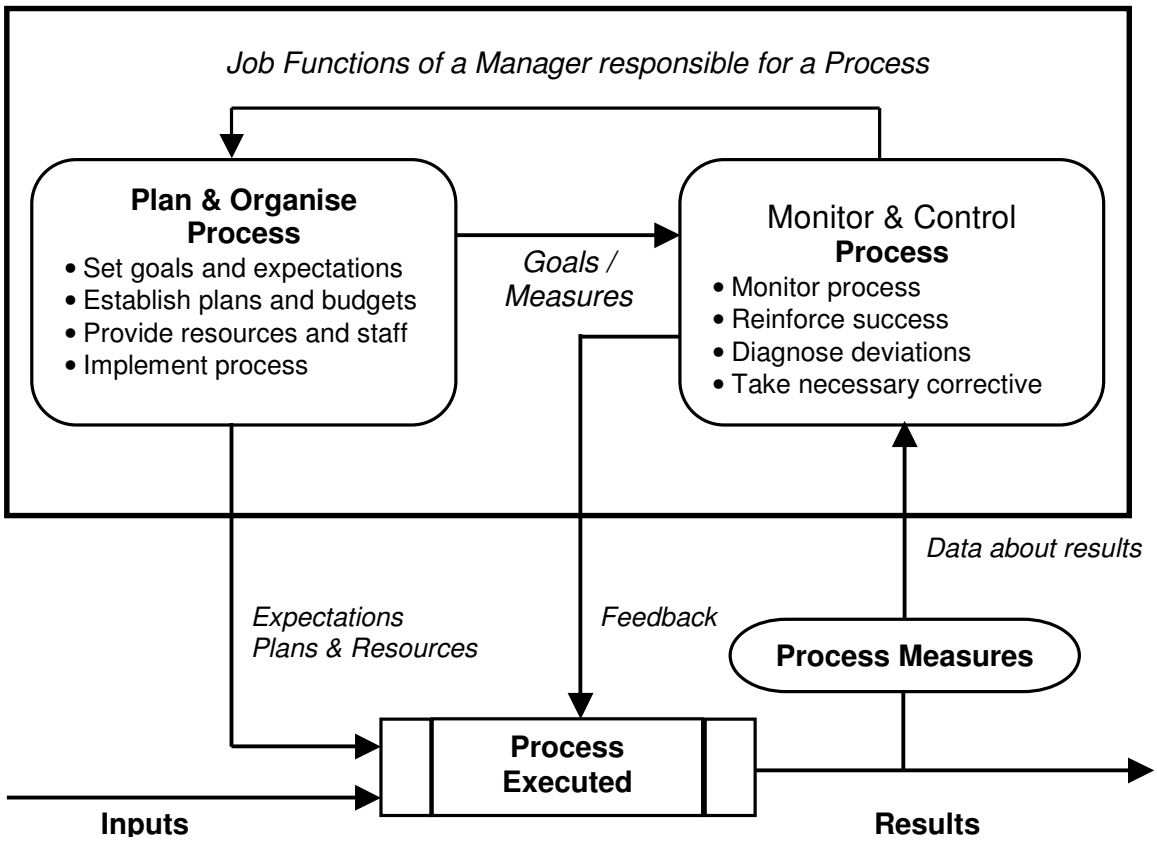


Figure 3.1 - The Juran Trilogy Diagram: Quality Planning, Quality Control, and Quality Improvement

Source - Capability Maturity Model for Software, Version 1.1

Traditional SPC, as advocated by Juran and Deming, has existed since the Fifties. Its tools include the PDCA cycle, data collection and analysis, graphs and charts to explain trends (Bhote, 1988). SPC, according to Pieterse (2005), is described as the process of "using statistics to determine the extremes between which a measuring parameter should fall, and then to take action only when the measured point strays outside these two extremes." An example of a system in SPC

illustrates that, in a stable system, its capability is within a specific range and the limits of variation are predictable. This statistical control needs to be established



before effective improvements can be made (SSE-CMM, 2003).

Figure 3.2 - A basic Process Management Model - Sourced Harmon (2004)

3.3 Process management

Process management is a core activity in any process-driven strategy (PPI Research Report, 2004, Harmon, 2004, Smith and Fingar, 2004a, Rosemann and de Bruin, 2005, Lee and Dale, 1998). It is pertinent to discuss this concept and its ramifications on CMM. Harmon (2004) presents a concise Process Management model based on the work of Geary Rummler.

The Process Management model, as illustrated in Figure 3.2, provides a management perspective. A manager is responsible for goal setting, process planning, resource provision, results monitoring and the necessary remedial actions for a specific process. This model is applicable to all levels of management whose tasks are divided into two broad groups; Planning and Managing. First, the Planning Process requires management to define the process in terms of its scope, inputs and outputs. Its context within the value chain is considered to avoid

a silo mentality. The process is implemented once its budget and plan are complete. The Process Executed stage comprises operations which are manual, computerised or both. Finally, Managing begins once the process begins functioning and comprises monitoring and control activities. Process goals are converted into specific measures which are compared against the process results. Preventative or corrective actions are taken to assure these goals are met. The level of remedial action taken by a manager, corresponds to his/her position in the management hierarchy. A top-level manager will correct a deviation by holding lower-level managers responsible while at the employee-level, corrective action takes the form of feedback, retraining or restructuring the task (Harmon, 2004). These activities are comparable to the PDCA cycle of Deming and to maintaining a process in SPC.

Lee and Dale (1998) investigate process management from a BPM viewpoint. It is viewed as a process during which processes are identified, documented and measured for effectiveness and, finally, improved. This is analogous to the PDCA cycle and to the ethos behind the CMM. The maturity of an organisation is evaluated by how management, together with their measurement processes, view process management (Harmon, 2004). The concepts of the CMM are examined to further explore this idea.

3.4 Capability Maturity Model History

The CMM was developed by the Software Engineering Institute (SEI) at the Carnegie-Mellon University and originally funded by the DoD. It provides organisations with the guidance to gain control of the processes that support their IS (Bardoloi, 2004, Tse, 2005). The SEI, in November 1986, commenced a Process Maturity Framework development program. Its aim was to assist organisations in the measured improvement of their software processes (SEI-CMM, 1993, Tse, 2005). It was initiated by the American Federal Government to evaluate the competence of their software contractors and its motivation was the disappointments experienced when utilising new software methodologies and technologies. The CMM is derived from manufacturing-oriented ideas, however, and notes that software engineering processes are dominated by design issues and are a knowledge intensive activity (SEI-CMM, 1993).

The SEI, in September 1987, released a brief narrative of the Process Maturity Framework and a Maturity Questionnaire. The Software Process Maturity Framework was advanced into the CMM for Software after four years of experience with the two instruments (SEI-CMM, 1993, Bardoloi, 2004). The initial release of the CMM, Version 1. was used and reviewed by the Software Community during 1991 and 1992. The CMM, Version 1.1 was released after a workshop held by the Software Community in April, 1992.

3.4.1 Capability Maturity Model Concepts defined

Harmon and Wolf (2005) remarks that the SEI expanded on the software process management work of Watts Humphrey, the traditions of Deming and the efforts of the Quality Control Movement. Tse (2005) maintains that the purpose of the SEI was to provide assistance during making measured improvements to software engineering capabilities and that its rationale is a form of continuous improvement process management to achieve business competitiveness. The CMM is built on two foundations (SEI-CMM, 1993):

- Knowledge gained from extensive software process assessments;
- Comprehensive feedback from industry and government sectors.

The CMM was developed to appraise *software process maturity* and applies two methods. First, a *software process assessment* method which measures the *software process performance* or the actual results achieved from following a software process. Second, a *software capability evaluation* method which measures *software process capability*. This *software process capability* describes the range of expected results from following a software process. These methods invoke the concepts of *software process maturity* and *institutionalisation*. *Software process maturity* is expressed as the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. *Institutionalisation* occurs when the organisation builds the infrastructure, corporate culture, standards and policies to support the *maturity* achieved. CMM provides organisations with the necessary guidance to develop and maintain process improvement strategies and evolve towards a culture of engineering and management excellence (SEI-CMM, 1993).

Tse (2005) describes the CMM as a normative model which describes the state of an organisation at each maturity Level. It does not prescribe the specific means to accomplish the maturity levels but provides a systematic method of CPI, management and control. It focuses on TQM aspects outside the software process scope, for example, corporate culture issues, which affect improvements and their institutionalisation (SEI-CMM, 1993).

Highsmith (2002) maintains that software development, as a defined process, is fundamental to the CMM. This belief holds that tasks can be accurately defined, measured and monitored. The process is refined until its results are repeatable to within very close tolerances. This is relevant when viewed against the BPM Agile enterprise ethos as is discussed in Chapter Four. The concept of maturity and its effects are now examined.

3.4.2 Concept of Maturity

The concept of *Maturity* is that mature organisations achieve their goals systematically whilst immature ones achieve their outcomes through spontaneous individual efforts. Improved maturity results in realised organisational process capability (Harmon, 2004, SEI-CMM, 1993, Smith and Fingar, 2004b, Rosemann and de Bruin, 2005).

A *Maturity Level* is defined by the SEI-CMM as a 'well-defined evolutionary plateau towards achieving a mature software process'. Each maturity level provides a foundation layer for CPI and marks an increase in process capability. The CMM arranges the five maturity levels as an ordinal scale which measure the software process maturity, evaluate the process capability and prioritise improvement efforts (Tse, 2005, SEI-CMM, 1993, Bardoloi, 2004). Harmon (2004) notes that the CMM literature describes maturity rigorously and uses terms such as *predictability* which is the consistency of meeting goals, *control* which refers to the consistency with which the goals are met and *effectiveness* which refers to achieving the right goals in an efficient manner. The CMM is described as providing an evolutionary path from an ad-hoc immature to a mature disciplined process (Crow, 2000, Miller, Pulgar-Vidal and Ferrin, 2002, Tse, 2005, Harmon, 2004, SEI-CMM, 1993). Harmon (2004), specifically, notes that immature organisations achieve their goals intermittently whilst mature ones achieve them

consistently. There are differences between an immature and a mature organisation which illustrate this progression.

3.4.3 Immature versus Mature Software Organisations

The setting of realistic goals for process improvement requires understanding the difference between mature and immature software organisations. An increase in maturity indicates an increase in process awareness, with each maturity level representing an increase in the conscious involvement across the organisation to manage, control and improve their processes (SEI-CMM, 1993, Tse, 2005). The following criteria, illustrated in Table 3.1, are sourced from the CMM and define these distinctions (SEI-CMM, 1993):

Immature Software Organisation	Mature Software Organisation
Software processes are improvised	Software development and maintenance is well-managed
Rigorous software process specification is minimal	Software processes are accurately communicated
The organisation is reactionary	Work activities are appropriate and consistent
Schedules and budgets are routinely exceeded	Defined processes are reviewed and updated
Product functionality and quality are compromised	Quantitative measures exist to judge and predict quality
Quantitative measures are minimal and quality is unpredictable	Realistic schedules and budgets are based on historical performance
Quality enhancing reviews and testing are curtailed	Disciplined processes are repeated using adequate infrastructure

Table 3.1 - Behavioural distinctions between an immature and mature organisation

This progression from an immature to a mature software organisation required the construction of a maturity framework to provide the foundation to support each successive improvement (Tse, 2005, SEI-CMM, 1993, Bardoloi, 2004). The five levels are (SEI-CMM, 1993):

- Maturity Level 1 (Initial);
- Maturity Level 2 (Repeatable);
- Maturity Level 3 (Defined);

- Maturity Level 4 (Managed);
- Maturity Level 5 (Optimising).

The maturity levels and their characteristics are important. The maturity levels represent an increase in the process awareness, process capability and a change in the behaviour of the organisation. Briefly, there are three types of improvement observed as maturity levels increase. First, the variance between targeted and actual results decreases. Second, the variability of the actual results decreases. Third, the targeted results improve as maturity levels increase. It is expected that an organisation, at the higher maturity levels, has processes capable of producing reliable software within predictable cost and schedule limits. SPC is exhibited (SEI-CMM, 1993).

Two main approaches emerge from a variety of maturity models. The first approach is based on levels or stages which assume that sets of related capabilities are achieved and the levels are progressed through sequentially. There are difficulties associated with the single level approach but it provides a dramatic representation of the state of an organisation and its goals are clear. The alternative approach is the *continuous representation* and its focus reflects the fact that organisations generally display a mix of capabilities. Its advocates avoid the idea of levels and focus on the capabilities that characterise the organisation (Harmon, 2004).

3.4.4 Uses of the Capability Maturity Model

There are four uses supported by the CMM. First, it is used by assessment teams to identify strengths and weaknesses in an organisation. Second, it is used by evaluation teams to identify the risks involved in selecting a business contractor and monitoring their performance. Third, it is used by management and technical staff to understand the necessary activities to plan and implement a process improvement program. Finally, it is used by process improvement groups to define and improve the software processes in an organisation (SEI-CMM, 1993).

3.4.5 Benefits of Capability Maturity Model

The CMM aids an organisation by instilling defined practices and by instilling a change in the corporate culture which helps moving up the CMM ladder. Each increase in a maturity level is accompanied by a variety of improvements including

an increase in overall performance and product quality, a shift to pro-active management with improved management decisions and an increase in customer satisfaction (Bardoloi, 2004). The CMM does not guarantee that the work done is excellent in quality or successful, but rather provides the organisation with the means to work in an orderly manner and obtain predictable results. There are behavioural characteristics aligned to each maturity level which are examined briefly (SEI-CMM, 1993).

3.4.6 Maturity Level Behaviour Features

The software process at Maturity Level 1 (Initial) is characterised as ad hoc. Few process definitions exist and success depends on individual effort. *Software Process Capability* is unpredictable. Quality and performance depends on the capabilities of individuals and is, therefore, erratic (SEI-CMM, 1993, Crow, 2000, Bardoloi, 2004). Harmon (2004) notes that immature organisations rely on goals and measures rather than the associated processes. The software process at Maturity Level 2 (Repeatable) is characterised as disciplined. Process management policies and controls are established. *Software Process Capability* is disciplined and project successes are repeatable. Software process management is institutionalised and a stable environment exists (SEI-CMM, 1993, Crow, 2000, Bardoloi, 2004). Harmon (2004) notes that a Level 2 (Repeatable) organisation has begun to climb the maturity ladder. Management view the process as an application which accomplishes a specific task. The software process at Maturity Level 3 (Defined) is characterised as formally defined and integrated. Processes are uniquely tailored. *Software Process Capability* is consistent because standardised, integrated software engineering and management processes exist in a stable environment (SEI-CMM, 1993, Crow, 2000, Bardoloi, 2004). Harmon (2004) notes that a Level 3 (Defined) organisation attempts to monitor and control specific processes using well-defined processes, metrics and goals. The software process at Maturity Level 4 (Managed) is characterised as predictable. The software process is measured, using established metrics, as part of a management program. SPC is achieved. The development process is predictable because the process operates within measurable limits. *Software Process Capability, Process Capability* and product quality are predictable (SEI-CMM, 1993, Bardoloi, 2004, Crow, 2000).

Harmon (2004) notes that a Level 4 (Managed) organisation focuses on developing an integrated process management and measurement system. Its aim is to provide the metrics necessary to align the processes, functioning within the *Value Chain*, to the strategic goals. There is an emphasis on the quality and quantity of the management system and on aligning the resources that support the processes. Maturity is assessed by inspecting how well processes are organised and the degree to which they are under control. This is revealed by inspecting the alignment between processes and their support facilities.

Harmon (2004) illustrates the difference of an organisation at Maturity Level 3 (Defined) and Level 4 (Managed) in terms of its *horizontal* and *vertical alignment*. *Horizontal alignment* involves defining all the processes and activities that comprise a *Value Chain*. *Vertical alignment* involves determining and using process measures to achieve individual goals as part of the achieving the strategic goals of the organisation at optimum efficiency. A Level 3 (Defined) organisation is *horizontally aligned* whereas a Level 4 (Managed) organisation is *vertically aligned*.

The software process at Maturity Level 5 (Optimising) is characterised as continuously improving. CPI is institutionalised. The innovative use of technologies and methods, which exploit integrated development practices, are identified and implemented. *Software Process Capability* and *process performance* continuously improve because the range of process capability is persistently improved (SEI-CMM, 1993, Bardoloi, 2004, Crow, 2000). Harmon (2004) notes, from the CMM schema perspective, that optimisation occurs once processes are well managed and measured.

Maturity Level 5 (Optimising) is characterised by measurable CPI at an organisational level. Process performance and quality are proactively improved and institutionalised. Disciplined innovation and continuous improvement become the corporate culture (SEI-CMM, 1993, Bardoloi, 2004).

There are two foci at Maturity Level 5 (Optimising). The first is Process control and the software process is managed so that it operates within a zone of quality control. This is the *institutionalisation* of Level 4 (Managed) maturity. The second focus is on CPI and the lessons learned in improving quality are used in planning

future processes. An organisation at Maturity Level 5 (Optimising) is expected to produce reliable software products within predicted cost and schedule limits (SEI-CMM, 1993).

3.4.7 The State of Organizational Process Management Maturity

Maturity Level 5 (Optimising) and its predecessor, Level 4 (Managed), are relatively rare occurrences. Inference about their attributes is drawn from other industries and the concepts of SPC and process management (SEI-CMM, 1993, Bardoloi, 2004).

Harmon and Wolf (2005) maintain that the majority of organisations operate at a Level 3 (Defined). There are few examples of organisations achieving Level 5 (Optimising) Maturity. The business initiative, Six Sigma is considered a tool to accomplish CPI (Miller et al, 2002, Harmon, 2004). It can be regarded as a Maturity Level 5 (Optimising) tool.

A 2004 Rummler-Brache Group report researched the state of process management in American companies. It concluded that, first, improvement efforts are well aligned to business strategies and are customer centric; second, process awareness and the prioritising of improvement initiatives are mediocre and, finally, process management capabilities are weak. The lack of solid performance metrics to monitor process results and steer change management was seen as a notable shortcoming (PPI Research Report, 2004). This corresponds to the standpoint of the CMM that few organisations are at Maturity Level 4 (Managed) or higher because the higher levels of maturity promote SPC which was assessed as weak during the Rummler-Brache Group study.

The focus of this research is to integrate security into the business paradigm, BPM, using a maturity model approach. It is therefore, relevant to discuss the descendant of the CMM, the Systems Security Engineering Capability Maturity Model. Its focus is security engineering.

3.5 Systems Security Engineering Capability Maturity Model

The SEI developed a CMM specifically for security and security engineering – namely the System Security Engineering Capability Maturity Model (SSE-CMM). It contains the fundamental security engineering process features needed to ensure high quality security engineering (Tse, 2005, SSE-CMM, 2003). It is a framework

for developing the security engineering process which as it matures, becomes formally defined, documented, institutionalised and CPI is used (SSE-CMM, 2003, Spears et al, 2004).

The increasing need for information security was discussed in Chapter One and its various definitions were presented in Chapter Two. It is pertinent to examine various security engineering concepts prior to discussing the SSE-CMM.

3.5.1 Security Engineering – an Overview

Security engineering is based on various well-accepted principles which include the Canadian Trusted Computer Evaluation Criteria and the Common Criteria for Information Technology Security Evaluation. It is based on security metrics and codes of practice including the NIST handbook, c:cure and the Pentana checker and the efforts of the SANS Institute who advocate security engineering (Eloff and von Solms, 2000a, Ferraiolo and Thompson, 1997, Sheard and Moini, 2003). Ferraiolo and Thompson (1997) and SSE-CMM (2003) contend that an effective framework to evaluate security engineering practices was absent and that using modern SPC produces quality products which are, therefore, more effective in developing mature secure system and trusted products.

There are a variety of characteristics inherent in engineering a secure system. These include the security concepts of confidentiality, integrity and availability which are expanded to include: repeatability which ensures that project success is repeated; efficiency which helps developers and evaluators work more proficiently and assurance which implies confidence that the security needs are satisfied (Ferraiolo and Thompson, 1997, SSE-CMM, 2003, Sheard and Moini, 2003).

Sheard and Moini (2003), in Security Engineering Awareness for Systems Engineers, describe security engineering as the systematic creation of systems which are “robust in the face of malice, error or mischance”. It is a systematic practice which concentrates on tools, technologies and processes to design, implement and test reliable systems, and to strengthen existing computer systems. It is a multidisciplinary field encompassing traditional computer security, cryptography, biometrics, business process analysis, organisational methods and the law. It is an evolving discipline that establishes a balanced set of security needs which is integrated into system activities, configurations and operation. This

establishes confidence in the effectiveness of the security measures (Ferraiolo and Thompson, 1997, SSE-CMM, 1997, SSE-CMM, 2003). The importance of security engineering has shifted and it should be considered a key component in multi-disciplinary, concurrent engineering teams. The SSE-CMM is the response to this shift.

3.5.2 SSE-CMM Development

The SSE-CMM initiative began in 1993 with an NSA-sponsored research project into existing work on CCM and the need for a specialised SSE-CMM was investigated. The First Public Security Engineering CMM Workshop was held in January, 1995 (Hefner, 1997). The SSE-CMM model and its appraisal method, the SSE-CMM Appraisal Method (SSAM) were first published in 1997 and its latest edition, Version 3.0, was published in 2003.

It was developed by members of the SSE-CMM Project representing some sixty members of American and foreign government and commercial organisations specialising in security engineering and process improvement. Its objectives include evolving security engineering into a mature and quantifiable discipline which enables focused investments (Ferraiolo and Thompson, 1997, SSE-CMM, 1997, SSE-CMM, 2003). It encompasses security engineering activities throughout the entire life-cycle, from concept definition to decommissioning and includes integration. It establishes capability-based assurance which ensures that system confidence is a function of mature security engineering practices (SSE-CMM, 2003).

It comprises two parts, a model for security engineering processes, project and organisational processes and an appraisal method to assess their maturity. It is applied in three ways; first, for process improvement by achieving higher maturity levels; secondly, for capability evaluation through establishing the capability levels of business partners and thirdly, for assurance through providing evidence of process maturity (Spears et al, 2004). It allows organisations to evaluate their security engineering practices and identify areas for improvement (Barton et al, 2000).

The practices of the SSE-CMM focus on the security needs of the customer and their assurance requirements. It focuses upon the requirements of implementing

security in IT Systems and is both methodology and process independent. Its purpose is to assess and improve the security engineering capability and promote its integration into other engineering disciplines which results in security engineering becoming pervasive across the organisation (SSE-CMM, 2003). It exhibits a conscious effort to improve, manage and control the effort to produce security awareness within the organisation by advancing through the Maturity Levels (Tse, 2005). Chan and Kwok (2001) maintain the SSE-CMM provides a generic framework for the design and development of a secured system.

The SSE-CMM defines the expectations of the processes and capabilities for each maturity level. At the higher maturity levels, the focus changes from a specific security attribute towards the role of security within the organisation. Security practices and technology are more business-appropriate as the security governance processes mature. Effectiveness reaches a degree that mirrors the desired security posture and risk profile of the organisation (Tiller, 2005). The development of the SSE-CMM has been examined and its architecture and concepts are discussed next.

3.5.3 An overview of the SSE-CMM Architecture and Concepts

The SSE-CMM was developed as a CMM-based framework to apply SPC to security engineering to advance the evolution of secure systems within anticipated cost, schedule and quality parameters.

Security engineering activities are practiced at all phases of the Systems Development Lifecycle (SDLC) by a variety of organisations including: Developers; Security Evaluation Organisations and Trusted Third Parties (SSE-CMM, 2003). The SSE-CMM establishes the security performance of an organisation according to a set of criteria or base practices which are expressed as a capability maturity level. These base practices comprise a set of recognised best practices. It specifies 129 base practices which are organised into 22 Process Areas. Each Process Area (PA) has a set of goals which are achieved through performing its base practices. These PAs are grouped into 11 security engineering, 11 project and organisational process areas and five capability maturity levels. They represent best existing practice in the security engineering community (Ferraiolo and Thompson, 1997, SSE-CMM, 2003, Chan and Kwok, 2001).

The SSE-CMM has two dimensions, Domain and Capability. The Domain dimension contains the security engineering base practices. A base practice is achieved when it is performed at a single level of abstraction. The Capability dimension represents the practices which indicate process management and institutionalisation capability. These are called generic practices because they are applicable across a wide array of domains and represent activities that must be performed as part of a base practice. They address process management, measurement and institutionalisation issues. They are used to assess, during an appraisal, the process capability of an organisation. They are assembled into logical areas called common features (Ferraiolo and Thompson, 1997, SSE-CMM, 2003).

Security Engineering Process Areas	
PA No.	**Process Area Topic**
PA 01	Administer Security Control
PA 02	Assess Impact
PA 03	Assess Security Risk
PA 04	Assess Threat
PA 05	Assess Vulnerability
PA 06	Build Assurance Argument
PA 07	Coordinate Security
PA 08	Monitor Security Posture
PA 09	Provide Security Input
PA 10	Specify Security Needs
PA 11	Verify and Validate Security.
Project and Organisational Process Areas	
PA No.	**Process Area Topic**
PA 12	Ensure Quality
PA 13	Manage Configuration
PA 14	Manage Project Risk
PA 15	Monitor and Control Technical Effort
PA 16	Plan Technical Effort
PA 17	Define organisation's Systems Engineering
PA 18	Improve organisation's Systems Engineering
PA 19	Manage Product line Evolution
PA 20	Manage Systems Engineering Support Environment
PA 21	Provide Ongoing Skills and knowledge
PA 22	Coordinate with Suppliers

Table 3.2 - SSE-CMM - Process Areas

The 22 security engineering and project and organisational process areas are illustrated in Table 3.2 and are numbered in no particular order because the SSE-CMM does not specify a specific process or sequence. The process areas of the security engineering domain are specifically organised to meet a broad spectrum of security engineering needs.

Common features describe major shifts in the organisational work performance. Each comprises one or more generic practices. They are ordered into the following levels which represent an increase in capability (Tiller, 2005, Tse, 2005, SSE-CMM, 2003):

- Capability Level 1 (Performed informally);
- Capability Level 2 (Planned and tracked);
- Capability Level 3 (Well defined);
- Capability Level 4 (Quantitatively controlled);
- Capability Level 5 (Continuously improving).

The common features and capability levels are important in performing an SSAM and improving organisational process capability. A capability level is achieved when its practices are established and used effectively (Tse, 2005).

3.5.4 SSE-CMM Capability Levels

The SSE-CMM defines five levels of process capability which correlate to the CMM-based maturity levels. The common features and capability levels perform an important role in process capability assessment and in planning improvement efforts (Siponen, 2002a). An SSAM determines the capability level of each PA which often exists at differing levels of maturity (Siponen, 2002a, Tse, 2005). The five capability levels represent an increasing level of security engineering awareness and maturity (Tiller, 2005, Tse, 2005, Ferraiolo and Thompson, 1997, Siponen, 2002a, Williams and Ferraiolo, 1999, Kormos, Givens, Gallagher and Bartol, 1999, SSE-CMM, 2003). It is pertinent to examine the capability levels with reference to their organisational and security engineering goals.

The Capability Level 1 (Performed informally) focuses on whether the organisation performs the processes which incorporate the base practices. It is represented by

the existence of security policies, management practices and security standards. The Capability Level 2 (Planned and tracked) focuses on the definition of planning and performance issues. Oversight practices are installed which focus on the performance of people, processes and technology. Quality control is performed which establish operational and maintenance metrics. The Capability Level 3 (Well defined) focuses on disciplined process tailoring. It represents an overarching security management and governance process. Evidence is produced, in quality documentation and other deliverables, that the defined processes are correctly performed and co-ordinated. The Capability Level 4 (Quantitatively Controlled) focuses on measurements which are tied to business goals. Project measures are instituted early but are not widely used until the higher capability levels are achieved. Performance is objectively managed through applying these measurements to the meeting of organisational goals. The Capability Level 5 (Continuously Improving) focuses on gaining leverage from the management practice improvements previously instituted and emphasises a cultural shift that sustains these improvements. It represents a state where security is supportive of business objectives. There is clearly articulated Return on Security Investments (ROSI) (SSE-CMM, 2003).

Security engineering maturity is achieved through the effective establishment of the management practices contained in the common features, generic practices, capability levels and their continuous improvement. Organisations are advised to adopt a pragmatic approach to the SSE-CMM and accept a particular maturity level that meets their desired business and security needs (Tiller, 2005). Security engineering, as viewed from SSE-CMM, comprises three areas or processes which are now discussed.

3.5.5 Security Engineering – SSE-CMM Viewpoint

Security engineering is divided into three major areas or processes, namely risk, engineering and assurance (SSE-CMM, 2003, Chan and Kwok, 2001). Figure 3.3 illustrates their relationship. The risk process identifies and prioritises systems threats. The engineering process works in concert with other engineering disciplines to implement appropriate solutions. The assurance process establishes confidence in the solutions and communicates it to the customers (Chan and Kwok, 2001). The three security engineering processes – risk, engineering and

assurance are examined from the perspectives of the SSE-CMM (2003), the protection profile improvement process of Williams and Ferraiolo (1999) and the integration of security design research of Chan and Kwok (2001). The three processes are inter-related and act co-dependently to produce a security solution and it is pertinent to examine them in more detail to understand their interrelationship during security development.

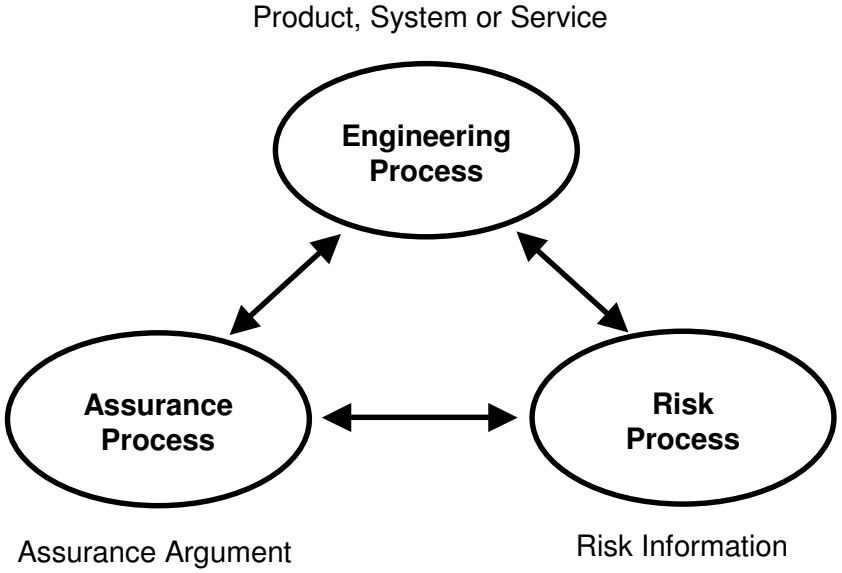


Figure 3.3 - Three major areas in security engineering
Source Chan and Kwok – 2001

3.5.5.1 Security Engineering – Risk Process

Risk, according to SSE-CMM (1997), is defined as "the likelihood that the impact of an unwanted incident will be realised." A major security engineering objective is the reduction of risk. Risk assessment was previously defined as the systematic consideration of the business harm likely to arise from a security failure. It involves the identification of business assets, their possible threats and vulnerabilities and the prioritisation of risk-mitigating techniques/resources (Margaritis et al, 2001, Carlson, 2001, ISO 17799-2:2002, SSE-CMM, 2003). Chan and Kwok (2001) note that the risk process identifies and prioritises dangers inherent to the developed service or product.

Williams and Ferraiolo (1999), in P³I - Protection Profile Process Improvement, examine the use of the SSE-CMM to develop a quality Protection Profile (PP) based on the functional and assurance requirements contained in the Common Criteria standard. Chaula, Yngström and Kowalski (2004), in Security Metrics and Evaluation of Information Systems Security, acknowledge the use of the processes in security evaluation, risk assessment, protection profiling and in assurance rating and use the PP to create the security specifications. The development of a quality PP is complex and involves all aspects of security engineering. Its quality is dependent on its creating processes and therefore, a mature process helps ensure the development of high quality PPs. The SSE-CMM is advocated as a means to ensure the security engineering processes are mature.

Williams and Ferraiolo (1999) note that PA04 (Assess threat); PA05 (Assess vulnerability); PA02 (Assess impact) and finally, PA03 (Assess security risk) relate to understanding risk. The selection of the most appropriate risk assessment method depends on various factors including the technology used, amount of information available and the expertise of the developers. A critical factor is the determination of the appropriate metrics for the risk components, otherwise, it is impossible to determine the severity of the risks. Chan and Kwok (2001) note that the risk process, in the SSE-CMM arena, requires the assessment of four important entities: impact; security risk; threats and vulnerabilities. The PA activities involved in gathering information about threats, vulnerabilities and impact are interdependent. Their goal is to discover which combinations are deemed sufficiently risky to justify action. An overall risk analysis is performed to determine what combination of threats, vulnerabilities and impact will present a significant risk. The risks are prioritised to discover which requirements are critical over those that 'are merely nice to have.' The SSE-CMM is seen as an aid and prevents the creation of solutions which are too costly, too difficult for users or which are insufficient (Williams and Ferraiolo, 1999).

3.5.5.2 Security Engineering – Engineering Process

The engineering process includes PA01 (Administer security control), PA07 (Coordinate security), PA08 (Monitor security posture), PA09 (Provide security

input) and PA10 (Specify security needs) (Chan and Kwok, 2001, SSE-CMM, 2003). Williams and Ferraiolo (1999) differentiate the groupings of the PAs and cluster PA10 (Specify security needs); PA07 (Coordinate security) and PA08 (Monitor security posture) together to develop an understanding of the security needs of the consumer through the security policies and the security usage assumptions.

The practices in PA10 (Specify security needs) include identifying the policies, laws, standards and other external influences and constraints that affect the security environment. These enable the identification of high-level security goals in a security policy. PA07 (Coordinate security) ensures the solution is valid across the solution and consumer environment whilst PA08 (Monitor security posture) contains the practices needed to ensure the underlying security needs do not change unnoticed during the development and vetting processes. This underlying security information demonstrates that the security solution fits its intended context which creates consumer confidence in its appropriateness (Williams and Ferraiolo, 1999). The risk and engineering (security engineering) processes are interlinked to the assurance process because the evidence which promotes assurance, demonstrates rationale behind the security solution.

3.5.5.3 Security Engineering – Assurance Process

Assurance is defined ‘as the degree of confidence that security needs are satisfied’. It is a product of security engineering and indirectly it reduces risk. SSE-CMM contributes to this confidence through the repeatability of quality results. It does not impose any additional security controls and provides the confidence that, once deployed, the security controls will function as intended. Assurance is often communicated in the form of an argument and reveals that its development has followed a mature engineering process subject to CPI. SSE-CMM activities provide assurance relevant evidence (SSE-CMM, 2003).

Activities in the assurance process use the products of the risk and engineering processes which establishes confidence in the security solutions and conveys this confidence to the users (Chan and Kwok, 2001). Williams and Ferraiolo (1999) maintain that choosing assurance requirements is a complex task and involves PA10 (Specify security needs), PA06 (Build assurance argument), PA09 (Provide

security input) and PA07 (Coordinate security). PA10 (Specify security needs), provides the practices necessary to select a set of assurance requirements.

PA06 (Build assurance argument) contains the practices which identify and manage the appropriate assurance evidence into arguments that the solution is achieved. This approach ensures that security claims are not overlooked and are supported by sufficient evidence. PA09 (Provide security input) guides the process of selecting and modifying the assurance requirements. A traditional problem is the tendency to develop the assurance evidence after the security system is developed. The SSE-CMM encourages developing the assurance requirements at the earliest possible stage and PA07(Coordinate security) contains these necessary practices. The early development of the assurance requirements will reduce the costs and increase the quality of the assurance efforts (Williams and Ferraiolo, 1999, SSE-CMM, 2003).

There are activities within the SSE-CMM model that facilitate establishing the trustworthiness of the security system. The practices in PA11 (Verify and validate security) and PA06 (Build assurance argument) help establish its consistency and completeness. PA11 (Validate and verify security) contains the practices which verify that the security solution meets its requirements and is valid for its intended environment. Its results are important inputs to PA06 (Build assurance argument) and are part of the assurance argument which increases the confidence in the security solution (Williams and Ferraiolo, 1999, SSE-CMM, 2003).

The SSE-CMM model can be applied to security engineering in three ways. First, it presents the SSAM which determines the capability levels of security engineering within an organisation. Second, it presents a methodology for security engineering process improvement and third, it presents a method to determine and improve assurance. The appraisal method is adapted in a variety of security assessment models to determine the state of security engineering within various environments and is examined next.

3.5.6 System Security Engineering-Capability Maturity Model Appraisal

The SSAM provides an appraisal method to establish security engineering process capability and process maturity levels (Kormos et al, 1999). These determine the

organisational capability levels for security engineering and the existence of appropriate project and organisational infrastructure (Siponen, 2002a).

The SSAM uses multiple data gathering methods to create process baselines and the momentum for improvement activities. Each PA conducts feedback sessions together with capability level progress reports and a set of prioritised strengths and weaknesses supporting process improvements are presented (SSE-CMM, 2003). Its appraisals are, according to Kormos et al (1999), usually aimed at third parties but do contain guidance for self-assessment. Appraisals are conducted to, firstly, facilitate organisational self-improvement by understanding the domain-related issues; to understand the deployment of new practices and determine the overall capability of the organisation and secondly, to benchmark, improve and institutionalise the processes. SSAM provides an important tool to gain insight into the current processes and provide guidance for process improvements. The SSE-CMM further provides a tool to improve the security engineering process of an organisation. This is the Initiating, Diagnosing, Establishing, Acting and Learning (IDEAL) approach which was developed by the SEI. It is briefly discussed in the next section.

3.5.7 System Security Engineering-Capability Maturity Model Supporting Process Improvement

The goals of security engineering improvement efforts include providing an overview of the current process capability and improved process design and capability. SSE-CMM developed the IDEAL approach which enables an organisation to maintain a continuous cycle of evaluating the current process maturity status and making improvements. Its main steps include an Initiating phase during which the groundwork for the improvement effort is established; a Diagnosing phase during which the current against the desired maturity status is determined; an Establishing phase during which the actions to achieve the desired status are planned and prioritised; an Acting phase during which the tasks are carried out and which needs the greatest amount of resources to create and refine the solutions and finally, a Learning phase which uses the improvement experience to improve future projects. Each phase is the input for the next phase. The IDEAL approach is analogous to the PDCA cycle.

The SSE-CMM promotes process improvement by moving the organisation through its capability levels, continually improving predictability, control and process efficiency. Process improvement efforts are expected to produce various benefits which cause an increase in capability maturity. Predictability is improved as an organisation matures. There is a decrease in the difference between targeted and actual results and at the higher capability level, the cost and schedule aspects are predicted with greater accuracy. There is increased control and at the higher capability levels performance is controlled to within an acceptable range. There is improved process effectiveness because targeted results improve as maturity increases, costs and development time decrease and there is an increase in productivity and quality (SSE-CMM, 2003).

The effect the SSE-CMM imposes on the assurance needs of a security system and its customers are examined.

3.5.8 System Security Engineering-Capability Maturity Model to Gain Assurance

The SSE-CMM is designed to both measure and improve the security engineering capability which translates into increased assurance in the resultant security system. This is achieved, firstly, through transforming the security needs of the customer into successful security engineering processes. It, secondly, provides an alternate assurance viewpoint to customers who do not require formal certification or accreditation. Thirdly, it presents a standard which provides the confidence that their security needs are adequately addressed.

An SSE-CMM rating implies that certain processes were followed throughout the SDLC and process evidence is available to support the trustworthiness of these claims. This process evidence is important and a comprehensive assurance argument must be established to confirm the trustworthiness of the security process. Assurance needs are treated like other security requirements which ensures they are integral to the security engineering process.

The SSE-CMM supports a variety of improvement activities including self-administered or internal appraisal which determines capability levels and identifies weaknesses and improvement areas. It is used to augment process-based assurance methods because it reduces evaluation and accreditation time due to

the confidence that is produced through advancing through the capability levels (Hefner, 1997). The role of metrics in the SSE-CMM is subsequently investigated.

3.5.9 The role of metrics in the System Security Engineering-Capability Maturity Model

The SSAM is used to appraise the security engineering process capability and process maturity of an organisation and together with SSE-CMM provide a means to measure and improve security engineering (SSE-CMM, 2003). A security metrics system, at a high level of abstraction, provides the quantifiable measurement of organisational aspects together with a quantitative approach to measure system compliance. It can be built from lower-level physical measures and through using quantifiable metrics, such as ratios, percentages and averages, to provide insight into the security posture (Kahraman, 2005). The SSE-CMM Project Metrics Action Committee presents process metrics which specify the level of maturity for a specific PA and security metrics which measure the effectiveness of the security engineering process. Process metrics are gathered from measuring the process itself whilst security metrics originate from measuring the security attributes of the process results (Kormos et al, 1999). There are various programs and approaches to generating metrics which is, however, a difficult task because it is a new discipline without a common vocabulary and few documented practices. The use of a process improvement framework is recommended and Six Sigma is cited as an example (Payne, 2006).

Security metrics facilitate an improved understanding and performance of the security system (Chaula et al, 2004). Security metrics, used continuously over time, evaluate security performance; monitor controls; track improvement and efficiency. Their benefits include demonstrating an improved accountability to stakeholders and compliance with regulatory and legal requirements. They ensure an appropriate level of support for business goals and risk management becomes pro-active through understanding the organisational security position (Kahraman, 2005).

It is necessary to critically view the SSE-CMM framework and CMM-based approaches to establish a balanced viewpoint of their benefits and limitations.

3.6 Critique of System Security Engineering Capability Maturity Model

There are various criticisms aimed at the SSE-CMM and it is necessary to review a selection to establish a balanced viewpoint. This critique again uses the research of Mikko T Siponen and the motivation for basing this criticism on his work was previously discussed in Chapter Two, Section 2.6.

Siponen (2002a) in, Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned From Software Maturity Criteria, examines a variety of security management oriented standards including the SSE-CMM. It was stated in Chapter Two, Section 2.6, that information security management standards are viewed as the product of checklist-based approaches to security. They offer convenient and generic protection measures based on the experience of practitioners. Maturity standards are the latest successor of the information checklists-management standards. The SSE-CMM presents both the maturity criteria as a ready package and practical directions for evaluating the maturity.

There are a variety of criticisms aimed towards maturity models and while some are outside the scope of this research, the most relevant are briefly discussed. The first criticism considered is operational focus which queries whether the maturity criteria support conventionalism, which insists on the use of existing operational practices, or support innovation. Organisations that develop cutting-edge security solutions rank weakly in maturity estimations because the new solutions are not recognised by the maturity criteria. Innovation is regarded as the major hurdle to adopting maturity approaches. SSE-CMM is regarded as anti-innovation and conventionalism is upheld through stressing the use of existing practices. Some development freedom is provided because it allows for tailoring to suit unique organisational needs (Siponen, 2002a).

Another criticism queries the support by maturity standards for development in emergent environments. These maturity standards imply that stable environments exist. This is a flawed notion because IS development is creative. Organisations are increasingly turbulent or emergent in their business environment and require appropriate IS development methods. The emergent environment needs the rapid development of security solutions which cannot wait for bureaucratic, long-term

security processes. SSE-CMM assumes a highly stable IS development environment and its evaluation process is formal.

It is the opinion of this author that maturity models do address innovation through Capability Level 5 (Continuously improving) and Maturity Level 5 (Optimising) which emphasise CPI which is innovative in its nature. SSE-CMM (2003) notes that CPI is enabled by quantitative feedback and from 'piloting innovative ideas and technologies.' Processes undergo continuous refinement and improvement based on a quantitative understanding of the impact of any process changes. The Generic Practices deal with establishing process effectiveness goals and continuously improving the standard process. The Common Features include performing causal analysis of and the prevention of defects, which is seen as a pro-active and re-active activity, and continuously improving the defined process through either incremental or innovative improvements (SSE-CMM, 2003).

3.7 Conclusion

Chapter Three discussed the CMM and its security version, the SSE-CMM. SPC and process management were examined to discover how they relate to the principles of statistical quality control in a maturity framework. The concepts of maturity and the behavioural effects of the increasing maturity levels were examined. Security engineering and the SSE-CMM were examined in detail. Its capability levels were discussed with particular reference to their effect on the security engineering processes of risk, engineering and assurance. The SSAM evaluation method was presented. The purpose of this research is to both integrate and achieve a level of mature security within the business process in a BPM environment. The SSE-CMM is a CMM specifically developed for security engineering and it plays a role in managing and evaluating a security position. It will be used in this research to evaluate, monitor and improve the security position of the business process.

4 - CHAPTER FOUR – BUSINESS PROCESS MANAGEMENT

Chapter Three discussed the second pillar of the BPSM model, the CMM and its security version, the SSE-CMM, which is envisaged as acting as the security metric to establish and evaluate the security position of the business process within the BPM environment.

Chapter Four introduces the third pillar of this research, the Business Process Management paradigm and its supporting IS, the Business Process Management System (BPMS). The business process, as the focus of the proposed security integration strategy in the BPSM model, is examined. The history, motivators and major trends of BPM are described. A generic BPM model is presented and the BPM standards are examined. The relationship between BPM and the so-called agile enterprise is discussed. A sample of agile software development methods are examined with particular focus on feature driven development. This chapter, therefore, analyses the business process environment in which the integrated security solution proposed by the BPSM model will exist.

4.1 Business Process Management

The methodology of BPM is introduced in stages in this work. It has assorted definitions amongst its various stakeholders which, together with its constituent concepts, are identified and examined. It is necessary to first define the concept of a business process, its implementation and relevance in an organisational context. The business process, by its existence, is the embodiment of BPM. Similarly to BPM, the business process has a broad range of interpretations which will be scrutinised in an attempt to ascertain some coherence. First, the history of the business process is discussed.

4.1.1 History of the Business Process

Frederick W. Taylor authored The Principles of Scientific Management in 1911 advocating a ‘science’ for every task (Thompson, 2003). Its central theory, Taylorism, maintains that all manufacturing activities are separate from those of development. Taylor postulated the three following principles (Pruijt, 2002):

1. The separation of the labour process from the skills of the employee;
2. The centralisation of planning;

3. The managerial prescription of worker tasks and output.

Taylorism was originally intended for the factory floor but extended to management systems. The following phrases describe its affects on organisations (Thompson, 2003):

- A product / outcome focus;
- Rigid work practices under a hierarchical leadership;
- Work tasks and offices became compartmentalised.

The principles and effects of Taylorism had a profound influence on the installation of IT infrastructures. Its strategic goal at management level is internal efficiency, holding that work products and circumstances are stable and predictable (Moreton and Chester, 1996). The result is a loss of innovative capacity and flexibility and the reaction to defects is the creation of more process rules (Pruijt, 2002). It was recently opined by Kinsey (2007) that Taylorism and its scientific management principles of task division and time and motion studies to determine the most efficient means of performance exist today only in the precision tools used by management consultants.

Taylorism-inspired management led to the development of IT infrastructures as substitutes for repetitive clerical work. Office work, consequently, was arranged utilising the computer as Transaction Processing Systems. A large-scale study undertaken on IT in the European service sector in 1990 concluded that the banking industry rarely exploited the possibilities of broader access to pooled information and knowledge, using Taylorism as the justification for designing computer-based systems as Operational Systems (Pruijt, 2002). This is inappropriate in the current milieu where organisations are required to be proactive.

A variety of definitions of the business process are examined and discussed next.

4.2 Business Process Defined

Recent business trends, from the Nineties, have motivated various strategic goals related to external market factors. One priority is customer satisfaction. The organisation of any business is determined by this objective and it drives them to arrange their activities into unique, cost-effective relationships. These are often

centred on business process flow and the *Value Chain* instead of the functional specialism advocated by Taylorism (Moreton and Chester, 1996). Business processes, as a concept, were first defined in the Twenties by Frederick W. Taylor in terms of "*methods and procedures*". This definition has been extended, though without any clear and agreed precision. This research considers a representative sample of these definitions.

4.2.1 Business Processes – Paul, Hlupic and Giaglis Viewpoint

Paul, Hlupic and Giaglis (1998) in their paper, Simulation Modelling of Business Processes, variously quote the definitions of a business process as:

- "*a set of activities that, taken together, produces a result of value to a customer.";*
- "*a set of logically related tasks performed to achieve a defined business outcome.*";
- "*Business processes are simply a set of activities that transform a set of inputs into a set of outputs (goods or services) for another person or process using people or tools*".

It is apparent from this panoply of descriptions that there does not exist an unambiguous definition, however, there are shared identifiable attributes:

- A set or cycle of activities comprising logically related and inter-related tasks;
- The transformation of inputs into outputs which achieve defined business objectives through the employment of various resources.

These common features garnered from this multitude of definitions are examined in juxtaposition with the viewpoints of other authors about the business process concept.

4.2.2 Business Processes – Business Process Management Initiative Viewpoint

Howard Smith is the co-chair of the Business Process Management Initiative (BPMI). Peter Fingar is an executive partner with the Greystone group. Together they have authored many seminal works on the BPM paradigm which form a significant source of research information in this field. BPMI, founded in 1999, is

instrumental in the development of BPM standards and the advancement of this emergent methodology (McGovern, 2004).

Smith and Fingar (2002) state that the foundation of BPM is the recognition of the business process as an "*information type*" comprising data, procedures, workflow and distributed communication which are expressible mathematically. Its acknowledgement as a fundamental building block is significant. Each element – the inputs, outputs, participants, activities and calculations – can be articulated in a format where every attribute is understandable in the context of its use, purpose and decision-making role. Processes are defined as *"the complete and dynamically coordinated set of collaborative and transactional activities that deliver value to customers"* and are seen as "*Difficult to make visible*" because they are often neither determined nor explicit. They are viewed as "*Large and complex*" and *"Dynamic"* involving Value Chain resources and are responsive to market demands. They are characterised as *"Widely distributed and customised"* and *"Long-running"* involving a process instance that executes over a long period and spans multiple applications on disparate technology platforms. Processes are seen as collections of individual tasks. It is their synchronisation and coordination that establishes them as business processes (Smith and Fingar, 2002).

4.2.3 Critique of Business Process Definitions

There is broad debate over the definition of the business process. It can be construed from the variety of process definitions that whilst some consensus exists, there is as yet no formal agreement. A business process can be expressed as a series of predefined actions needed to achieve a set goal. It can be as trivial as a unique action, for instance, an email, or alternatively be a well-defined sequence of formal events achieving a business objective such as Order-Processing. This is a simple and inclusive definition (Pyke and Whitehead, 2003). It can be viewed, in a more complex manner, as an interdependent set of business activities and decisions that mediate their inter-relationships (McGovern, 2004).

Business processes are seen as organisational activities that achieve a business goal. The common attributes, identified by Paul et al (1998), are well-aligned with the definition and characteristics postulated by the BPMI. It contends that business processes deliver value and adds the refinement of collaboration to its definition (Fingar and Smith, 2002).

Business processes develop in size, complexity and instability over time and are generally not engineered from their outset. BPM is a vital tool, emerging to manage and improve these evolving business processes (Pyke and Whitehead, 2003). It views each business process as uniquely identifiable with a minimum of one objective whose degree of success is either measured qualitatively or quantitatively (McGovern, 2004).

4.3 Business Process Management History

The phrase BPM is not new and evolved from the related fields of business process improvement, BPR and business process innovation. BPM efforts exist under a variety of names, including Six Sigma, Business Process Intelligence (BPI), BPR, Integrated Definition Function Modelling (IDEF0) and Lean Thinking (Smith and Fingar, 2003a). Its supporting technologies have evolved from Workflow Management (WfM), ERP, EAI, process automation and integration, process modelling and process optimisation (McGovern, 2004). The history of BPM and its predecessors require examination to understand its place within the current IT milieu.

A BPM system requires study from a historical perspective. Generic and specific applications such as database management systems and decision support software were absent during the Sixties ensuring that IS were mainly bespoke, built on top of an operating system and possessing limited functionality. The Seventies and Eighties were dominated by data-driven approaches with IT focused on information storage and retrieval. Data modelling became the starting point for IS. The business process was neglected and expected to adapt. Recent management trends towards BPI illustrate the emphasis on processes and system engineers are adopting process-driven approaches. A final BPM driver, is the shift in IS development from carefully-planned designs towards redesign and organic growth. The omnipresence of the Internet and its standards have resulted in software development becoming dynamic (van der Aalst, ter Hoftstede and Weske, 2003). Concurrently, an equally dynamic business environment developed which required that IT implementations keep pace with its turbulent nature. The so-called agile enterprise is the result of these dynamic business conditions.

4.3.1 The Agile Enterprise

BPM evolved in response to a changing business environment. The current dynamic business environment has created organisations which continually adapt their structures, strategies and policies to suit this environment (Nerur et al, 2005). Organisations, and their associated IS, which are constantly changing are called emergent organisations or alternatively, Agile Enterprises. Every organisational feature is in continual motion and follows no pre-defined pattern (Baskerville and Siponen, 2002). This description is applicable to many organisations in the current business environment which are under pressure to remain competitive within an ever-changing and demanding marketplace and they need to respond effectively and proactively (Moreton and Chester, 1996). Emergent organisations need their IS to evolve to meet these changing requirements. This need led the progression of IT systems to the current development, BPM.

4.3.2 Application Integration Drivers

The current, uncertain and changing business environment has necessitated organisations to develop an effective response. The following require enterprises, in all industrial sectors, to respond competitively (Moreton and Chester, 1996):

- Market liberalisation including the expansion of globalisation;
- Shortened product life-cycles with the mass customisation of products or services;
- Improved methods of business management.

The growth of successful enterprises is reliant on their ability to rapidly deploy integrated applications and interactive data which enables them to be competitive. An effective organisation needs to standardise the management of its business processes across a multitude of applications and stakeholders to help achieve this (Sinur and Thompson, 2003).

The trend towards an IT process-oriented approach began in the mid-Eighties. Previous IT development had been driven by the data, functional and application approaches. Recent developments in hardware and software enabled a transformation in IT installations. The roots of BPM lie in a variety of process and

enterprise integration modalities and workflow management. Many of these developments occurred concurrently whilst others were successive.

4.3.3 Enterprise Resource Planning

The definition of ERP or Packaged Applications, according to the Workflow Management Coalition (WfMC) Glossary, refers generically to any pre-packaged software suites used to integrate the main software applications of an organisation. An ERP installation, through multiple packaged applications, ensures the major business processes of finance, accounting, human resources and manufacturing communicate seamlessly and share a common database. It assumes its inputs and outputs and the installing enterprise is required to re-engineer their processes to fit the applications The main vendors in ERP and Customer Relationship Management (CRM) are SAP, Baan, Oracle and PeopleSoft (Workflow Management Coalition Glossary, 2005).

These ERP applications, according to Smith and Fingar (2002), initially provided greater visibility into the business process allowing enterprises to develop cross-functional installations. They provided considerable internal savings and advantages in speed and management (Clarity Integration, 2001). The demand, however, that an enterprise adapt its structure emerged as inappropriate because current market drivers require a more proactive approach.

The philosophy of TQM, based on the work of Dr William. E. Deming, is based on BPI (McGovern, 2004). The focus of ERP concentrates on improving process efficiency through implementing best-of-practice solutions and a degree of quality is sacrificed. This prevents the delivery of high-quality business processes in a competitive environment.

4.3.4 Enterprise Application Integration

Enterprise Application Integration (EAI) is another branch on the BPM tree. Currently it and its successor, Business-to-Business Integration (B_2Bi) or E-business, are the most popular field in IT installation. The WfMC (2005) Glossary defines EAI as the linking of existing software applications, jointly and across enterprise borders, enabling them to exchange data. It comprises various approaches from tailored code to middleware. This definition is extended to

include the integration of applications within a business, being Application to Application (A2A), which coupled with a sequence engine is characterised as EAI.

The achievement of process collaboration across a Networked Value Chain, in B_2Bi, is problematic because of the varying business process schemas amongst the business partners. There are large technological overheads incurred in project upgrades. The installation of EAI and B_2Bi exploit a bottom-up, technical integration approach which amalgamates diverse, often incompatible, application components. This generates integration challenges for which current tools and techniques are inadequate, resulting in projects which fail to deliver the expected benefits (Smith and Fingar, 2002).

4.3.5 Business Process Engineering

The term, Business Process Engineering / Re-engineering (BPR), was coined by Hammer and Davenport in the early Nineties. It is defined as radical change with complete restructuring of enterprise-wide business processes, using IT infrastructure, to achieve improved business performance. It is an invasive, time-consuming and disruptive process and achieved some success possibly through the existing inefficiency of the processes under replacement (Smith and Fingar, 2004a, McGovern, 2004).

The focus of BPR is aimed to re-engineer the organisation through shifting management focus from specialised departmental functions to cross-departmental activities delivering value to clients, using end-to-end business processes. Its premise stems from a reductionist viewpoint of business process coordination. They are viewed as linear, serial in nature and a function of the “Input-Process-Output” modality (Smith and Fingar, 2004a). They required thorough analysis and redesign followed by transition to the new process state. The dynamic nature of the business processes created inherent difficulties in the analysis and redesign phases, and in the transition planning (McGovern, 2004). BPR exposed the framework of the required business process transformation but failed to provide a workable solution applicable to the multitude of problems that arose simultaneously (Smith and Fingar, 2002).

The term BPR was extended to include the definitions of Business Process Design and Business Process Redesign by the WfMC. It includes improving existing

processes or creating new processes. These are either major or small undertakings and once executed should be followed by CPI efforts (Workflow Management Coalition Glossary, 2005). Another concurrent step in IT evolution is the emergence of Workflow Management Systems (WfMS).

4.3.6 Workflow Management Systems

The evolution of Workflow technology encompasses a variety of product areas including the following: Image processing; Document Management; Electronic Mail and Directories; Groupware and Transaction-based applications; Project Support software, and BPR and Structured System Design tools. These provide interactivity and support to business procedures and between the stakeholders (Workflow Management Coalition, 2005, Plesums, 2002).

The WfMC defines Workflow as "*the computerised facilitation or automation of a business process, in whole or part*". Workflow is concerned with the automation of procedures where the elements are passed between the participants according to a defined set of rules. A business process, from the WfMC viewpoint, is defined as "*the computerised representation of a process that includes the manual definition and workflow definition"*. This is expanded to include its discrete activity steps, association with IT and human resources and the rules which govern these steps.

The WorkFlow Reference Model comprises a broad view of workflow management and accommodates a variety of implementation and operational techniques. The following common characteristics provide the basis for developing integration and interoperability capability (Workflow Management Coalition, 1998, Hollingsworth, 2004):

1. Build-Time functions which enable workflow process definition and modelling;
2. Run-Time control functions which manage and sequence the workflow process in an operational environment;
3. Run-Time interactions which control the activities with human users and IT interfaces in processing the various activity steps.

These characteristics provide a common vocabulary of workflow processes and their supporting technologies together with functional descriptions of the software

elements and their interactions and, finally, functional and abstract definitions of the information interfaces. Workflow processes are traditionally defined in office terms. Workflow technology includes both Horizontal and Vertical Workflow routing to ensure all work tasks are completed. A WfMS ensures that workflows are neither lost nor stalled and their procedures are formally executed, in parallel, optimally using the resources (Plesums, 2002).

A WfMS is defined as "*a system that completely defines, manages and executes 'workflows' through the execution of software whose order of execution is driven by a computer representation of the workflow logic".* It delivers procedural automation to the business processes by managing the sequence of work activities and the provision of their appropriate human and IT resources. Its generic model contains three components (Workflow Management Coalition, 1998):

1. Software components which support the various workflow system functions;
2. System definitions and control data;
3. Application and application databases.

These provide the necessary process definitions and other information which are enacted by the Workflow Engine. A WfMS presupposes the organisation to be static and its workflows traceable and monitored. It produces various advantages including increased control and monitoring reports which once analysed expose improvement opportunities such as; improved service; security and privacy; and organisational options, for example, decentralisation. These advance process performance (Plesums, 2002). These opportunities to improve business process performance and the related benefits of such efforts, led to a greater concentration on the management and development of BPI as a system in its own right.

4.4 Business Process Management Development

There appears to be certain dissension in the origins and history of BPM. Its definition, architecture, official standards, components and its application model are still under informal debate by the IT industry (Dubray, 2001, Smith and Fingar, 2004a, Ghalimi and McGovern, 2004, McGovern, 2004, Pyke and Whitehead,

2003). The BPM moniker can be said to describe anything from legacy workflow products, ERP, EAI, BPR to WfMS.

The first group to address BPM directly was the BPMI. Its mission was to "*promote and develop the use of business process management (BPM) through the establishment of standards for process design, deployment, execution, maintenance, and optimisation"* (McGovern, 2004). Business and IT stakeholders, with interest in methodologies for automating, redesigning and managing business processes to improve their efficiency, attended the first BPM summit. Its objective was to understand organisational perceptions about processes and process management, developed from prior experience with BPR and other process management strategies (Harmon and Wolf, 2005). Business goals were separated into three categories (Smith and Fingar, 2002, McGovern, 2004):

- Efficiency, the need to continually reduce operating and capital costs;
- Business agility, the need to reduce the delivery cycle and market reaction gap;
- Customer Demands, focusing on customer retention and satisfaction.

BPM was seen as a consequence of and a solution to the changing business climate, as reflected in the stated business goals.

The BPMI viewpoint of BPM considers it primarily as a strategic management philosophy. It involves recognising that business processes and their management are the key performance drivers for the organisation and its stakeholders. It means achieving a balance between efficiency, effective service and organisational agility. It is a core managerial discipline that implies thinking at the business process design and related performance objectives level (Miers, 2005).

BPM is characterised by changes which occur throughout the project lifecycle within new or existing processes and this change is periodic, continuous or evolutionary. A BPM implementation is long-term, incremental and involves many processes and its scope is enterprise-wide (Smith and Fingar, 2004b). A BPM delivers a controlled evolution using a *'spiral implementation methodology'* of optimising, enhancing and adapting existing processes. It incorporates monitoring and analysis features allowing the optimisation of enterprise-wide processes (Miers, 2005).

The Delphi Group White Paper 2003 Report (Delphi Group, 2003) explicates their perspective on BPM. Their view of BPM is eloquently stated as a resource to channel existing automation into orchestrated business processes, with its motivators being continually changing business environments, integration challenges, regulatory pressures and systems complexity following merger and acquisition activity.

It is appropriate to investigate BPM at a more detailed level, following the understanding that has been gained of its history, motivators and meaning.

4.4.1 Business Process Management – An Overview

Business Process Management is both a theory and an associated group of methods for the strategic management of business from a process perspective and for the operational management of the business processes themselves. BPM, in the strategic scenario, comprises representing, understanding and managing a business in terms of an interdependent collection of business processes responsive to internal and external events. BPM, in the operational scenario, includes process definition, resource allocation and scheduling, process management and quality and efficiency measurement, and process innovation and optimisation (McGovern, 2004).

A fundamental characteristic of BPM is *"the ability to support the flexible management of dynamic business change"*. This is conceived from the process perspective as compressing time around the lifecycle model and the deployment of adaptive technology within process execution. BPM features *Late Bindings* which introduces flexibility into the run-time environment; a *Rules Engine* which facilitates complex expression evaluation independent of core process specification and *Adaptive Processes* which facilitate dynamic process changes during execution (Hollingsworth, 2004). Business process design is carried out by all BPM projects and is aligned to process modelling. The choice of the Business Process Modelling product is important and the expressive power of the language must be considered. Business Process Analysis (BPA/M) forms another important role in a BPM project and encompasses simulation, diagnosis, verification and performance analysis (van der Aalst et al, 2003).There is a perception that BPM is a synonym for 'advanced' workflow management. The relationship between Workflow management and BPM is illustrated in Figure 4.1.

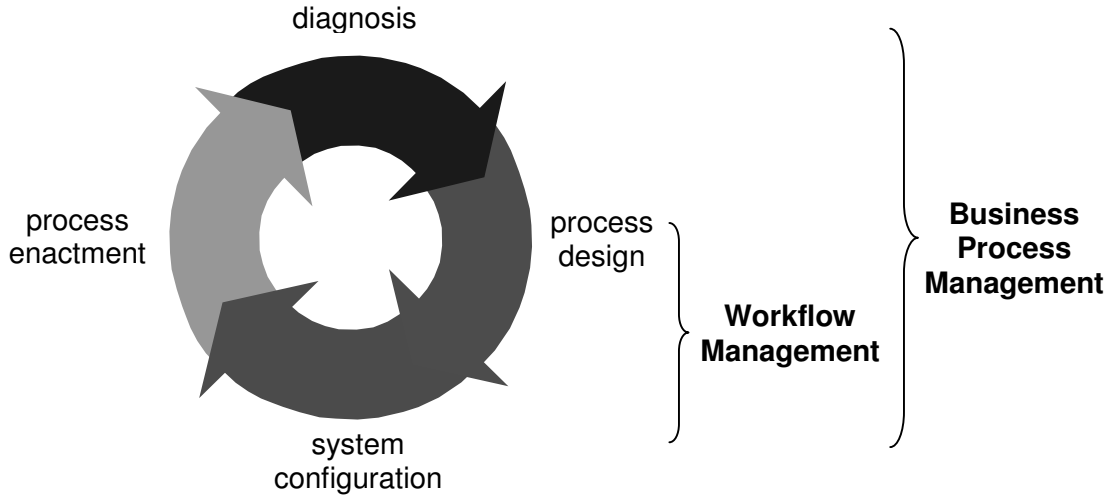


Figure 4.1 - Comparison between Workflow Management and Business Process Management
Sourced – van der Aalst et al (2003)

The BPM lifecycle describes the supporting phases of an operational business process as follows (van der Aalst et al, 2003).

- Design phase during which the processes are (re) designed;
- Configuration phase where the designs are implemented by configuring a process-aware IS;
- Enactment phase where, after configuration, the operational processes are executed;
- Diagnosis phase during which the operational processes are analysed to identify problems and improvement opportunities.

Traditional WfMSs concentrate on the lower half of the cycle with limited support for design and diagnosis. Few support the simulation, verification and validation of process designs through the collection and interpretation of real-time data. Conversely, BPM uses Business Process Analysis (BPA) and Business Activity Monitoring (BAM) as tools to diagnose operational processes.

4.4.2 Business Process Management Systems

The term BPMS pertains to an IS which manages the definition, supervision, customisation and evaluation of tasks evolving from business processes and from organisational structures (Karagiannis, 1995, van der Aalst et al, 2003). Its components can be characterised as belonging to six groups: User facilities; BPA/M facilities; Run-time components; Business Activity Monitoring (BAM) and Enterprise Performance Management (EPM); Infrastructure and System management (McGovern, 2004). The System management and User Facilities components, comprising B_2B portals and various dashboards, are self-explanatory and not examined further. The other four components are subsequently discussed in more detail.

A BPMS incorporates a suite of ***BPA/M tools*** through which users interact with the system. The definitions they provide are stored in a repository for both direct and indirect access by the *Run-Time system*. It includes a *Business Process modeller* which is the primary process design and change interface. An *IT Orchestration modeller/mapper* is used to define and maintain the technical flows which manage the IT resources. A *Business Transaction modeller* relates the transactions to process events. A *Technical Transaction modeller/mapper* maps the flows and events with various Atomicity, Consistency, Isolation and Durability (ACID) properties. A *Business Metrics modeller* relates the Key Performance Indicators (KPIs) to the raw measurements. A *Technical Measures modeller/mapper* specifies the technical measures and methods from which the business metrics are derived. A *Business Process Simulation and Animation* tool is an invaluable aid in the design and optimisation process. It permits the visual highlighting of bottlenecks and the identification of best-of-alternate process designs. A *Simulation Engine* increases the simulation validity through accurately representing the *Process Engine*. *Dashboards* are facilities which allow the monitoring of process instances and metrics as needed by business and technical stakeholders. They are personalised by the *Dashboard Designer.* The *Business Process Administrator* provides users with the ability to modify and control live process instances. The *Business Analyser and Report Generator* provides the computational analysis and report generation necessary in a customised Business Process environment (McGovern, 2004).

The ***Run-Time Components*** are the core of the BPMS. Their technical architecture, features and functions determine its operational availability, performance, efficiency and flexibility. The *Process Engine* is a central component and its purpose is to implement the business process and manage the real-time activation and completion of business functions. A *Distributed BPM Coordinator* enables B_2B and remote process invocation and requires a federated or distributed *Process Engine*. Each conversant has an independent view of the process and distinct security policies. A R*esource Manager* independently matches resource capabilities with run-time and definitional requirements and orchestrates the execution of the function. A *Scheduler* balances the timing dependencies and constraints, authorisations, load and capability of business functions to enable the BPMS to perform efficiently. A *Rules Engine* augments the *Process Engine* and the *Resource Manager*. It represents the permissible transactions of a process, its activity initialisation and completion conditions and resource optimising conditions. A *Hardware Interface Manager* supports the control of robotic and process control interfaces in a Business Process. An *Interface Manager* enables the *Process engine* to communicate with both control and data flows in a coordinated manner. It handles communication with transports, adapters and technical orchestration engines. The *Worklist Manager* provides the means for task delivery using either a push or pull method. A *Repository* is needed to store the data and metadata in the form of a Database Management System (DBMS). It contains many data objects including, for example, business process definitions, integrity rules, analytic and report definitions, security and policy definitions and transaction definitions (McGovern, 2004).

Business Activity Monitoring and Enterprise Performance Management is another important aspect of the BPMS. The ability to monitor events, analyse measurements and data and compute Key Performance Indicators is essential to managing processes because they enable intelligent BPI. BAM, which focuses on detection and response to real-time events, and the EPM, which focuses on detection, response and prediction based on business performance, both have the *Semantic Layer*, *Analytics Engine* and the *Rules Engine* in common. The *Semantic layer* handles the mapping between the business user views and the technical descriptions and references and enables the monitoring of the Business

metrics. The *BI/Analytics Engine* enables the execution of the packed, rules-driven computation of business metrics from low-level or technical measures. *Portal Management and Personalisation* allows the individual presentation of business metrics through dashboards deployed as portals. *Event Management* is the ability to detect business and technical events, interact with the *Rules Engine* and the *Analytics Engine* classifying the event, determining and executing the appropriate response. *Enterprise Information integration* (EII) provides the EPM and BAM with access to a wide variety of data sources not available to them as stand-alone products. The incorporation of the *Content Manager* into the BAM facility enables the detection of a broader range of data events because most business data is embedded within documents (McGovern, 2004).

The technology within the ***Infrastructure*** can be either simple or complex. The BPMS needs a *System Manager* as an IT support facility for installation, configuration and system management. An *Audit Facility* enables the auditing and tracking of the Business Processes, their audit conditions and points. It supports audit trail querying and report generation. The *Error Facility* handles unanticipated errors in a managed, consistent and auditable manner. The *Security and Policy Facility* enables a security model with respect to access, use and administration of the Business Processes. It ensures the security policy is enforced and business policies are not violated. The *Integration Infrastructure* covers a large spectrum of communication issues; from point-to-point integration to manually implemented business function communication to a full suite of business integration products. A BPMS operates best in a complete integration layer which can comprise the traditional EAI stack, Web services or other architectures. *Integrated Development Environment (IDE)* enables the development of new adapters and Web services which are process-aware. These suites of development tools, producing process-driven design and process-enabled, event or rules-based applications, become important as the use of BPMS matures (McGovern, 2004).

The elements within a BPMS (or BPMS components) have developed from simple workflow capabilities with limited support for BAM to sophisticated suites supporting manual and automated processes, BPA/M and with improved support for both BAM and EPM (McGovern, 2004).

An understanding of BPM and BPMS has been established. It is pertinent to examine the so-called agile enterprise, mentioned previously and to demonstrate the relationship between the agile enterprise, agile development methods and BPM, having established an understanding of BPM and BPMS.

4.5 Agile Enterprise Development

The business community required that the IT industry respond to their dynamic operating environment which obliges them to continually adapt their structures, strategies and policies (Abrahamsson et al, 2003, Nerur et al, 2005). Agile enterprises are the result of these developments (Baskerville and Siponen, 2002). This necessitated the progression of IT systems to the current instalment, BPM, which is characterised by agile development methods.

4.5.1 Agile Software Characteristics

The agile movement is broad in scope and is characterised by three features. First, it possesses a chaordic perspective which arises from the unpredictable software development environment. Project goals are defined whilst the details remain unpredictable. Second, it has collaborative values and principles in which Agile processes capitalise on individual and team strengths. Third, it uses the concept of barely sufficient methodology to establish the development structure needed. Agile methods balance flexibility, structure and bare sufficiency to reduce costs, through streamlining, whilst increasing innovation through incorporating the chaordic perspective (Highsmith, 2002). There have emerged numerous agile development methods.

4.5.2 Agile Software Methods

Agile software development is both incremental and iterative with short release cycles which enable fast verification and correction. There is close customer and developer interaction which results in a collaborative working style. Its methods are simple and provide sufficient documentation and are regarded as adaptive because they can react to last moment changes. Its goal is to increase the ability to react and respond to changing business, customer and technological needs at all organisational levels (Abrahamsson et al, 2003).

Examples of agile development methods include Adaptive Software Development (ASD); Extreme programming (XP); FDD and Internet-speed development (ISD)

(Gotterbarn, 2004, Abrahamsson et al, 2003, Highsmith, 2002). Some of their objectives are briefly described. The ASD method replaces the traditional plan-design-build lifecycle with a dynamic speculate-collaborate-learn cycle and is dedicated to continuous adaptation (Beznosov and Krutchen, 2004, Highsmith, 2002). It promotes an adaptive paradigm and claims to provide sufficient guidance to prevent chaos but without suppressing emergence and creativity (Abrahamsson et al, 2003). XP provides a set of recognized engineering practices, which enable software development despite changing requirements. It is characterised by small releases, rapid and continuous feedback, integration and close developer / client relationships. FDD is a process-driven method for developing business critical systems. It typifies the iterative development approach and emphasises quality through accurate monitoring of the project process (Highsmith, 2002, Abrahamsson et al, 2003). ISD is typified by short development cycles which produce fast released software. It draws from the 'synch-and-stabilise' approach of Microsoft that aims to cope with rapid software development and emergent organisations (Abrahamsson et al, 2003). These agile methods rely on the gradual emergence of the design and requirements and emphasise collaboration. They differ fundamentally, in concept, from traditional software development methodologies (Nerur et al, 2005).

4.5.3 Agile versus Traditional Software Development Methods

The agile software development trend is enduring and adopting it into organisations immersed in traditional software development methodologies presents challenges because the two are conceptually opposite.

A rational, engineering-based approach has dominated the traditional software development environment which assumes that problems are fully specifiable and solutions are optimal and predictable. It is process-centric and focuses on variance-elimination through continually controlling and refining the process in a PDCA cycle. The waterfall or spiral lifecycle models are generally used which specify tasks and their outcomes. Communication occurs with the customer during the specification phase and through the formal specifications documentation. Agile software development methods are people-centric which deal with unpredictability through short, iterative development cycles. Product features, collaborative decision-making and project-decomposition favour the development

and delivery of sub-projects. Developers work in small teams and the customer is an active participant, therefore, communication is continuous through the evolutionary-delivery lifecycle. Formal documentation is discouraged (Nerur et al, 2005, Turner and Boehm, 2003).

These differences create organisational culture and management issues. Culture wields significant influence during decision-making and management strategies. Traditional cultures provide clear policies and procedures within a production-line like environment. The roles of the stakeholders are defined and empowered by providing an operational comfort zone. Agile cultures, however, empower through the degree of freedom provided, in a classic craftsman environment, to define and complete work projects. Agile methods need a leadership-and-collaboration style of management to facilitate its dynamic features instead of the traditional style of command-and-control. Both traditional and agile development projects need their customer representative to be Collaborative, Representative, Authorised, Committed and Knowledgeable (CRACK) within their own organisation to enable the developers to deliver acceptable products (Nerur et al, 2005, Turner and Boehm, 2003).

Both approaches affect information security issues which is of special interest to this research. Traditional methods exploit a 'plan-build-implement' model whilst agile methods use a 'speculate-collaborate-learn' approach. Traditional approaches use the waterfall lifecycle model whose planning and design features promote security assurance and external security certification. However, the agile method feature of de-emphasising intense documentation is contrary to system certification (Beznosov and Kruchten, 2004). There are a variety of methods which address agile security assurance. FDD is an agile development approach that is used in a variety of agile security and assurance solutions and it is pertinent to briefly examine its approach.

4.5.4 Feature Driven Development

Feature Driven Development (FDD) is an agile software development method. It provides concrete modelling techniques and accepts the concept of software development as a people-centric process. FDD provides an agile and adaptive systems development approach. It focuses on the lifecycle phases of design and build and is cooperative across development activities whilst maintaining a

process-model independence. It is an iterative development approach which uses industry best practices. Quality is continually emphasised through frequent deliverables and accurate monitoring (Beznosov and Kruchten, 2004, Gotterbarn, 2004, Siponen, Baskerville and Kuivalainen, 2005, Nerur et al, 2005, Highsmith, 2002, Palmer and Felsing, 2002).

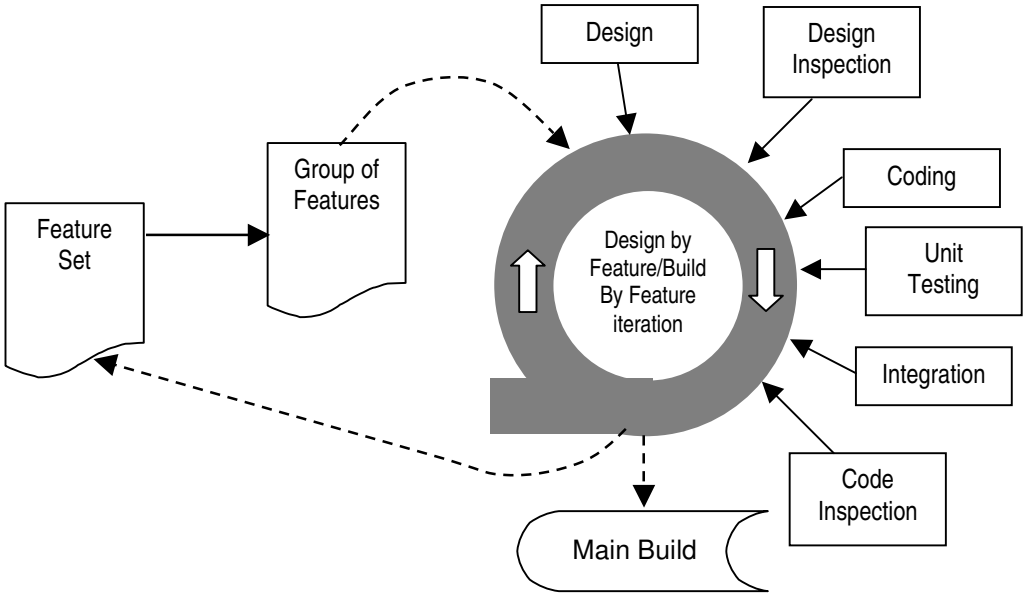


Figure 4.2 - Design and Build by Feature Phases
Source Abrahamsson et al (2003)

Feature Driven Development comprises processes which are both sequential and iterative as illustrated in Figure 4.2. Its sequential processes are used during the system design and implementation while its iterative processes support agile development through rapidly adapting to changing business needs. The five processes of FDD are (Palmer and Felsing, 2002):

- Develop an overall model during which the overall system scope and context is established and decomposed into object models. These are continuously reviewed and refined;
- Build a features list during which a comprehensive list of features is constructed using the domain object models;

- Plan by feature during which a high-level plan is developed to sequence feature sets by their priority and dependencies and which assigns their goals, schedules and deliverables;
- Design by feature during which the feature design packages are produced. It is an iterative process;
- Build by feature which entails coding the features, performing unit testing, integration and code inspection.

The Design and Build by Features phases are re-iterative and comprise the development engine room. A features list is built using the object models and documented requirements and includes client-valued functions or features for each domain area. Features are client-valued and, in a business system, a feature maps to a step in an activity within a business process. The features list is reviewed by the system stakeholders for validity and completeness. Features are expressed in Client-valued terms, using the <action><result><object> syntax. Their level of granularity is specified and they allow measurable, visible progress which improves project confidence and enables early feedback opportunities. Examples are 'RETRIEVE the BALANCE of an ACCOUNT' and 'VALIDATE the PASSWORD of a USER' (Palmer and Felsing, 2002).

The FDD approach provides a resilient conceptual framework. The iterative and self-organised Design and Build by Feature phases provide an agile operational environment that is adaptable (Palmer and Felsing, 2002). The best practices that comprise FDD are not original but, it is claimed, their specific combination makes the FDD processes unique. Each practice complements and reinforces the others. These practices comply with FDD development rules, however, their use is based on the experience of the development team (Palmer and Felsing, 2002). The benefits of FDD and its place within the current milieu of agile methods are relevant to this research.

4.5.5 Relevance of Feature Driven Development

Feature Driven Development is considered by many practitioners to be the epitome of agile software development methods because it meets many of the specified agile criteria. It is highly iterative and co-operative, delivering frequent and quantifiable results together with accurate progress reports. It is considered to

be a people-centric approach whilst remaining documentation-light. It is seen as flexible to changing business needs (Palmer and Felsing, 2002). It is used as a basis for a variety of security solutions because it provides the means to integrate security features into the agile development process (Siponen et al, 2005). Its applicability is further examined in the research solution presented in Chapter Five.

The FDD approach emphasises quality from two interrelated aspects. Internal quality from the system viewpoint of the developer, and external quality from the system viewpoint of the user. Its incremental approach emphasises the role of internal quality. The design must be sufficiently strong to accommodate any extended functionality without needing rework. The short cycle time and early testing of features together with monitoring and metrics tools are methods used by FDD to enhance quality throughout the development process (Palmer and Felsing, 2002).

4.6 Critique of Agile Methods

It is proposed during this research that using an agile approach will aid the integration of security into a business process. It is necessary to critique these approaches to present a balanced viewpoint.

Agile approaches are people-centric and depend on using customers who are active participants. This is not always possible especially during complex projects (Nerur et al, 2005, Turner and Boehm, 2003). The changing of organisational attitudes, from a process to people-centric focus, is problematic especially where a CMM-based program has achieved higher levels of maturity. It requires considerable time and resources to change organisational behaviour (Nerur et al, 2005, Highsmith, 2002). Agile methods rely on tacit knowledge which is shared though communication and collaboration. This reliance is dangerous because of the scalability laws for group communication which maintain that a larger team requires more communication paths to be kept current (Nerur et al, 2005, Turner and Boehm, 2003).

Agile methods use minimal documentation. This poses difficulties for security assurance and accreditation, certification, evaluation and third party review. Agile methods use refactoring and its testing philosophy clashes with security assurance

practices. The involvement of security evaluators and third parties during the iterations may be prohibitively expensive. The testing philosophy focuses on a test-driven development (TDD) which is thought to facilitate the continuous integration of changes. This early and routine functionality testing is different to security testing which uses a depth-of-test analysis (Abrahamsson et al, 2003, Nerur et al, 2005, Beznosov and Kruchten, 2004). In terms of the solution proposed in this research (i.e. using an agile development method to integrate security into business processes), these security-related predicaments require that a means of achieving agile security assurance be further investigated. This is done in Chapter Five

Agile methods favour object-oriented (OO) technologies which progressed through UML and the Rational Unified Approach (RUP) to the current ISD (Abrahamsson et al, 2003, Nerur et al, 2005). The people-centric emphasis of agile methods support developer creativeness but without concern for those affected by the system. This narrow focus ignores software development as part of a functioning system that interacts with other entities. This is surprising given their stated objective is to avoid unplanned side-effects. UML is often used to document the system and its scope. Failed projects confirm that these failures occur because the identified stakeholders are limited to the developer and the customer. Neither agile methods nor UML, however, address this problem and specifically narrow the design focus (Gotterbarn, 2004). It is suggested that a revised notation for UML to include a broader range of stakeholders may reduce the problem of narrow context. An agile testing scenario which includes a wider consideration of the affected stakeholders may equally help reduce this problem (Gotterbarn, 2004).

Agile approaches were developed to satisfy the needs of the business community to produce lighter weight and faster, nimbler software development processes (Abrahamsson et al, 2003). This business environment created the IT development, BPM, in answer to this need and agile methods support this paradigm. BPM requires a similar critique to present a balanced viewpoint.

4.7 Critique of Business Process Management

The evolution of BPM centres on existing technology, including workflow, EAI, activity monitoring, BPR and Web services (Pyke and Whitehead, 2003,

McGovern, 2004). Much of the technology efforts that underpin BPM originates from the Workflow community which is augmented to provide robust, scalable transactional BPM products. The arrival of sophisticated process engines and EAI infrastructure allowed the management of the business process life-cycle. It has, as an industry, matured over the last five years into a category of products and services (McGovern, 2004).

The analyst definitions of BPM are approaching close agreement, with differences in perspective only. The BPM products offered by EAI vendors are seen as middleware which is used to accomplish business process automation and integration. The increased role of Web Services orchestration in process integration blurs the distinction between BPM and EAI. It is likely that application areas which are highly responsive to BPM, such as CRM, supply chain management and similar application areas, will be subsumed or incorporated by BPM. Other analysts recognise that there is a synergistic relationship between BPM and integration infrastructure. BPM enables focused, business-driven application integration whilst an integration infrastructure enables BPM. Some analysts consider the BPMS to be a natural extension of a WfMS while others view BPM as a revitalisation of BPR. The overall view of BPM is dependent on the market it is servicing (McGovern, 2004).

The BPR movement promoted the concept of CPI and early BPM implementations supported this methodology. The practical implementation of CPI can be problematic because it often involves the entire process life-cycle. The newer BPM promotes dynamic process optimisation in which key elements are optimised piecemeal, without redeploying the entire process. This approach allows an enterprise to make regular changes to processes which can take many years to complete, proving that BPM supports long-running processes. An example of the longevity and endurance of BPM cites the Dutch Government maintaining processes which possess a quarter of a million activities with five-year long change periods (Ghalimi and McGovern, 2004).

There are many organisational and commercial variables within a BPM solution. The implementation of improved BPM software tends to produce improved business processes which needs to be proven through scenario simulations (Pyke and Whitehead, 2003). The success of any IT initiative is judged by determining

the degree to which it has improved the business processes it was designed to support.

4.8 Conclusion

Chapter Four discussed the business paradigm, BPM, as one of the three pillars of this research. It provides the business paradigm from which the business process originates. The evolution and drivers of BPM together with the business process, as the foundation of BPM, were discussed. The principles of BPM and BPMS were investigated in some detail. Finally, the concept of the agile enterprise and its supporting development methods were introduced. The agile software development method, FDD, was examined in detail because it is used as a means to illustrate the integration of security into the business process which forms a component of the BPSM, as proposed by this research.

In Chapter Five, the relationship between security and the agile development methods is discussed. The convergences between the information security management framework, being the ISO17799 standard and the security metric, being the SSE-CMM, and the business methodology, BPM are presented. The relationship between the ISO 17799, the CMM and BPM is examined. A method to both promote security assurance and to integrate security into the agile enterprise using an agile software development method is discussed.

5 - CHAPTER FIVE – A BUSINESS PROCESS SECURITY MATURITY MODEL

Chapter Five presents examples of models which use both the ISO 17799 security standard and the SSE-CMM to assess security maturity. Business Process (Management) maturity models which assess the maturity of the business process and the maturity of the BPM implementation are discussed. The paradigm convergences that exist between the three pillars of the BPSM model are examined. Methods to ensure security assurance and to introduce security into the business process in an agile enterprise environment are discussed. Finally, the BPSM model is presented and its phases are described in detail together with a possible example of its output.

5.1 Introduction

The three pillars of this research, namely the ISO 17799 security standard, the SSE-CMM metric and the business paradigm BPM were discussed in the previous chapters. The ISO 17799 and its application through an ISMS were examined. The increasing need for security in the current emergent environment was examined together with the attendant increasing importance of security engineering. The SSE-CMM was examined and the impact of process maturity on the security engineering process was considered. The BPM paradigm was examined together with the components of a BPMS and an agile software development method to integrate security at the business process level.

The premise of this research is that sufficient paradigm convergences exist in the three pillars of this work – the ISO 17799 security standard, the SSE-CCM security metric and BPM, to formulate a means to integrate security into the business process itself. In this chapter, various examples of security assessment models using a combination of the ISO 17799 and the SSE-CMM to evaluate the maturity of security are examined. Examples of CMM-based maturity models to evaluate business process and BPM maturity are discussed. The aim is to establish the relationship between the SSE-CMM, ISO 177999 and BPM to identify specific points of convergence. The agile enterprise and the agile development methods pose specific security and assurance challenges and a means of introducing

security into the agile development paradigm is examined. Finally, the BPSM model is detailed as the primary output of this research.

5.2 Preliminary explication of paradigm convergence

Security engineering is part of information security efforts at an organisational level. An organisation exists to satisfy its strategic goals which are related to its external market factors. These drive it to arrange its activities into cost-effective relationships or 'value chains' which include the support and core business processes. The security engineering process, in an ideal world, is integral to these business processes. Information security issues are broad and encompass security policy, risk analysis and management; security architecture; security standards and procedures and the ISMS (Hong et al, 2003, Eloff and Eloff, 2003). This security posture does not exist in isolation. The lack of security process maturity and control represent the inability to sustain a security posture which results in security slippage (Tiller, 2005).

Security engineering exists within the overall information systems security process. The system security position is evaluated and evidence is identified, gathered and analysed against criteria for security functionality and an assurance level. This results in a measure of trust indicating the degree to which the system meets its particular security targets (Chaula et al, 2004).

An ISMS approach, when based on a recognised standard such as ISO 17799, ensures internal or external certification by First Party or Third Party auditors (Spears et al, 2004). This certification proves that the organisation, who is implementing the standard; is in compliance, demonstrates '*due diligence'* and can be considered a trusted party in a business relationship (Carlson, 2001).

The SSE-CMM approach will help overcome the 'development duality' phenomenon by dynamically designing security into the business process within the BPM environment. It allows organisations to evaluate their security engineering processes through a governance program which provides a quality cycle. The use of a security guidance standard, such as the ISO 17799, together with the SSE-CMM enhances its effectiveness and the return achieved (Tiller, 2005).

It becomes apparent, taking cognisance of the discussion in the dissertation so far, that the establishment of an information security management system, based on the internationally recognised security standard, the ISO 17799 which is the focus of this research, together with a security maturity measurement capability, based on the SSE-CMM as proposed by this research, is indispensable when considering the openness and interconnectedness of the current enterprise environment as reflected by the BPM paradigm. The literature reveals an abundance of research outputs which are typically based on the convergence of these two areas, namely the ISO 17799 and the SSE-CMM. An overview of literature relevant to this research is presented in Section 5.3.

5.3 Research Addressing the Concomitant Use of the ISO 17799 and the SSE-CMM

There are a variety of research projects and methods available which combine the use of the ISO 17799 security standard and the CMM and its security version, the SSE-CMM. It is relevant to examine some models and methodologies which are of particular interest to the proposed solution of this research, the BPSM model.

5.3.1 Security Assessment Model (SAM)

Tse (2005) in, Security in Modern Business: Security Assessment Model for Information Security Practices, examines a variety of security frameworks including SSE-CMM and ISO 17799. The ISO 17799 is seen to offer a model to govern business information security and it possesses a clear set of security goals and objectives. It can be used as the foundation to build a security model. The SSE-CMM is seen to describe essential security engineering processes but is only a consultative model. A new Security Assessment Model (SAM) is developed which combines the benefits of the authoritative ISO 17799 with the SSE-CMM improvement concept.

Tse (2005) states that the security topics of ISO 17999 are similar to key SSE-CMM Process Areas. They describe information security domains and logically list their tasks. The domains are not of equal strength and will possess different maturity levels. The criteria of the maturity levels are investigated to fit to the appropriate ISO 17799 components. The result is SAM and an example is presented in Table 5.1.

Key Process Areas / Practices	Maturity Level			
	2	3	4	5
Security Policy **Information Security policy**				
Information security policy document	✓			
Review and evaluation		✓		

Table 5.1 - "SAM" Information Security Assessment Model - Source Tse – 2005

Tse (2005) concludes that there are a variety of results from using SAM. It provides an awareness of the information security practices of the organisation and its business partners. A higher maturity level implies the existence of good information security practices whilst, conversely, the lower levels imply a non-appreciation about their importance. A higher-level organisation, when dealing with a lower level organisation, risks data contamination which can cause the higher-level organisation to lose its competitive advantage or affect its relations with organisations with still higher maturity levels. SAM provides a yardstick through which organisations can measure any improvement in their security practices. It provides the guidelines to achieve the desired security maturity level per the domains as defined by the ISO 17799:2000.

There are limitations to SAM, according to Tse (2005), for example, because it uses continuous improvement to either maintain security maturity or enhance security practices, it requires investments in hardware and software to achieve the initial certification and subsequent investments in continuous improvement costs.

The SAM provides a good example of convergence between the ISO 17799 and the SSE-CMM and that it is possible to construct a viable security management approach by combining two diverse models.

5.3.2 S-vector Methodology

Spears et al (2004) in, An Analysis of How ISO 17799 and SSE-CMM Relate to the S-vector Methodology, analyse the ISO 17799 and SSE-CMM, to determine whether these standards can be integrated into a web-application security assessment tool called S-vector or security scoring vector. The ISO 17799 is examined and its concepts are applied to S-vector which results in a Scoring Metric for incorporated ISO 17799 controls. SSE-CMM and its appraisal method, SSAM, are examined and the applicability of its process areas and capability levels are explored.

The S-vector methodology focuses on the periodic assessment of web applications whose security needs are mapped to a requirements vector which contains a target score. Its goals are to prioritise security enhancements, evaluate security strategies and measure security improvements in web applications security (Spears et al, 2004).

The S-vector relies on organisational policies to classify the assets and determine their security requirements. It uses the ISO 17799 to evaluate the quality and existence of policies and controls. A potential scoring metric is proposed, which incorporates the requirements vector containing the relevant ISO 17799-based controls. A 5-level Lickert scale is used to score the quality of each control. A security appraisal checks the existence and quality of each control and compares the actual to the target scores. S-vector elements can be re-grouped by scope and topic and scores sub-totalled to compare across groupings (Spears et al, 2004).

Spears et al (2004) maintain that the process areas and capability maturity levels are both applicable to S-vector. The 11 security-related process areas can be incorporated into the S-vector using a metric scheme which is different to the maturity levels. The maturity of the S-vector components can be assessed regardless of their origin. Capability levels assess the maturity of a given process but do not measure its quality. They determine that a component is well defined and monitored based on its scoring objective. A requirement S-vector can be populated with a target capability level and by using the SSAM will determine the actual capability levels (Spears et al, 2004).

Spears et al (2004) state that the ISO 17799 provides the controls to populate the security vectors whilst the SSE-CMM establishes a mature, institutionalised framework for security administration. Specific security controls, provided by ISO 17799, require a security infrastructure which is provided by SSE-CMM, to develop, monitor and control them. It was determined there was no overlap or redundancy between the ISO 17799 and SSE-CMM and that the two standards complement each other. SSE-CMM has a PA for administering controls without recommending the controls, for example. ISO 17799 recommends the controls but does not provide details on their administration but, it does recommend conducting periodical risk assessments. The SSE-CMM furthers this recommendation by assessing the maturity of the risk assessment process.

The benefits from using the SSE-CMM and ISO 17799 in the S-vector security assessment tool are (Spears et al, 2004):

- A security framework developed and maintained by SSE-CMM ensures, with a high degree of assurance, that processes reach the desired level of maturity and are maintained on a continuous basis;
- All documentation, including the security policy, is maintained and is current;
- The incorporation of ISO 17799 controls is valuable because the standard is internationally recognised and provides a comprehensive set of web application controls to support S-vector procedural controls.

It is noted that both an asset inventory and risk assessment provide input for the security requirements and that formal methods should be employed to ensure an effective S-vector appraisal (Spears et al, 2004).

5.3.3 TrustCheck Approach

TrustCheck is a security measurement tool developed by International Network Services (INS). It combines evaluation tools and various certified methodologies. It evaluates a security program, assuming the use of industry best practices, to provide a perspective of maturity and capability. Trustcheck has modules for a variety of industry standards including the ISO 17799. It is used to establish the existence and overall management of security compliance efforts and its combination of an established analysis process based on SSE-CMM and the specific modules represent a departure from traditional assessments. It permits a degree of customisation by producing both industry and organisation-specific modules (Tiller, 2005). The INS-certified methodologies and SSE-CMM are non-prescriptive frameworks which provide guidelines. A CCM-based matrix is developed which defines the attributes required at each level. The matrix appears in two forms: first, as supportive documentation and secondly, as statements incorporated into each ‘investigative point’. The ISO 17799 module is the focus of this research. It contains some 600 ‘investigative points’ (questions or statements) which guide the appraisal process.

The appraisal process appears complex and time-consuming but is seen as an efficient process. The ‘investigative points’ are used as the basis for the evaluation and TrustCheck frees the investigator from excessive calculation duties. The

assessment data provides various visual representations including a scorecard with textual commentary, findings and recommendations on leveraging strengths and addressing weaknesses (Tiller, 2005).

Tiller (2005) summarises that:

- Adopting a CMM allows organisations to investigate the effectiveness of their processes, clearly visualise their current state and make informed investment decisions about security whilst being able to predict the outcome and its effect on their security posture;
- The use of a CMM further allows the evaluation method to remain constant and makes it possible to demonstrate direct process improvements.

It is further concluded that the advantages of linking these efforts to an industry-accepted standard, such as the ISO 17799, are to exhibit compliance, best practice support and due diligence.

5.3.4 Discussion of Security Maturity Approaches

Three security maturity approaches, namely SAM (Tse, 2005), S-vector (Spears et al, 2004) and TrustCheck (Tiller, 2005) have been discussed and it is necessary to examine their points of comparability, divergence and their relevance to the proposed solution of this research. There are commonalties between these approaches. There appears to be neither overlap nor redundancy between the ISO 17799 and SSE-CMM and they are seen as complementary. SSE-CMM administers the security controls without recommending the actual controls. ISO 17799 recommends the actual security controls but provides no details on their administration. The integration of the two standards is possible and the capability levels can be applied to the ISO 17799 controls to measure their maturity (Spears et al, 2004). Tiller (2005) maintains that increasing maturity shifts the focus of security from the attribute to its organisational role. Therefore, maturing security processes create security practices that are more business-appropriate and reflect the security posture and risk profile of the organisation. SSE-CMM provides a consultative model to govern business information security, whilst the ISO 17799 provides the security goals and objectives and the specific security controls to populate the security framework. The domains of the ISO 17799 are similar to the key security process areas of the SSE-CMM (Tse, 2005).

SSE-CMM provides the framework for developing an institutionalised security process that operates in an environment of continuous security process improvement. The ISO 17799 provides guidelines for security controls at both organisational and application-level and is used as a guideline to provide the security controls that populate the security framework (Spears et al, 2004).

The focus now shifts to an investigation of published literature on the convergence between the CMM and BPM (i.e. Business Process Management Maturity Models). Harmon and Wolf (2005) note that there are ongoing efforts to create new maturity models which extend beyond the CMM and are tailored to current business needs. Examples are the Business Process Maturity Model (BPMM) developed by Drs Bill Curtis and John Alden which views the BPMM as a natural extension of the CMM, and the Harmon CMM-based model developed as part of BPMI efforts, for evaluating the maturity of business processes. Rosemann and de Bruin (2005) comment that BPM is a potential area for the development of a maturity model. Two such maturity models are subsequently discussed.

5.4 Business Process Management Maturity Models

It is significant that attempts to define BPM Maturity models as proposed by Rosemann and de Bruin (2005), Harmon (2004) and Smith and Fingar (2004a) are all based on the CMM. The Harmon (2004) and Smith and Fingar (2004a) models are discussed as examples. These two maturity models are distinct in focus and represent the dilemma that has emerged in developing a BPM Maturity model and evaluating BPM maturity status.

5.4.1 Business Process Maturity Model – Harmon Model

Harmon (2004) developed a light-weight, generic approach to evaluate business process maturity. It employs the CMM levels of maturity and the same terminology. An audit approach is proposed to establish a benchmark to determine progress and to recommend improvements. This analysis includes interviews, documentation reviews and questionnaires. The author (2004) presents a simple checklist to informally evaluate the maturity level of a business process, an example of which is presented in Table 5.2. It illustrates his use of the CMM maturity level nomenclature. There are basic similarities between the maturity levels in the Harmon model and the CMM.

Checklist for evaluating the Maturity of an Organisation / Process	
Level 1 Initial	Processes are not defined.
Level 2 Repeatable	Some processes are defined.
Level 3 Defined	Most processes are defined. The relationship between specific processes and super-processes, and value chains is well defined. Some process measures are defined.
Level 4 Managed	Processes have well defined measures which are vertically aligned. Data from Process metrics is recorded, analysed and consulted to predict future outcomes.
Level 5 Optimising	Company processes are well measured and managed. Process improvement teams constantly work to improve the effectiveness, efficiency and consistency of existing processes.

Table 5.2 - Checklist for Assigning a Maturity Level to an Organisation or a Process

5.4.2 Business Process Maturity– Smith and Fingar Model

Smith and Fingar (2004a) note that developments in process maturity are motivated by the CMM. BPM focuses on delivering optimised business performance and accelerating strategic innovations. However, it is necessary to separate BPM methods from the processes they manage when developing a BPM maturity model.

Smith and Fingar (2004a) illustrate the orthogonal relationship between process maturity and BPM maturity as depicted in Figure 5.1. It details the progression to Operational Excellence on the CMM-inspired X-axis from an immature organisation to a mature one. The lower right-hand corner represents an organisation as CMM-mature while the lower left-hand corner represents an organisation that is CMM-immature. The BPM-inspired y-axis represents Operational Innovation in the top left-hand corner. Its characteristics represent an organisation explicitly using BPM. The Operational Innovation descriptors namely; creative and collaborative, are similar to those of agile development methods, as discussed in Chapter Four, Section 4.5.1.

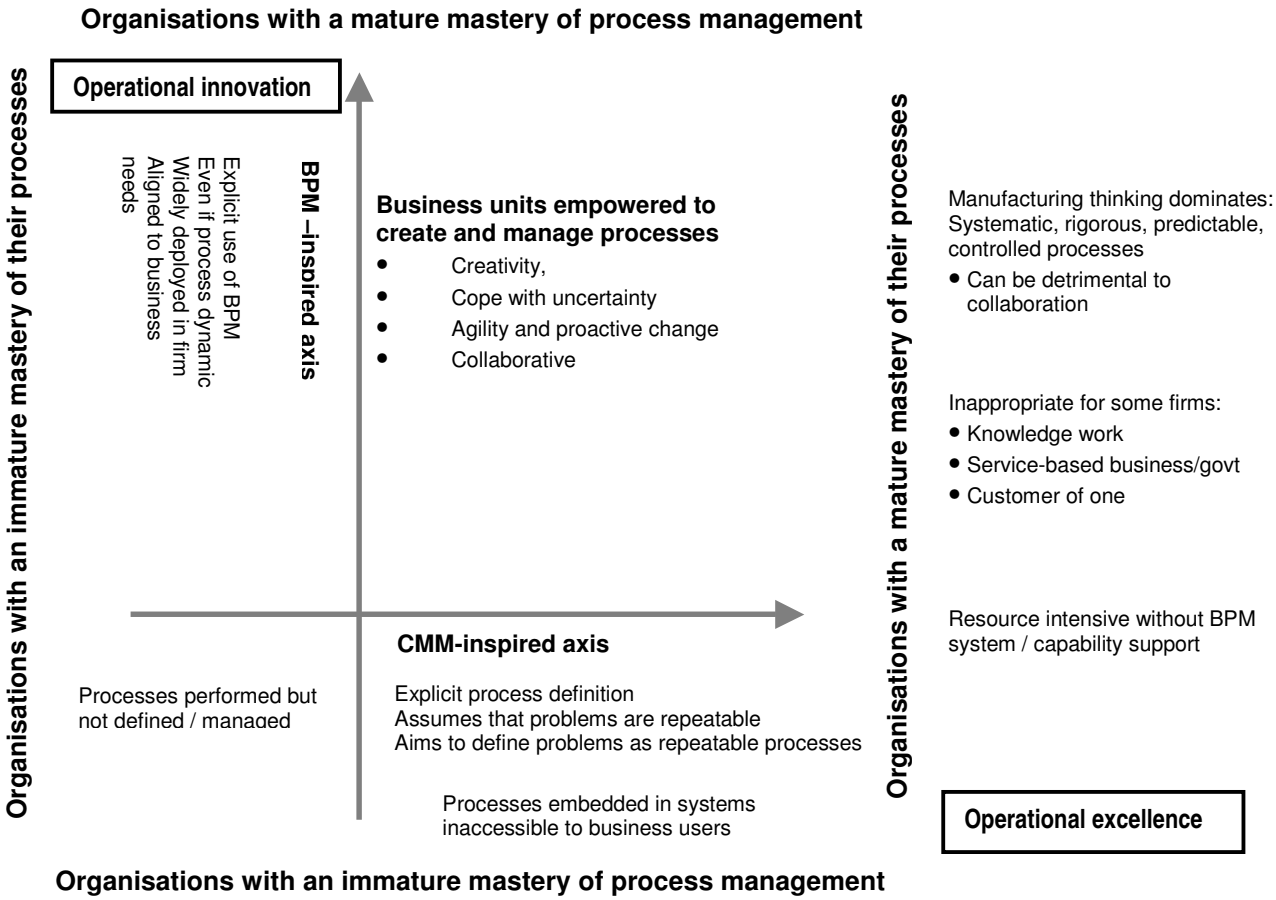


Figure 5.1 - BPM Maturity Orthogonal Model - Source Smith and Fingar (2004a)

Smith and Fingar (2004a) propose five levels of BPM maturity in their Process Management Maturity Model:

- Level 1 (Absent) which implies the organisation has no BPM system in place;
- Level 2 (Present) which implies the existence of some BPM systems which are applied in an ad hoc manner;
- Level 3 (Utilised) which implies BPM is applied to one or more core process and is aligned to business goals;
- Level 4 (Aligned) which implies the enterprise-wide use of BPM which is proactively used to align operations with optimal design criteria;
- Level 5 (Leveraged) which implies the use of BPM to actively implement agile course corrections.

The focus is on the maturity of a BPM culture within an organisation. Smith and Fingar (2004a) maintain that the CMM brings value to the business process arena, but poses the dilemma that operational excellence is achieved but through a level of conformity. CMM provides little guidance on process management capability and rather replaces an old process with an improved one.

Smith and Fingar (2004a) further maintain that CMM-based maturity frameworks concentrate on process improvement whilst the objective of BPM maturity concentrates on the process management capability. The principles of CMM are applicable to BPM but require extension to accommodate business innovation. Therefore, the term maturity adopts a new meaning in a BPM-maturity framework and implies the comprehensive use of executable process knowledge throughout the organisation.

5.4.3 Discussion of BP(M)-Maturity Models

The previously discussed examples of BPM maturity models are both CMM-based but exhibit differing focus. The Harmon CMM-based Business Process Maturity Model, evaluates the maturity of the process improvement efforts within the organisation. The evaluation is carried out to determine the current status of the business processes and to recommend areas for process improvement. It is based on the premise that a mature organisation achieves its goals systematically while immature organisations use ad hoc and spontaneous methods to achieve their goals. The model holds that mature organisations have systematic and documented processes which can be used to accurately predict future results. There is an emphasis on continuous process improvement enabled through quantitative feedback and piloting innovative projects.

The Smith and Fingar Process Management Maturity Model uses CMM-based principles to initiate the maturity levels of the model but maintains that business innovation is beyond the CMM ambit. In a CMM-based maturity stack, an increase in a maturity level implies that the processes are progressively formalised and controlled and that at Maturity Level 5 (Optimising) process improvement efforts are continuous. It is their concern that the CMM-based maturity of business processes can be incorrectly conflated with the maturity with which organisations apply business process management. CMM brings great value to the business process improvement efforts but the concern is that as an organisation achieves

operational excellence, it brings process conformance. This may be inappropriate in a growth-market business environment where innovation is needed to harness the necessary operational transformation.

It is apparent that the two models have a different focus but they are both examples of maturity models for BPM that are based on the CMM. There is concordance between the maturity model presented by the CMM and in the BPM maturity models examined. The factors motivating the use of the maturity model are similar, namely to improve process efficiency and quality. The results of conducting the maturity appraisal sets the development targets based on the maturity level that the organisation wants to achieve. The gap between the desired and actual maturity levels aids planning the development projects. It provides the guidance needed to prioritise, implement and monitor any improvement efforts.

The BPSM model proposed in this research does not target the maturity or performance of the business process or the maturity of the BPM implementation. Distinctly, its focus is on the maturity of the security process as implemented within the business process. The three pillars of this research have been extensively reviewed together with examples of models and methodologies which represent their combination. It is relevant to shift the research focus on to their paradigm convergences to support the premise behind the BPSM model.

5.5 Paradigm Convergence

It is the opinion of the author that the proposed solution of this research, to provide mature process security, within the BPM environment, by employing the SSE-CMM and ISO 17799, is feasible. A variety of examples have been discussed and the overall opinion is that it is a workable and advantageous union of two complementary standards which provide specific security controls within a security framework to administer and manage the security program, together with a governance framework which ensures the creation of mature and institutionalised security processes. The discourse in this dissertation, up to this point, can be illustrated diagrammatically in a conceptual framework as depicted in Figure 5.2.

Various examples of research positioned in the converging areas indicated by A and B respectively in Figure 5.2 were discussed. These comprise, firstly, the CMM-based BPM maturity models which are depicted in Area A and secondly, the

combination of the ISO 17799 security standard and the CMM or its security version, the SSE-CMM, to create an information security management framework as depicted in Area B. It was not possible, during the literature review, to find publicly accessible research results which address the paradigm convergence of BPM within both an information security management and a security maturity approach.

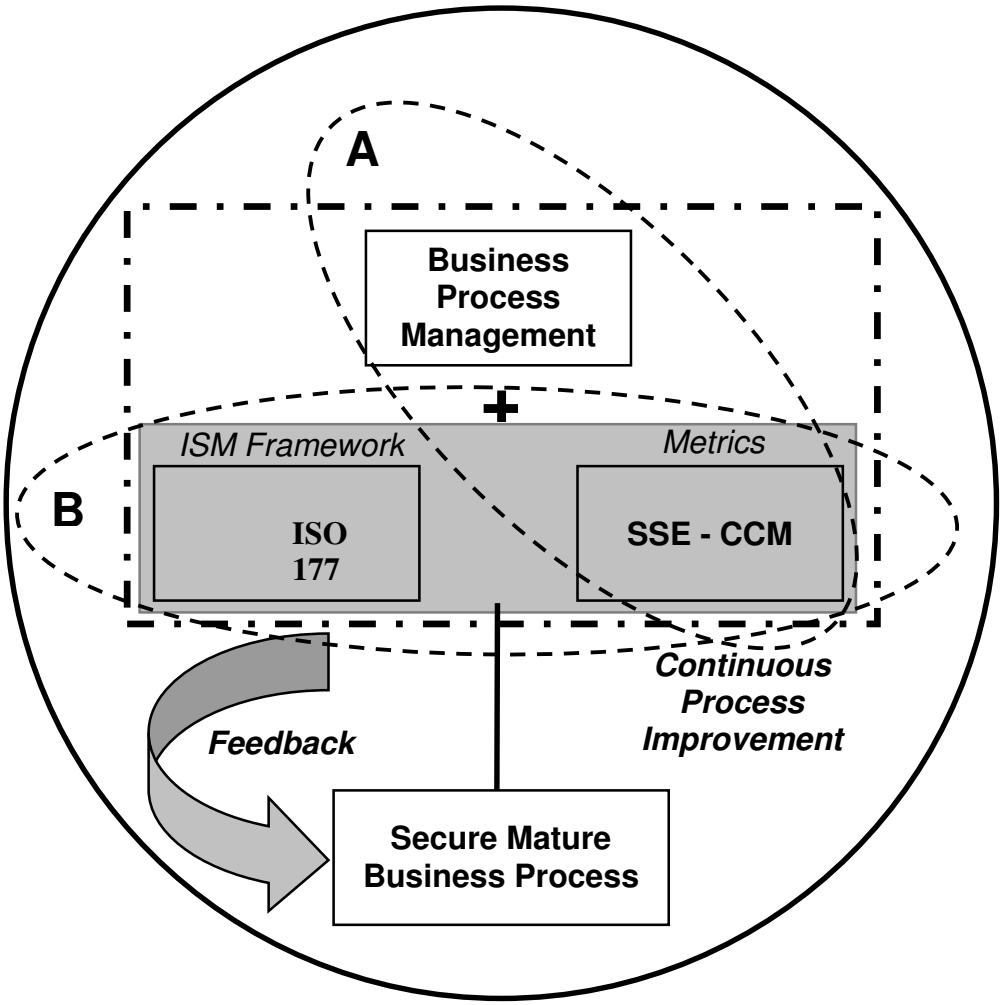


Figure 5.2 - Paradigm Convergence

It is the objective of this research to propose a model which incorporates the three paradigms. However, it is first necessary to explore a development method which can be used to illustrate the output of this research in a tangible way, therefore, it is necessary to discuss agile security assurance methods. Emergent or agile organisations, as mentioned in Chapter Four, require their IS to evolve to meet their changing requirements. Agile development methods were investigated and discussed in Chapter Four and their underlying concepts examined. During the

critique on agile methods, presented in Section 4.6, it is stated that agile approaches support the BPM paradigm but that it has various characteristics which pose difficulties for security assurance, accreditation, certification, evaluation and third-party review. This requires investigating a means of achieving agile security assurance.

5.6 The Complexities of Agile Security Assurance

Assurance was previously defined as the degree of confidence that security needs are satisfied. This confidence is expanded to ensure that the security solution satisfies its operational and administrative requirements. It does not impose additional security controls and ensures that those controls once deployed will function as expected. Security engineering, from the SSE-CMM viewpoint, includes an assurance process which comprises various Process Areas, namely PA11 (Validate and verify security), PA10 (Specify security needs), PA09 (Provide security input), PA07 (Coordinate security) and PA06 (Build assurance argument). The assurance argument contains both appropriate and sufficient assurance evidence to ensure that security needs and claims are supported (SSE-CMM, 2003).

There are a variety of assurance methods available including the use of best practices; design principles which ensure the inclusion of security; the use of dynamic testing and static analysis, internal and third-party review and, evaluation and vulnerability testing. The goal is to provide sufficient assurance evidence which, however, produces documentation-rich development. This is in conflict with agile development methods (Beznosov and Kruchten, 2004).

The iterative and emergent nature of agile development, together with its refactoring and test-driven environment poses challenges to security engineering. Beznosov and Kruchten (2004) in, Towards Agile Security Assurance, examine attempts to reconcile these problems and identify various remedies which include adding a part-time security engineer to the development team to assess risk, document the security architecture and build an assurance argument. Various security assurance practices in the context of agile development were examined and it was found (Beznosov and Kruchten, 2004):

- There is a high degree of inter-activity between developers and practitioners which may lead to functional development that is blind to security flaws;
- The iterative lifecycle increases the cost of third party reviews through their involvement at each interaction;
- Refactoring leads to redesign and modules can receive new functionality which is outside the security constraints;
- The agile testing philosophy tests for functionality early and routinely throughout development while the security testing philosophy focuses on testing the least-used and pathological aspects and on boundary values.

It was concluded that an accommodation is needed between the methods of security assurance and the practices of agile development to prevent creating delays, increasing costs or deterring developers who are adverse to extensive documentation (Beznosov and Kruchten, 2004).

It is important to note that not all assurance techniques are in conflict with agile development. It is in the so-called *Natural match* where agile practices fit well with security ones. These include the pair programming advocated by XP which through immediate feedback, enables the inclusion of security guidelines. There are *(semi-) automated* methods and techniques which are guided by a security-oriented philosophy and can be applied at each iteration without incurring significant overheads. Examples are penetration and vulnerability testing and static and dynamic analysis of source code. Finally, there is the Mismatch group which poses the greatest challenge and involves almost half the assurance methods. The point of conflict is their reliance on extensive documentation and high time and cost overheads. Examples are external security or formal verification activities. This group is the most important but poses the greatest challenge to integrate into agile development (Beznosov and Krutchen, 2004).

External Security Certification is important in building trust between organisations. The simplest remedy is to implement new agile-friendly assurance methods to replace the existing methods. This is as yet to be researched. A second, practical strategy suggests that assurance methods are applied at least twice during agile development. This method will instil early confidence and ensure security assurance in the final product. This compromise can still lead to agile-adverse

over-documentation. A core activity of agile security assurance is the early identification of design and system changes that may cause security problems and to apply these guidelines throughout the SDLC (Beznosov and Kruchten, 2004). This poses the problem of integrating security into the agile development methods.

5.7 An Agile Security Integration Method Using Feature Driven Development

It has become necessary, in the current, emergent environment, for developers to use agile development methods to create the needed business applications. These, however, are particularly risky environments and agile development methods possess few features that directly address security risks. This can result in agile products which lack security protection unless it is treated as an add-on. This type of solution will increase, however, the 'development duality' problem as the fundamental conflict between functionality and security (Margaritis et al, 2001, Siponen and Baskerville, 2001). Agile methods ignore security issues because it is felt they hinder development and research has proven this true of most of the existing security methods (Siponen et al, 2005). Methods are under-development to address the integration of security into agile software development and it is relevant to examine an example.

Siponen et al (2005), in Integrating Security into Agile Development Methods, elegantly discuss and illustrate how it is possible to integrate security into agile software development provided it meets several requirements. The security approach used must be adaptive to the agile development methods. It must be simple and not hinder the project. It must provide tools for and concrete evidence of all the phases of the development. Finally, the security component itself needs to be adaptable to its changing environment and capable of supporting incremental iterations. A set of key security elements are proposed to form a generic and modifiable security process which can be added seamlessly into the agile development methods (Siponen et al, 2005).

The key security elements, proposed by Siponen et al (2005), are based on both information security 'meta-notation' and database security principles. Meta-notation is discussed and illustrated through a security enriched Use case example. Siponen and Baskerville (2001) in, A new paradigm for adding security into IS development methods, note that firstly, using a meta-method level of

abstraction presents a perspective of IS design methods that are in a constant state of emergence and change. Secondly, system problem settings and developmental approaches are neither totally chaordic nor relative. Thirdly, developers recognise that patterns emerge during problem-solving and a meta-methodology needs to capture a sufficient range of these patterns to be useful. Notation systems appear regularly across methods and problem settings allowing developers to understand and model reality with respect to the system-to-be-built. Developers need an agreed-upon method to describe and understand the system under analysis. Various agile approaches use the UML notation as the unit of analysis at the organisational level. The UML Use case is adopted in meta-notation (Siponen and Baskerville, 2001).

The meta-notation contains five dimensions: security subjects, security objects, security constraints, security classifications, and security policy. The terms security subjects and objects originate from database security literature. Security subjects have a relevant security connection to the assets of the organisation and are depicted as 'Actors' in Use cases. Examples are employees and business partners. Security objects are the organisational assets that are relevant to information security. Examples range from documents to electronic files. Security constraints comprise the security concepts of confidentiality, integrity, availability and non-repudiation. It is necessary to define the type of access between the security objects and subjects, for example read or write access, therefore their security classification is important. The security policy dimension defines the other security constraints (Siponen and Baskerville, 2001).

In Figure 5.3, the author incorporates the meta-notation and the security enriched Use case as proposed by Siponen and Baskerville (2001) and Siponen et al (2005) to illustrate the agile security integration method. The Validate Client Use case example is a product of the FDD methodology and it illustrates the five meta-notation dimensions. The security subject is the User-Admin clerk who has access to the organisational security assets. The security object is the Client Account data and its security classification is Confidential as decided through the security policy. The meta-notation forms part of the key security elements integral to the proposed generic security process (Siponen et al, 2005).

USE CASE: Validate Client – *SECURITY VERSION*

VERSION: 1:0

ACTOR / SECURITY SUBJECT*: User-Admin clerk.*

SCOPE: Process Sales Order.

LEVEL:

FUNCTIONAL SUMMARY: User-Admin Clerk verifies SALES ORDER Client Account Details.

FREQUENCY: Several times a day.

SECURITY CLASSIFICATION: CONFIDENTIAL.

SECURITY OBJECTS AND SECURITY OBJECTS ACCESS TYPES: *User-Admin Clerk must have Read/write Access to Client Account data.*

SECURITY POLICY/SECURITY SPECIFIC RESTRICTIONS: *User-Admin Clerk permitted access to Security Objects classified as Confidential.*

USABILITY REQUIREMENTS: Any BPML query must be able to execute in X seconds.

User Identity/Security Subject has been authenticated.

PRECONDITIONS: SALES ORDER Document must exist.

MAIN SUCCESS SCENARIO:

User-Admin Clerk confirms Client Account validity.

ALTERNATIVES:

1.1 Client Account invalid – cancel SALES ORDER.

1.1 a Client Account invalid with a GOOD CREDIT RATING – Capture Client Account details.

1.1.b Client Account valid with POOR CREDIT RATING – Cancel SALES ORDER.

EXCEPTIONS: CASH SALES ORDER do not require CREDIT RATING Check.

Figure 5.3 - Security Enriched Use Case Example – Validate Client Use Case (Adapted from Siponen et al, 2005)

The method of integrating security into agile methods, as proposed by Siponen et al (2005), applies the five key security elements and a risk management framework to a business process during the agile software development process. The security elements, within the generic security process, are applicable to the different phases of a project lifecycle. The security-relevant objects are identified during the requirements analysis phase. The identified organisational assets are the candidate security objects. The users of the objects are identified as the candidate security subjects. The sensitivity of the security objects and which users possess authorised access is determined and the security classification is set. These elements are documented using the Use case notation.

The activities of the risk management framework occur during the project requirements analysis phase and are adapted to accommodate agile development. The security objects and subjects are identified and their security classification is assigned, and potential threats need to be identified. The use of 'abuse cases' to efficiently detail threat scenarios is recommended. The unwanted actions or risks are determined and listed in terms of abuse scenarios. The cost of the damage resulting from their occurrence is calculated together with an estimation about their likelihood. Counter-measures are selected to minimise their impact together with a cost estimate. Decisions about their economical and feasible implementation are taken. This process allows developers to analyse potential threats and recovery costs (Siponen et al, 2005).

The project design phase includes the security requirements by incorporating the security subjects, objects and security classification into the modelling notation. Risk management is applied to prioritise the security features. The implementation phase ensures the required security features are installed. The security requirements and counter-measures are implemented according to their security sensitivity, using an implementation priority list which indicates the priority of the features to be implemented. The testing Phase ensures the security features work as intended. The Use and abuse cases check that the software is satisfactory prior to hand-over to the customer. The features with a higher priority are tested first.

The method proposed by Siponen et al (2005) for integrating security into the agile software development method (using FDD), was discussed. The feasibility of this proposal leads to the use of FDD to illustrate the proposed BPSM model in Section 5.9. The BPSM model itself is first presented.

5.8 Business Process Security Maturity Model – An Overview

The BPSM model is proposed to harness the convergent themes of the pillars of this research, namely the ISO 17799 security standard and the SSE-CMM security metric within a BPM business environment. The purpose is to integrate security into the business process itself and to continually monitor and correct the security posture, maturity and performance of the security process. The BPSM model is illustrated in Figure 5.4.

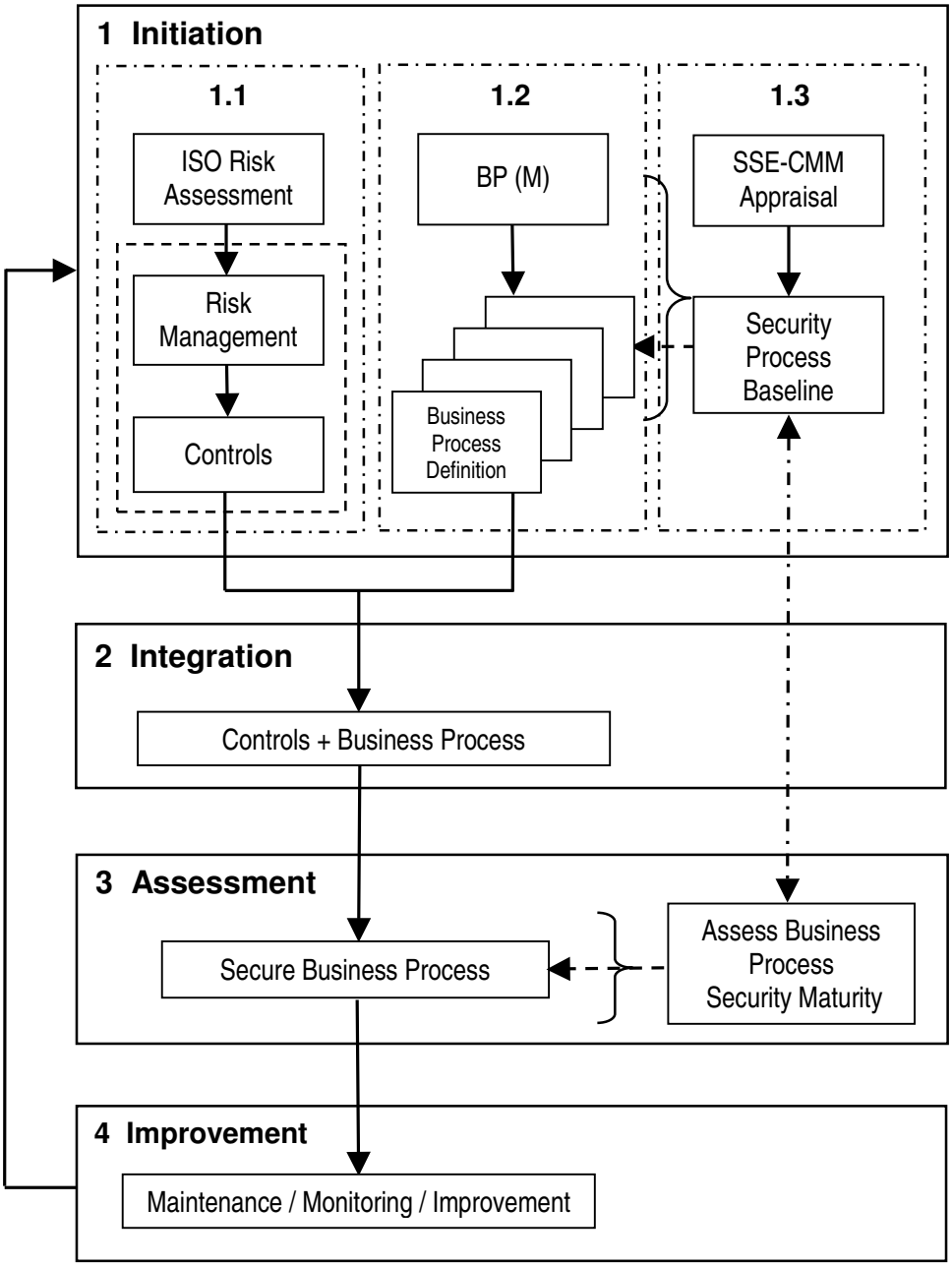


Figure 5.4 - Business Process Security Maturity Model

5.8.1 Phase 1: Initiation

It is during the Initiation Phase that the business process, which originates from a BPM environment, is initially analysed using a business process modelling technique as illustrated in Step 1.2. FDD and meta-notation are examples of agile development methods applicable to this task. The initial risk analysis and management activities are carried out to design a security plan. This security plan includes the security controls or counter-measures as illustrated in Step 1.1. The security metrics are established during this phase and are based on the security

baselines and potential maturity as determined by the ISO 17799 and the SSE-CMM. The risk assessment process institutes the security policy and determines which security controls are to be used. The ISO 17799 is used to establish the security counter-measures and is used to provide the security guidelines about which security controls to select and implement. A security appraisal is conducted using the SSE-CMM to establish the security baselines and to establish security performance or maturity targets as illustrated in Step 1.3. It is used to set up the continuous monitoring process by establishing the current and potential status of security in the business process.

The Initiation Phase creates the following deliverables; the organisational security policy, the security controls, the security baseline for the business process, the process definition together with its security elements using meta-notation, a risk treatment and risk priority plan, SoA, SoC, the assurance argument, the requisite security metrics and security goals. The result of the Initiation Phase is a security-element enhanced business process which contains its security elements.

5.8.2 Phase 2: Integration

The security controls and counter-measures are inserted into the business process during the Integration Phase and are represented as the Controls + Business Process in Figure 5.4. This results in a security-enhanced business process. FDD and meta-notation are used to document this representation. The meta-notation includes the security element dimensions, namely, the security subjects, security objects, security constraints, security classifications and security policy. The security controls originate from Step 1.1 in the Initiation Phase, namely the risk assessment activities and ISO 17799-selected counter-measures, which are assessed, using the SSE-CMM, against the current security baseline of the business process and its potential security maturity or performance. The output of this phase is a security-enhanced business process which is the input to the Assessment Phase.

5.8.3 Phase 3: Assessment

It is during the Assessment Phase that the security-enhanced business process is evaluated. It is represented as the Secure Business Process in Figure 5.4. Security metrics are applied to the Secure Business Process which is assessed

and evaluated, using the SSAM, to establish its maturity status. The goal is to achieve an optimising or Capability Level 5 maturity which ensures the security elements of the business process are continuously improving. However, the organisation utilising the BPSM model may choose to achieve a level or maturity of security that meets their desired security position. The analysis and evaluation of the Secure Business Process identifies the gaps in the performance by analysing its current status against its targeted performance. This analysis and assessment constitutes the input for the Improvement Phase.

5.8.4 Phase 4: Improvement

It is during the Improvement Phase that the improvement opportunities are identified by measuring the changes in the security performance as reported by the Assessment Phase. These security improvements are implemented to improve the security performance, strength or maturity of the Secure Business Process. This results in the Secure Business Process together with its new needs which are returned to the Initiation Phase to be re-evaluated.

These steps are analogous to the PDCA cycle and to maintaining a process in SPC. They result in the management of the security maturity posture in business processes in a continuous cycle of evaluation, assessment, improvement and re-assessment against the established and proposed security maturity status and performance.

The BPSM model provides the means to both initiate and maintain the security posture of a business process. It accommodates changes to both the business process and its security profile. Any changes to the business process originating from the BPM environment or any changes to the security profile of the business process in the form of new threats, vulnerabilities or any changes to the IT infrastructure such as the introduction of new technology for example, will result in a re-commencement of the Initiation Phase to incorporate the changes. This will produce a new business process definition which is re-evaluated by the risk analysis and management activities to establish its security needs. This affects the security plan, the counter-measures and the security policy. The ISO 7799-based security controls as counter-measures are re-selected to match the new demands of the amended security needs of the business process. Similarly the SSE-CMM

security appraisal will be repeated to establish a set of new baselines and maturity targets to meet the altered security position.

5.9 Example of Output of the BPSM Model

A theoretical example is followed through various phases of the BPSM model to illustrate its operation and a possible output. The FDD agile development approach is used to develop one of the possible features from the security enriched USE case "Validate Client" example discussed in Section 5.7 (refer to Figure 5.3). A feature represents a step in an activity within a business process. The new security enriched USE case example is illustrated in Figure 5.5 and represents the "Validate User Access to Client Account data" feature from the "Validate Client" example.

USE CASE: Validate User Access to Client Account File – ***SECURITY VERSION***

VERSION: 1:0

ACTOR / SECURITY SUBJECT: *User-Admin clerk*

SCOPE: Client Account data

FUNCTIONAL SUMMARY: User-Admin Clerk validates access to Client Account data.

FREQUENCY: Several times a day.

SECURITY CLASSIFICATION: **CONFIDENTIAL**
SECURITY OBJECT: *Client Account data*

SECURITY OBJECTS ACCESS TYPES: *User-Admin Clerk must have Read/write Access to Client Account data*

SECURITY POLICY/SECURITY SPECIFIC RESTRICTIONS: *User-Admin Clerk permitted access to Security Objects classified as Confidential.*

USABILITY REQUIREMENTS: Any BPML query must be able to execute in X seconds
User Access is authenticated.

PRECONDITIONS: Valid Password must exist.

MAIN SUCCESS SCENARIO:

1. User-Admin Clerk access is verified to Client Account File.

COUNTERMEASURES::

1.1 Encryption of passwords

1.1. Limit of number of login attempts

PRIORITY 1 – 10: *10 – must be avoided!*

Figure 5.5 - Security Enriched Use Case Example – Validate User Access to Client Account Data

The business process which originates from the BPM environment is presented to the Initiation Phase and is modelled using an agile development tool, such as

FDD. Meta-notation is used to illustrate the possible feature example in Figure 5.5 which includes the security elements. The business process definition is passed to the ISO 17799-based risk assessment process which identifies the information assets, their owners and their calculated risk profile. It provides the guidelines to manage the security requirements and guides the selection of the security controls, as counter-measures, from the ISO 17799. A SoA and SoC are created which document the objectives and selection policy of the controls, the actual controls and includes their risk mitigation strategy. These guide the ISMS by providing information about the installed security controls. The meta-notation security elements, security objects and security subjects, are identified by the risk assessment. The security policy of the ISO 17799-based ISMS designates their security classification and guides the security policy security element.

It is during the Initiation Phase that the security evaluation method, SSAM, is conducted to establish the security baselines and their security metrics. This establishes the current maturity status of the security engineering process and will establish the security performance or maturity targets. The security engineering process is interrelated to the risk and assurance processes which help build the assurance argument that provides the evidence and confidence that the security controls are relevant, satisfactory and functional. The security-element enhanced business process, as illustrated in the USE case in Figure 5.5, is the output of the Initiation Phase and constitutes the input to the Integration Phase of the BPSM model.

The security-element enhanced business process can be used by various BPMS components. These include the *Business Process Modeller* which uses the primary process design; the *Business Metrics Modeller* which relates the raw measurements to the KPI which result from the SSAM security evaluation during which the security baselines and metrics are created. The business process definition, the security policy and risk treatment plan act as inputs to a variety of *Run-Time Components*. These include the *Process Engine* which implements the business process together with the *Resource Manager;* the *Rules Engine* which represents the permissible process transaction; the *Repository* which stores the data and metadata which include the process definition, integrity rules, security and security policy definitions. The BAM monitors events and measurements to

compute the KPIs essential to managing the processes. The BPMS provides a *Security and Policy Facility* which enables a security model to ensure that the security policy is enforced.

The security controls selected from the ISO 17799 during the risk assessment and risk management tasks are inserted into the business process during the Integration Phase. This creates the security-enhanced business process.

It is during the Assessment Phase that the security-enhanced business process is evaluated and the security metrics are applied to assess and evaluate its maturity status. This identifies the gaps in performance by analysing the current maturity status against the targeted performance established in the Initiation Phase. This gap analysis is passed to the Improvement Phase.

The gap analysis is used to identify improvement opportunities during the Improvement Phase which considers the changes in security performance as reported by the Assessment Phase. The SSE-CMM provides the IDEAL tool to improve the security engineering process. Improvement opportunities are identified and the Secure Business Process together with its new needs are returned to the Initiation Phase.

5.10 Conclusion

Chapter Five presented a variety of examples of methods combining the ISO 17799 and the SSE-CMM to evaluate the maturity of security, namely the SAM assessment model of Tse (2005), the S-vector methodology proposed by Spears et al (2004) and finally, the TrustCheck approach of Tiller (2005). These ISO 17799 and SSE-CMM-based models are unanimous in their contention that both paradigms are complimentary and provide a feasible method to evaluate the capability levels of the ISO 17799 based controls. Additionally, examples of methods which evaluate the maturity of BPM were discussed. These models are different in focus but established the feasibility of evaluating the maturity of the BPM paradigm using a CMM-based model.

A means of introducing security into the agile development paradigm, using FDD and meta-notation, was presented due to the specific security and assurance challenges posed by the agile enterprise and the agile development methods. The chapter concluded by presenting the BPSM model as the proposed solution to provide mature and integrated security process within the BPM environment as a precursor to presenting an example of the output of the model.

6 - CHAPTER 6 - CONCLUSION

The three pillars of this research, the ISO 17799 security standard, the CMM and specifically, its security version, the SSE-CMM and the business paradigm, BPM, have been discussed in detail in the preceding chapters with the aim of uncovering sufficient information and evidence to determine whether these paradigms are compatible and have enough convergences to develop an integrated security model for the BPM paradigm.

This chapter concludes the dissertation by firstly revisiting the problem statement as a reminder of the motivation for the research. Secondly, an overview of the chapters in the dissertation is presented, as a precursor to showing how the aims and objectives of the research were reached. Thirdly, as a standard consideration of research, the benefits and limitations are reviewed, together with some suggestions for future research.

6.1 Revisiting the Problem Statement

Information security and security engineering have become increasingly important due to the recent and significant developments in IT together with the progressive reliance of society and the business community on information. It was noted that security is rarely treated as an integral part of an IS or IT implementation. This led to the development of the problem statement of this research in Chapter One which is as follows:

The problem that is addressed in this research can, therefore, be summarized as originating from the 'development duality' phenomenon, which implies that security is not integrated into IS design at the business process level.

The fact that security is not treated as an integral part of the BPM paradigm at the business process level is a critical issue in secure systems development. It results from the systems software and its security being separately designed and implemented (Margaritis et al, 2001, Siponen and Baskerville, 2001, White and Dhillon, 2005). This raises crucial security concerns due to the wide range of processes that are involved, including core operational, tactical, strategic, internal

and external processes. An increase in the priority of information security in systems development is required because the potential security problems may need tremendous resources to remedy. This highlights the need to focus on security as an integral part of the systems development effort. It appears, currently, however, that systems are designed based on an ideal business process, rather than the actual process in operation. Practical input from the system stakeholders appears to be largely ignored and unrealistic systems are created.

There are a variety of reasons for the development duality problem. These include:

- The requirements and design stages of SDLC are unclear about the inclusion of security features because security is not recognised as a central component by the developers. The systems development process appears dependent on the mindset of the developers who determine its goals and its design. There is a fundamental difference in orientation between general system developers and IS security developers which directly influences the handling of security issues (White and Dhillon, 2005);
- Security methods lag behind development methods (Siponen and Baskerville, 2001);
- The rapidly changing needs of organisations require that their IS reflect this almost perpetual development. This resulted in the emergent agile development methods which do not facilitate the integration of security (White and Dhillon, 2005);
- There are many separate IS development methods and many widely published, secure systems development methods but the two are not well integrated. Security integration efforts are needed to make the emergent development approaches secure at their initial implementation (White and Dhillon, 2005).

This research, based on the problem statement, set out to define a solution, namely the BPSM Model, to provide a broader, organisational approach to embedding security in IS development (specifically at business process level) and

which facilitates the maturity progression of the security processes. A number of chapters were written, to achieve this, as presented below.

6.2 Chapter Discourse

Chapter One presented the outline of the research in broad detail. The three pillars of the research; namely the BPM business paradigm, the CMM and its security version, SSE-CMM and the ISO 17799 security standard were briefly introduced. It was noted that a BPM deployment requires security to ensure its efficient and reliable operation and its particular turbulent nature presents unique security challenges. The problem statement , as developed in Chapter One, arose from a variety of realisations which include:

- Security is not treated as an integral part of BPM at the business process level;
- Technical information security approaches are limited in their effectiveness;
- A secure IS system is both reliable and trust-worthy.

These realisations identified the following needs:

- Security needs to be integrated into the business process to ensure its security;
- The security status needs evaluation to ensure it is meeting the needs of the organisation and the security posture of the business process needs to be constantly monitored, managed and improved as needed;
- A security system needs to be based on an internationally recognised standard to create confidence and business trust.

These needs and realisations highlighted the need for a cogent approach, the BPSM model, to monitor, evaluate and improve the security position within the business process to provide integrated and mature security in the BPM environment.

The aim of the BPSM model, as discussed in Chapter One, is to combine the ISO 17799 and SSE-CMM into an information security framework to initiate and evaluate the security posture within a business process. Its objective was to

produce a secure mature business process into which security is integrated. The objectives of this research were to determine that sufficient convergences exist between the pillars of this research to develop the BPSM model. This was achieved through conducting a comprehensive literature study on secondary resources collected on the three research topics or domains under investigation. The BPSM model was developed through logical argumentation to demonstrate that the converging characteristics of the three pillars provide enough cohesion and compatibility to develop a feasible solution to the research problem of the non-integration of security in a business process.

The purpose of Chapter Two was to introduce the ISO 17799 security standard. The need for information security was discussed. The advent of new IS technology has raised the eminence of security in an IT implementation. The treatment of information security as a technological issue and as an afterthought to system implementation produces unique challenges. The security domains and controls of the ISO 17799 were discussed in detail. An eight phase process to implement an ISMS based on the ISO 17799 was presented. The ISO 17799 is one of the pillars of the BPSM model and provides the necessary security controls or countermeasures and the guidance for an information security framework.

The purpose of Chapter Three was to introduce the CMM and its security version, the SSE-CMM. The history of the CMM and a detailed discussion of the SSE-CMM were presented. Security engineering was discussed as an evolving discipline that establishes a balanced set of security needs and goals. The five capability levels of the SSE-CMM and their effect on security engineering goals were examined. The SSAM appraisal method and the IDEAL tool were introduced. These tools and methods both measure and improve the security engineering capability which results in increased assurance in the resultant security system. The SSE-CMM is proposed as the security metric of the BPSM model which evaluates and identifies improvement opportunities in the security position of the business process.

The purpose of Chapter Four was to introduce the business paradigm, BPM. There was a detailed discussion of the business paradigm, BPM and the business

process, as its foundation. The relationship between BPM and the agile enterprise was examined together with a variety of agile software development methods. FDD received particular attention. BPM is the environment in which the BPSM model operates. It supplies the business process into which security is incorporated.

The purpose of Chapter Five was to motivate and ultimately, demonstrate the BPSM model. It presented examples of models which combine the ISO 17799 and the SSE-CMM to assess the maturity of the security practices and processes. The consensus of opinion was that the two approaches are compatible and complementary. Examples of models which assess Business Process (Management) maturity, from both a business process focus and an implementation focus, were examined. The Paradigm Convergence model was presented. The use of meta-notation and FDD with a security-enhanced business process were described as a solution to ensuring security assurance and to integrate security into the business process. Finally, the BPSM model was described together with an example of its output.

6.3 Revisiting the Aim and Objective of the Research

The research aim and objectives of this research were stated as follows in Chapter One:

The aim of this research is to align the concepts of the ISO 17799 security standard and the SSE-CMM framework, with the corporate methodology of BPM. The objective is to develop a Business Process Security Maturity (BPSM) model. Its goal is to provide an integrated and holistic security strategy for BPM.

The aim of the BPSM model is to combine the ISO 17799 and SSE-CMM into an information security framework to initiate and evaluate the security posture within a business process. The objectives of this research were to determine and demonstrate that the converging characteristics of the three research paradigms provide enough cohesion and compatibility to develop a feasible solution to the research problem of the non-integration of security in a business process. The

following discussion briefly demonstrates that objective has been achieved in this dissertation.

6.3.1 Aligning the concepts of the ISO 17799, SSE-CMM and BPM

It was apparent during the initial literature review that there were paradigm convergences between the three research pillars. It was initially noted that the security paradigm, ISO 17799 and its ISO 17799-based ISMS advocate the use of the Deming Wheel (Plan-Do-Check-Act cycle) to provide feedback about the security position in a continuous process of monitoring, correction and management. The goal of the CMM and its security version, the SSE-CMM, is to achieve continuous improvement which is epitomized by Maturity Level 5 (Optimising) which is exemplified by the use of CPI to facilitate quantitative feedback to achieve constant course correction. BPM focuses on improving business process efficiency to enable the business to achieve its strategic goals and provide the necessary agility or flexibility to respond to the current changing and dynamic marketplace. It advocates a culture of CPI to achieve these goals and advance process improvement and management.

There further exists a convergence between the founding principles of the three paradigms which affects their style of process management and operation. BPM is based on TQM and QM efforts which focus on business process improvement. The ISO 17799 and its ISMS use QM principles in the maintenance and management of the information security process. The CMM and its security version, the SSE-CMM, are based on TQM principles to improve process efficiency and to prioritise improvement efforts. Both TQM and QM are motivated by quality as a business driver which is relevant in the current business environment. These apparent convergences supported the development of the BPSM model based on the three paradigms.

The ISO 17799 and SSE-CMM, as components of the BPSM model, are complimentary and can be used to initiate, monitor, maintain and improve the integrated security position in the business process. Three approaches which combine the ISO 17799 and SSE-CMM were examined in Chapter Five. The ISO 17799 and SSE-CMM are compatible. There are commonalities between the

approaches and there is neither overlap nor redundancy between them (Tse, 2005, Spears et al, 2004, Tiller, 2005). The SSE-CMM administers the security controls and the ISO 17799 recommends them. Increasing maturity shifts the security focus from the security attribute to its organisational role and it becomes supportive of organisational goals (Tiller, 2005). A progression through the maturity levels improves process efficiency and quality.

Carlson (2001) and Wynes (2001) state that the ISO 17799 provides the guidelines and acts as the standards specification for an ISMS which monitors and controls the security program. The security engineering process is measured through the SSE-CMM. The ISO 17799 is used to establish the IS security program whilst the SSE-CMM assesses its maturity level which ensures an appropriate level of security (Barton et al, 2000, Spears et al, 2004, Tiller, 2005, Tse, 2005).

There is convergence between the CMM and the BPM paradigm. Rosemann and de Bruin (2005), van der Aalst et al (2003) and McGovern (2004) maintain the focus of BPM is process improvement through design, implementation and CPI. Its goal is to strategically align its business processes to its business objectives. The paradigms of CMM and SSE-CMM strive to operate at the optimising level, through CPI and using quantitative feedback, pilot testing and new technology insertion. They require processes that are defined, documented and managed which translate into resilience and responsiveness to the dynamic business environment. It is at Maturity Level 5 (Optimising), characterised by CPI, that the goals of BPM and CMM meet.

The CMM-based BP(M) Maturity models, discussed in Chapter Five, deal variously with an increase in maturity through a growth in process awareness which translates into improved process efficiency and quality. The CMM and through its security version, the SSE-CMM, can transfer this awareness and related maturity to the security practice and each maturity level indicates an increase in the effort to manage and improve security efforts (Tse, 2005). Security becomes supportive of the business objectives (Tiller, 2005). This is relevant because security must be supportive of the business objectives. It needs to react

to changes in the business process which occur because of the dynamic agile environment and result in changes to the security posture and risk profile. There exists sufficient paradigm convergences and cohesion between the three research pillars to warrant their combination into the BPSM model.

6.3.2 The Development of the Business Process Security Maturity Model

The BPSM model was proposed to address the lack of integrated security within the business process in the BPM paradigm. Its purpose is to integrate security into the business process and provide a means to continually manage the security posture, maturity and performance of the security process. The ISO 17999 and the SSE-CMM are combined to provide an information security framework to evaluate, manage and correct the integrated security position within a business process. It operates within the BPM environment which provides it with the business process. It uses the ISO 17799 to guide the selection of the security controls as counter-measures to the security needs which are assessed from the business process. The integrated security position is evaluated using the SSE-CMM to continually monitor, manage and improve it as necessary.

The BPSM Model attempts to address the problems of development duality through the use of the SSE-CMM which treats security engineering as an integral part of the entire SDLC. It combines a variety of compatible security methods into a cogent model which initiates and evaluates security within the business process. It advocates initiating security into the business process definition using the agile software development method, FDD and the meta-notation methodology. This produces the security-enhanced business process which has its security elements integrated into its design from its conception to its implementation. This Security-enhanced business process is continually re-evaluated through the BPSM model to maintain its security position. Any changes to the business process or its security posture results in its re-evaluation which accommodates the dynamic nature of the BPM environment.

6.3.3 The Provision of an Integrated and Holistic Security Strategy for Business Process Management

The literature review undertaken for this research revealed a variety of deficiencies in the integration of information security and security engineering into IS and IT infrastructures. It was realised that a BPM deployment needs integrated business process security to ensure its safe and efficient operation within its emergent and turbulent environment. There are particular security needs posed due to its dynamic nature which causes changes in both the business process and its security needs. Typical security efforts are treated as after-thoughts and as add-ons to the IS development which are problematic in the BPM paradigm due to their inflexibility and slow development. This need for integrated security was identified together with the need to base a security framework on an international standard to ensure its certification which promotes security assurance and confidence in the security controls or counter-measures selected. The need for a security program to be monitored, evaluated and corrected was identified because this maintains the currency of the security position.

The BPSM model answers these needs and identified deficiencies. It addresses the integration of security into the business process and the attendant problems of development duality. The Initiation Phase uses the agile development method FDD and meta-notation to analyse and present a business process definition which contains the necessary security elements. This ensures security is integrated into the business process from its outset. It uses the ISO 17799 as part of the information security framework to guide the selection of the security control as counter-measures. This is achieved through conducting a risk assessment and devising a risk treatment plan based on the identified needs provided by the security-element enhanced business process. It uses the SSE-CMM to appraise the current security position to establish their initial security baselines and their maturity targets. The Integration Phase combines the business process and its security controls to create the security-enhanced business process. The Assessment Phase uses the security metrics developed by the SSE-CMM and its SSAM appraisal method to measure and identify security performance gaps in the Secure Business Process. These, in turn, identify improvement opportunities the

Improvement Phase which maintain the security position of the business process as suitable to its changing business or security position needs.

The BPSM model provides a holistic and integrated security process to ensure security is incorporated into the business process to overcome the problems of development duality and to address the lack of such an appropriate and needed approach.

6.4 Benefits and Limitations of the Business Process Security Maturity Model

The BPSM model provides a variety of benefits, however, it equally has its limitations. It presents an integrated and holistic approach to integrated and mature security within a business process. It is relevant to discuss the benefits or limitations presented by each of its pillars and consider their effect when combined in the model.

6.4.1 Business Process Security Maturity Model - Benefits

The combination of the ISO 17799 security standard and the SSE-CMM security metric are seen as compatible and together they comprehensively analyse the business process to assess its security needs, select and apply the counter-measures, and evaluate and establish the security baselines which drive later improvement efforts. The overall paradigm convergences between the maturity models and BPM suggests that they are equally compatible in their operation and objectives. It is seen that each pillar of the research supports and enhances the others. This implies that the BPSM model is a feasible and workable solution.

6.4.1.1 The Currency of Business Process Security Maturity

The risk assessment process in the Initiation Phase provides the necessary cost justification for the security program. It advances management support and promotes security as an enterprise-wide activity. The SoA, as a deliverable of the risk management process, documents the security controls together with their risk treatment plan. Another deliverable is the security policy which set the guidelines for the ISMS and provides the basis for the SSAM appraisal method to create the

set of necessary security metrics. These provide the baselines against which the security posture is continually evaluated to determine its current status and identify any improvement opportunities. This is important to safeguard against the 'security slippage' problem. The two security paradigms dovetail to provide an integrated and mature security posture within a business process. Their combined use enables an organisation to establish and maintain a unique combination of Process Areas and security controls that are tailored to achieve their unique business objectives. This provides an integrated and holistic security position within a business process.

6.4.1.2 Business Process Security Maturity Focus

The BPSM model provides security with an organisational focus because it is designed into the business process from its outset. Security engineering design and maintenance are the focus of the SSE-CMM. The BPSM model, through its feedback mechanism, maintains the current security posture within the business process to ensure that it meets any changing business or security needs. It evaluates the integrated security posture of the business process, sets the target maturity status, motivates and identifies the improvement opportunities. This is important in the current, dynamic business environment. It provides evidence about the level of security assurance which creates inter and intra-business trust and confidence.

6.4.1.3 Integrated Business Process Security Maturity

The aim of the BPSM model is to instil an organisational culture of continuous improvement which is the ethos behind the BPM, the ISO 17799-based ISMS and the maturity models. Security and process awareness are inculcated into the organisation. Security goals are aligned to the business goals and security is not treated as a technological afterthought which may hamper system functionality but is integrated into the organisational IS. This can help overcome the development duality problem that exists in IT and IS development. The BPSM model uses an agile software development method, FDD and meta-notation to enable the inclusion of security factors into a rapidly evolving business process. This is seen as another method to overcome development duality.

The BPSM model uses its particular components because together they support for each other. The BPM paradigm provides a current version of the business process which is analysed and designed using FDD and represented using meta-notation. This agile method maintains the currency of the business process definition. The ISO 17799 provides the needed internationally recognised security standard which promotes security assurance and confidence in the security controls and ISMS that is implemented. The SSE-CMM is a recognised maturity model and presents the SSAM appraisal method which acts as the security metric against which the security posture and target maturity of the business process managed.

6.4.2 Business Process Security Maturity Model – Limitations

There are a variety of possible limitations that the BPSM is vulnerable to. It relies on the existence of its three pillars to operate effectively. Therefore, the limitations of its pillars are discussed together with the impact of their removal on the BPSM model.

6.4.2.1 The Effect of the Pillars of the Business Process Security Maturity Model

The BPSM model is a particular combination of two security paradigms and a business paradigm which are mutually supportive. The BPM paradigm supplies the current business process definition to the model. The ISO 17799 provides the guidance for the selection of the security controls and facilitates the formulation of the security policy which guides the ISMS. The SSE-CMM provides the necessary appraisal method, SSAM, which evaluates and sets the security measures, security baselines and security maturity targets. These are two internationally recognised security approaches which represents their industry-acceptance. The omission of one of the pillars will cause the model to be in-effective and not operate as intended. For example, the removal of the SSE-CMM pillar would prevent the progression through the maturity levels to achieve constantly improved security performance. The removal of the ISO 17799 pillar would mean that the security controls implemented cannot be certified and there will be a loss of business confidence and security assurance. The BPM paradigm is vital because it provides the business process definition.

6.4.2.2 Agile Development Method

The use of an agile development method within the BPSM Model may be problematic as minimal documentation is used. This poses difficulties for security assurance and accreditation, certification, evaluation and third party review. Agile methods use refactoring and its testing philosophy clashes with security assurance practices. The involvement of security evaluators and third parties during the iterations may be prohibitively expensive. The testing philosophy focuses on a test-driven development (TDD) which is thought to facilitate the continuous integration of changes. This early and routine functionality testing is different to security testing which uses a depth-of-test analysis (Abrahamsson et al, 2003, Nerur et al, 2005, Beznosov and Kruchten, 2004).

6.4.2.3 Adherence to Business Process Security Maturity Model

The BPSM model relies on its users to carry out all its activities thoroughly. This is seen as a limitation. The intervention of the human-element often poses the problem of compliance with a schedule of tasks. The effectiveness of an ISMS is dependent on the thoroughness of its risk analysis, risk treatment and management plans.

The BPSM model, at present, is a manual model and this poses the difficulty of maintaining all its relevant information and data in a current form which may be seen as time-consuming and over-detailed. The design and re-design of the business process is dependent on the skill of the system analysts and designers. The identification and selection of the security controls as counter-measures is equally dependent on the skill of the security professionals. The use of the SSE-CMM may help mitigate this problem because it creates the security baselines and security metrics against which security performance and status is evaluated.

6.4.2.4 Continuous Process Improvement - Maturity Approach

Another possible limitation of using a maturity model based approach is that the ability to innovate business processes can be lost due to its CPI-based culture. This culture implies that optimal operational performance is achieved through

refining the existing processes and the innovation of processes is under-represented. This is inappropriate in the current inter-connected environment where previously unfeasible business solutions are possible and process innovation is needed. It has been highlighted that there may be management resistance to the continual investment in resources that is required by a CPI approach and this is seen as a drawback.

6.4.2.5 Research Methodology

The method of research is seen as a limitation. The use of the literature survey type of qualitative research approach is seen as challenging. The BPSM model is a theoretical one at present and it will be of interest to investigate its implementation as a case study. The model is a theoretical concept, however, there are challenges to implementing it as a case study or series of action research projects due to the resources that will be needed in a practical implementation.

6.5 Future Research

The BPSM model, presented in this research, is a theoretical model and it would be of great interest to apply the model to a real-life BPM implementation. It is of equal interest to investigate whether it could be created as a generic model which will accommodate a variety of security standards (and possibly legal instruments) to provide the guidelines for the selection of security counter-measures and controls. This is of particular relevance in the current environment where the establishment of laws and standards is proliferating.

The BPSM model is, currently, a manual process and the possible semi- or total automation of a variety of its tasks is an area that needs further investigation. These include the creation of the security metrics and the subsequent evaluation of the integrated security posture within the business process.

The area of agile security assurance is a young field and needs further research to refine the possible solutions. FDD and meta-notation are used in BPSM model and further research in the area of agile development methods may affect the

operation of the model. It may become simpler to analyse, design and include the security needs in a security-element enhanced business process, for example.

This research project is concluded in this chapter. Further research directions have been discussed together with the benefits and limitations of the BPSM model.

6.6 Conclusion

The business paradigm, BPM, is the culmination of current developments in IT software and hardware. The BPM environment has a turbulent nature as organisations seek to remain competitive within a dynamic marketplace and it is characterised by the agile enterprise. This constantly changing business environment poses particular problems to the integration of security into the business process. Security engineering and information security have become significant IS issues but are, however, generally treated as an add-on to the system development and not integrated into the SDLC which causes the problem of development duality. Technological solutions are limited in their effectiveness and the absence of a security management program causes 'security slippage'.

The motivation for the BPSM model was to provide a framework to initiate, monitor, correct and improve the security posture with a business process. The ISO 17799 and the SSE-CMM comprise its information security framework. The ISO 17799 provides the means to establish an ISMS and guides the selection of the security controls using risk analysis, risk management and a risk treatment plan. The SSE-CMM presents the SSAM appraisal method together with a means to advance through its maturity levels to constantly improve the security engineering process. The agile software development method, FDD, and meta-notation are used to analyse, design and incorporate security into the business process. The BPSM model provides integrated security maturity within the business process and through its feedback mechanism continually corrects and amends its security position and accommodates changes which originate from the business process or its security posture. Information and its supporting technology are of paramount importance in the modern world which has raised the importance

of its protection. The BPSM model appears to be a promising solution to address this security need.

6.7 Additional Research Presented

The author presented a paper at the South African Institute of Computer Scientists and Information Technologist (SAICSIT) Annual Research Conference in 2004. The paper was accepted and published in the Proceedings of the SAICSIT PostGraduate Symposium.

REFERENCES

Abrahamsson, P., Warsta, J., Siponen, M.T., & Ronkainen, J. (2003). New Directions on Agile Methods: A Comparative Analysis. *Proceedings of the 25th International Conference on Software Engineering (ICSE'03) / Computer Society*, 244-25.

Bardoloi, S. (2004). Quality: A Health Capsule to Retain Growth. *Pinnacle Systems, Inc*. Retrieved November, 2004 from http://projectperfect.com/downloads/info/info_cmm.pdf

Barton, R.R,. Hery, W.J., & Liu, P., (2000). An S-vector for Web Application Security Management. *ACM*.

Baskerville, R,. & Siponen, M. (2002). An information security meta-policy for emergent organisations. *Logistics Information Management / MCB UP Limited, 15(5/6),* 337-346.

Beznosov, K., & Kruchten, P. (2004). Towards Agile Security Assurance. Proceedings of the 2004 Workshop on New Security Paradigms *ACM 2005,* 47-54.

Bhote, K.R. (1988). *World Class Quality.* New York: American Management Association.

Brewer, Dr.D, & List, W. (2004). Measuring the effectiveness of an internal control system. *Gamma Secure Systems Limited / Wm.List & Co*. Retrieved December, 2006, from http://www.gammasl.co.uk/topics/time/time040317.pdf

Carlson, T. (2001). Information Security Management: Understanding ISO 17799. *International Network Services Inc. INS Whitepaper*. Retrieved February, 2006, from http://www.netbotz.com/library/iso_17799.pdf

Chan, M.T., & Kwok, L.F. (2001). Integrating security design into the software development process for e-commerce systems. *Information Management & Computer Security / MCB University Press*. *9 (3)*, 112-122.

Chaula, J.A., Yngstrom, L., & Kowalski, S. (2004). Protection Profile and Evaluation Of Information Systems Security. *Department of Computer and systems Sciences, Stockholm University*. Retrieved February, 2006, from http://www.cs.kau.se/~simone/swits-iv/chaula.pdf

REFERENCES

Clarity Integration White Paper (2001). *Why integrate?* Retrieved June, 2005, from http://www.Clarity-integration.com

Crow, K. (2000). Capability Maturity Model. *Product Development Forum, NPD Body of Knowledge, DRM Associates*. Retrieved November, 2004, from http://www.npd_solutions.com/cmm.html

DeFeo, J.A., & Janssen, A. (2001). The economic driver for the twenty-first century: quality. *The TQM Magazine / MCB University Press 13(2),* 91-94.

Delphi Group White Paper. (2003). *A Delphi Group White Paper Featuring a Delphi Group Assessment of Business Process management.* Retrieved December, 2004 from http://www.delphigroup.com

Dhillon, G. (2005). Realising benefits of an information security program. *Virginia Commonwealth University, Richmond, Virginia, USA.* Retrieved March, 2005 from http://isy.vcu.endu/~ghillon/papers.htm

Dubray, J-J. (2001). Enough is enough. Retrieved May, 2004, from http://www.ebPML.org/enough.html

Eatock, J., Giaglis, G.M., Paul, R.J., & Serrano, A. (2000). The Implications of Information technology infrastructure capabilities for Business Process Change Success. In P. Henderson, *Editor Systems Engineering for business process Change*, Springer. Retrieved May, 2004, from http://www.brunel.ac.uk/research/assessit/sebpc1.pdf

Eloff, J. & Eloff, M. (2003). Information Security Management - a New Paradigm. *Proceedings of ACM International Conference, 2003,47.* 130-136

Eloff, M.M., & von Solms, S.H. (2000a). Information Security management: an approach to combine process certification and product evaluation. *Computers & Security 19(8).* Retrieved May, 2005, from http://www.sciencedirect.com

Ferraiolo, K., & Thompson, V. (1997). Let's be Mature About Security. Retrieved February, 2004, from http://www.sse-cmm.org/docs/mature_security.rtf

Fiedler, A.E. (2003). On the necessity of management of Information security. Retrieved March, 2005, from http://www.noweco.com/wp_iso17799.htm.

REFERENCES

Goede, R. (2003). A framework for the explicit use of specific systems thinking methodologies in data-driven decision support system development. Retrieved January, 2007 from http://upetd.up.ac.za/thesis/available/etd-05132005-080727/unrestricted/00front.pdf

Ghalimi, I., & McGovern, D. (2004).Standards and BPM. *Business Integration Journal - Business Process Management supplement*. Retrieved March, 2006, from http://www.bijonline.com

Gotterbarn, D. (2004). UML and Agile Methods: In support of Irresponsible Development. *Inroads - The SIGCSE Bulletin, 36(2),* 11-13.

Harmon, P. (2003). Six Sigma Today. *Business Process Trends Newsletter June 2003*, 1(6). Retrieved May, 2006 from http://www.bptrends.com

Harmon, P. (2004). Evaluating an Organisation's Business Process Maturity. *Business Process Trends Newsletter March 2004, 2(3).* Retrieved February, 2006, from http://www.bptrends.com

Harmon, P., & Wolf, C. (2005). CMM and BPM. *Business Process Trends Advisor 3(20*). Retrieved May, 2006, from http://www.info@bptrends.com

Hefner, R. (1997). Lessons Learned with the Systems Security Engineering Capability Maturity Model. *Proceedings of 1997 (19th) International Conference on Software Engineering.* 566-567

Highsmith, J. (2002). What is Agile Software Development. *CROSSTALK - The Journal of Defense Software Engineering.* Retrieved February, 2006, from http://www.stsc.hill.af.mil

Hollingsworth, D. (2004) The Workflow Reference Model 10 Years On. 295-312. Retrieved January, 2006, from http://www.Wfmc.org/standards/docs/tc003Vii.pdf

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Security & Computer Security, 11(5)*, 243-248

Hoepfl, M.C. (1997). Choosing qualitative research: A primer for technology education researchers, Journal of Technology Education, 9(1), 47-63.

REFERENCES

Information Security Breaches Survey 2002. *Department of Trade and Industry, UK / PriceWaterhouseCoopers*. Retrieved February, 2006, from http://www.security-survey.gov.uk

Information Security Breaches Survey 2004. *Department of Trade and Industry, UK / PriceWaterhouseCoopers*. Retrieved February, 206, from http://www.security-survey.gov.uk

ISO/IEC 17799:2000. Information Technology - Security techniques - Code of practice for information security management. ISO/IEC 2000 / http://www.iso.org

ISO/IEC 17799:2005. Information Technology - Security techniques - Code of practice for information security management. ISO/IEC 2005 / http://www.iso.org

ISO 17799-2:2003 / BS 7799-2:2002. Information security management systems - Specification with guidance for use. Standards South Africa 2003 / British Standards Publishing Ltd.

IT Governance Ltd. (2005). *ISMS & 17799 Revisions Briefing*. *IT Governance Ltd. 2005, 4*.

Kahraman, E.(2005). Evaluating IT Security Performance with quantifiable metrics. *University of Stockholm, Institutionen for Data-och Systemvetenskap.* Retrieved November, 2006, from http://dsv.su.se

Karagiannis, D. (1995). BPMS: Business Process Management Systems. *SIGOIS Bulletin*, 16(1).

Kinsley, M. (2007). Bring in the Consultants! *Time, 170(21),* 21.

Kormos, C., Givens, N., Gallagher, L.A., & Bartol, N. (1999). Using Security Metrics To Assess Risk Management Capabilities. *SSE-CMM Project Metrics.* Retrieved February, 2006, from http://www.08.nist.gov/nissc/1999/proceedings/papers/p29.pdf

Lee, R.G., & Dale, B.G. (1998). Business process management: a review and evaluation. *Business Process Management Journal / MCB University*, *4(3),* 214-225.

REFERENCES

Lester, S. (1999). *An introduction to phenomenological research.* Retrieved December, 2007, from http://www.devmts.demon.co.uk/resmethy.htm

Margaritis, C., Kolokotronis, P., Papadopoulou., P. Kanellis., & Martakos, D. (2001). A Model and Implementation Guidelines for Information Security Strategies in Web Environments. In *Advances in Information Security Management & Small Systems Security*. Eighth Annual Working Conference on Information Security Management & Small Systems Security, Las Vegas. 13-33

McGovern, D. (2004).An Introduction to BPM & BPMS. *Business Integration Journal - Business Process Management Supplement,* 2-10. Retrieved March, 2006, from http://www.bijonline.com

Miers, D. (2005). BPM: Driving Business Performance. *Enix Consulting Ltd. / Business Process Trends July 2005*. Retrieved January, 2006, from http://www.bptrends.com

Miller, M.J., Pulgar-Vidal, F., & Ferrin, D.M. (2002). Achieving Higher Levels of CMMI Maturity Using Simulation. *Proceedings of 2002 Winter Simulation Conference*

Moody, D. (2002). *Empirical Research Methods.* Retrieved January 5, 2007, from http://www.idi.ntnu.no/~ekaterip/dif8916/Empirical%20Research%20Methods%20Outline.pdf

Moreton, R., & Chester, M. (1996).*Transforming the Business - the IT contribution,* McGraw-Hill Publishers, New York

Myers, M. D. (1997). *Qualitative Research in Information Systems.* Retrieved January , 2007, from http://www.qual.auckland.ac.nz/#Introduction

Nerur, S., Mahapatra, R., & Mangalaraj, G. (2005). Challenges of Migrating to Agile Methodologies. *Communications of the ACM, 48(5)*, 73-78. Retrieved March, 2006, from http://www.acm.org

Neubauer, T., Klemen, M., & Biffl, S. (2005). Business Process-based Valuation of IT-Security, *ACM*

Olivier, M.S. (2004). *Information Technology Research. A practical guide for Computer Science and Informatics.* South Africa: Van Schaik Publishers

REFERENCES

Palmer, S.R., & Felsing, J.M. (2002). *A Practical Guide to Feature-Driven Development.* Upper Saddle River, New Jersey: Prentice-Hall Inc.

Paul, R.J., Hlupic, V., & Giaglis, G. (1998). Simulation modelling of business processes. *Proceedings of 1998 Winter Simulation Conference.* Retrieved March, 2005, from http://www.brunel.ac/uk/research/assessit/publications.html

Payne, S.C. (2006). A Guide to Security Metrics. *SANS Institute / Information Security Reading Room.* Retrieved December, 2006, from http://www.sans.org/reading_room/whitepapers/auditing/55.php

Pieterse, K. (2005). *Leaning the South African Way. Implementing lean manufacturing in the Rainbow Country* .Port Elizabeth, South Africa: Trilean Publishing

Plesums, C. (2002). Introduction to Workflow. *Workflow Handbook, 2002*. retrieved January, 2006, from http://www. Plesums.com/image/introworkflow.html

PPI Research Report. (2004). *Business Process Management in U.S. Firms Today*. Rummler-Brache Group. Retrieved March, 2006 from http://www.ppi_research_results.pdf

Pruijt, H. (2002). Repainting, modifying, smashing Taylorism. *Journal of Organisational Change Management, 13(5),* 439-451.

Pyke, J., & Whitehead, R. (2003). Does Better Math Lead to Better Business Processes? Retrieved December, 2004, from http://www/wfmc.org/standards/docs/better_maths_better_process.pdf

Rosemann, M., & de Bruin, T. (2005). Application of a Holistic Model for Determining BPM Maturity. BPTrends. Retrieved January, 2006, from http://www.bptrends.com

SEI-CMM Technical Report. Paulk, M.C., Curtis, B., Chrissis, M.B., & Weber, C.V. (1993). Capability Maturity Model for Software, version 1.1. Software Engineering Institute, Carnegie Melon University, Pittsburgh, Pennsylvania, USA

REFERENCES

Sheard, S.A., & Moini, A. (2003). Security Engineering Awareness for System Engineers. *Proceedings of 13th Annual Symposium of the International Council on Systems Engineering*.

Sinur, J., & Thompson, J. (2004). Gartner on the BPM Market. *Business Integration Journal - Business Process Management supplement*. Retrieved March, 2006, from http://www.bijonline.com

Siponen, M., & Baskerville, R. (2001). A new paradigm for adding security into IS development methods. In Advances in Information security management & small systems security. *Eighth Annual Working Conference on Information Security Management & Small Systems Security*. 99-111

Siponen, M. (2002a) Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security, 10(5)*, 210-224.

Siponen, M. (2002b). Designing secure information and software, Critical evaluation of the existing approaches and a new paradigm. *Academic Dissertation / University of Oulu, Oulu, Finland*.

Siponen, M.T. (2003). Information Security Management Standards: Problems and Solutions. *Proceedings of 7th Pacific Asia Conferenc on Information Systems.* 1550-1561

Siponen, M., Baskerville, R., & Kuivalainen, T. (2005). Integrating security into Agile Development Methods. *Proceedings of the 38th Hawaii International Conference on System Sciences – 2005.*

Smith, H., & Fingar, P. (2002). *Business Process Management – The Third Wave.* Megan-Kiffer Press, Tampa

Smith, H., & Fingar, P. (2003). *The Third Wave of Business Process Management: Digital Six Sigma*. Retrieved December, 2005, from http://www.bptrends.com

Smith, H., & Fingar, P. (2003a). *The Third Wave, Business Processes: From Reengineering to Management*. Retrieved May, 2004, from http://www.darwinmag.com/read/030103/wavehistory.html

REFERENCES

Smith, H., & Fingar, P. (2004a). The Third Wave - Process Management Maturity Models. *BPT Column July 2004.* Retrieved February, 2006, from http://www.bptrends.com

Smith, H., & Fingar, P. (2004b). The Third Wave. *A BPT Column*. Retrieved May, 2004, from http://www.bptrends.com/publicationfiles/01-04COL/thirdwavesmith-Fingar2.pdf

Spears, J., Barton, R., & Hery, W. (2004). An Analysis of how ISO17799 and SSE-CMM Relate to the S-vector Methodology. *The Penn State ebusiness Research Center / SMEAL College of Business Administration.* Retrieved February, 2006, from http://www.ebrc.psu.edu

SSE-CMM Model Description Document. Abzug, C., Adams, J., Aldrich, M., Bacoyanis, G., Barret, C., Bartol, N., et al. (2003 / 1997). *Systems Security Engineering Capability Maturity Model - SSE-CMM Model Description Document version 3.0.* Pittsburgh, Pennsylvania, USA. Software Engineering Institute, Carnegie Melon University.

Theobald, J. (2003). *The Road to BS7799 Accreditation and using ISO 17799 as an Information Security Framework*. Retrieved June, 2005, from http://www.I-defense.co.uk

Thompson, J. (2003). What is Taylorism? *Management for Productivity*. Retrieved May, 2004, from http://instruct1.cit.cornell.edu/courses/dea453_653/ideabook1/thompson_jones/taylorism.html

Tiller, J.S. (2005). Measuring the Maturity of Your Security Program. *SITA-INS Whitepaper / International Network Services Inc.* Retrieved January, 2006, from http://www.sita.aero

Tse, D.W.K. (2005). Security in Modern Business: Security Assessmentmodel for Information Security Practices. Department of Information Systems, City University of Hong Kong, 1506-1519. retrieved January, 2007, from http://www.iswktse@cityu.edu.hk

REFERENCES

Turner, R., & Boehm, B. (2003). People Factors in Software Management Lessons from Comparing Agile and Plan-driven methods. *CROSSTALK, The journal of Defence Software Engineering.* Retrieved February, 2006, from http://www.stsc.hill.af.mil

van der Aalst, W.M.P., ter Hofstede, A.H.M., & Weske, M. (2003). Business Process Management: A Survey. Springer-verlag, Berlin, 1-12. Retrieved December, 2005, from http://www.is.tm.tue.nl/staff/wvdaalst/publications/p183.pdf

von Solms, S.H. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*, 99-104.

von Solms, S.H., & Eloff, J.H.P. (2001). Information Security Development Trends. Retrieved January, 2006, from http://cs.unisa.ac.za/technicalReports/unisa-tr-2001-20.pdf

von Solms, S.H., & von Solms, R. (2007). *Information Security Governance (Draft).* 50-52

White, E.F.R., & Dhillon, G. (2005). Synthesizing Information Systems Design Ideals to Overcome Development Duality in Securing Information Systems. *Proceedings of the 38th Hawaii International Conference on System Sciences – 2005*.

Williams, J.R., & Ferraiolo, K.M. (1999). P_3I - Protection Profile Process Improvement. *Arca Systems, Inc*. Retrieved February, 2006, from http://www.sse-cmm.org/lib/lib.asp

Workflow Management Coalition. (1998). *Workflow Reference Model / TC00-1003 Issue 1*. Retrieved January, 2006, from http://www.wfmc.org/standards

Workflow Management Coalition Glossary (2005). Retrieved January, 2006, from http://www.wfmc.org

Wynes, J. (2001). Entirety Services - Information Security Management Standard ISO 17799 / BS 7799. *Total Network Solutions Ltd, Whitepaper.* Retrieved March, 2005, from http://www.entiretyservcies.com

Business Process Security Maturity – A Paradigm Convergence

The standardisation of practices and processes to ensure the design, implementation and management of effective, organizational Information Security (infra-) structures and secure Information Systems are gaining widespread acceptance. Prominent examples are the ISO17799, GASSP/GAISP and the NIST Handbook. These methods fall into the characteristic checklist/standard category of security implementation and typically have a holistic approach to Information Security and its management. The SSE-CMM, conversely, attempts to measure the maturity of the Systems Security Engineering processes implemented by an organisation. The fundamental premise is that a more mature process will yield a better-quality outcome.
The goal, in this research, is to align the security paradigms of the ISO17799 and the SSE-CMM with the process management paradigm of Business Process Management (BPM). The objective is to provide a mature security strategy for BPM ensuring the convergence of Information Security and its management at the business process level.

Keywords: Business Process Management, ISO17799, Capability Maturity Model, SSE-CMM, Continuous Process Improvement

Debra Box (Lead Author)
Department of Applied Informatics, Port Elizabeth Technikon, Private Bag X6011, Port Elizabeth, 6000, South Africa,
debbie.box@webmail.co.za

Dalenca Pottas
Department of Applied Informatics, Port Elizabeth Technikon, Private Bag X6011, Port Elizabeth, 6000, South Africa,
dalenca@petech.ac.za

Postgraduate Symposium Submission

Business Process Security Maturity – A Paradigm Convergence

The standardisation of practices and processes to ensure the design, implementation and management of effective, organizational Information Security (infra-) structures and secure Information Systems are gaining widespread acceptance. Prominent examples are the ISO17799, GASSP/GAISP and the NIST Handbook. These methods fall into the characteristic checklist/standard category of security implementation and typically have a holistic approach to Information Security and its management. The SSE-CMM, conversely, attempts to measure the maturity of the Systems Security Engineering processes implemented by an organisation. The fundamental premise is that a more mature process will yield a better-quality outcome.
The goal, in this research, is to align the security paradigms of the ISO17799 and the SSE-CMM with the process management paradigm of Business Process Management (BPM). The objective is to provide a mature security strategy for BPM ensuring the convergence of Information Security and its management at the business process level.

Keywords: Business Process Management, ISO17799, Capability Maturity Model, SSE-CMM, Continuous Process Improvement

4.4 INTRODUCTION

The current trend of sustained and unpredictable change in the business world is envisaged to continue. The ingredients – namely marketplace changes, tailored products and services, changing social and demographic patterns – are present [Moreton & Chester, 1997:4]. Globalisation with its attendant effects has necessitated organisations reviewing the way they operate [Smith & Fingar, 2002:9]. Information Technology (IT) is perceived as the potentially the most pervasive enabler in these business transformations, evolving information from functional silos to shared data models culminating in the paradigm Business Process Management (BPM). A BPM implementation can be considered a technological panacea for dealing with business process integration but it represents an incomplete solution without the necessary policies,

procedures, standards and controls that effectively establishes it as a *secured* business process management installation.
It is generally accepted that security should be applied in an integrated approach, for example, in Information Systems development. This has proved to be a noble thought though as historically security is applied as an exception to the rule in an IT implementation and treated as an afterthought. This motivated the concept of formulating a model of integrating security inherently within the paradigm of BPM. The overarching requirements of such a framework will be to align the overall organizational security initiatives and ensure continuous improvement through constant evaluation and adaptation of the security processes. These requirements are achievable through aligning the process management methodology of BPM, with the security paradigms of the ISO17799 and the SSE-CMM. These contend the three pillars of such a framework and will be discussed in the following sections.

4.5 THE THREE PILLARS OF A SECURE BPM SOLUTION

5.1 Business Process Management

Business Processes were initially defined by Frederick Taylor in the 1920's. They are a dynamically coordinated set of collaborative and transactional activities that deliver value to clients and are characterised as being large and complex, automated where possible, market responsive and often discrete [Smith & Fingar, 2002:47].

Business Process Management has a variety of predecessors. Automated Enterprise Resource Planning (ERP) systems with the addition of document-centered workflow structures still provided little management control over the processes. Process management is an activity most companies perform. It became more important after the advent of Business Process Re-engineering (BPR) whose foundation is Quality Management (QM) with the effectiveness of business process improvement as its focus. BPM is the latest shift in this process management paradigm.

Business Process Management creates a single definition of the business process. This Process Definition presents the appropriate views to different role players and from which new Information Systems can be built [Smith & Fingar, 2003:13]. There are various BPM vendors who incorporate workflow technology, activity monitoring and integrations tools [Computer Business Review, 2003:Online]. The essential elements of a BPM system are, by general consensus, graphical tools; a runtime execution engine; agility features for process amendment and tools for monitoring and managing the process flows and for post-completion analysis [Gartner, 2003:Online].

A BPM deployment aids businesses in facing two distinct but related pressures; the need to eliminate unproductive costs through improved efficiency and the need to provide flexible processes that are responsive to changing markets and client requirements. These are met through the capacity of BPM to advance Continuous Process Improvement (CPI) efforts.

5.2 ISO17799 Security Standard

The information of an organisation comprises its past experience and its potential future. It is a critical success factor and needs protection. Any threats to it or its mediating procedures are risks to the effectiveness and existence of the enterprise [Fiedler, 2003:Online]. Information Security is the consequence of responding to these hazards.

The British Standards Institution implemented, in 1995, the British Standard, the BS7799, which provides recommendations for the design of an Information Security Management System (ISMS). The standard was internationally accepted as the ISO17799 [Fiedler, 2003:Online].
The ISO17799 encompasses security standards for IT installations. It is a vital tool in identifying corporate structural weaknesses and endeavours to expose information vulnerabilities, regardless of their level, form or handling method. It provides the guidelines for establishing security requirements, security risk assessment and security control selection. It is broad-based and not merely a technological approach. It addresses various topics, such as Process Control; Business Continuity and Compliance, in terms of policies and good practices.

Information Security is not usually a priority in an IT installation. The QM principles of the Deming Wheel (Plan-Do-Check-Act) are applicable in an ISMS. The initial Planning step requires carrying out a security audit and confronting it with the security requirements to identify vulnerabilities. These are derived from a risks analysis and legal and contractual requirements [Fielder, 2003:Online]. This vulnerability identification furthers Security Policy development. The Security Policy is an integral part of the ISMS defining its strategy, objectives and responsibilities. The commitment of an ISMS to an international standard like the ISO17799 promotes trust, confidences and credibility in its tenets [Fiedler, 2003:Online].

5.3 Capability Maturity Model

The Capability Maturity Model (CMM) was developed by the Carnegie-Mellon university in 1986 following decades of dissatisfaction with the productivity and quality gained from IT deployments. It was realised that the fundamental problem was the inability to manage the software process. Projects are late and over-budget [Paulk et al, 1993:1]. Quality is deemed as important and an aid to cost-reduction and competitiveness. CMM provides organisations with the guidance to gain control over the processes that support their Information Systems and enhance their maturity through improving their quality [Bardoloi, 2003:Online].

2.3.1 Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM describes the characteristics of the security engineering process to ensure high-quality security engineering development. It portrays general industry practices. It covers as a standard metric - the system life cycle; entire organisation; concurrent activities with other disciplines and interactions with other organisations [Aldrich et al, 1997:1-5]. The SSE-CMM intends for security to become an integral part of the engineering efforts of an ISMS and IT infrastructure. Security engineering is manifestly defined, controlled and administered and thus effective [Aldrich et al, 1997:2-2]. An SSE-CMM provides the benefits of continuously improving overall security performance and the core competencies of the ISMS.

4.6 A PARADIGM CONVERGENCE

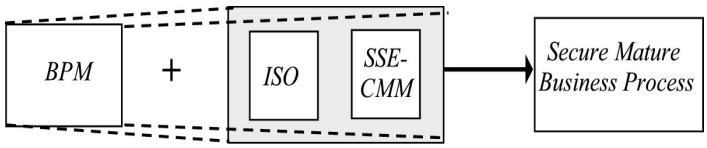


Figure 1. *Paradigm convergence*

A secure, mature business process, as illustrated in Figure 1, is a function of an Information Security Management framework (i.e. ISO17799) and a security metric (i.e. SSE-CMM), superimposed on the business methodology of BPM. The objective of this research is, therefore, to uncover the converging characteristics of the three paradigms to create a Business Process Security Maturity (BPSM) model. Security is not treated as an integral part of BPM at the process level. The development of the BPSM model will address this omission. An extensive literature study will be conducted, followed by critical arguments towards a possible solution. This will be followed by the definition of the BPSM model, motivated and based on sound analysis.

4.7 ACKNOWLEDGEMENTS

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily attributed to the NRF.

4.8 REFERENCES

ALDRICH, M. BACOYANIS,G. CAMPBELL, C. CASIMIR, M. CHILDERS, S. CRAFT ET AL. (1997). *Systems Security Engineering – Capability Maturity Model Description. Version 1.1.* Carnegie-Mellon University, Pennsylvania

BARDOLOI, S. (2003) . *Quality: A Health Capsule to Retail Growth.* Retrieved February, 2004, from http://www.pinnacle-sys.com/pdf/final.

FIEDLER, A.E. (2003). *On the necessity of management of information security. The ISO17799 as international basis.* Retrieved December, 2003, from http://www.noweco.com/wp_iso17799e.htm.

MORETON, R & CHESTER, M. (1997). *Transforming the Business: the IT contribution*. Cambridge: McGraw-Hill

PAULK, M.C, CURTIS, B, CHRISSIS, M,B & WEBER,C,B. (1993). *Capability Maturity Model for Software, Version 1.1.* Carnegie-Mellon University, Pennsylvania

SMITH, H & FINGAR, P. (2002). *Business Process Management, the third wave.* Florida : Meghan-Kiffer Press

SINUR, J & THOMPSON, J. (2003). *Ultimus Advantage, The Essential Elements of a Complete BPM System.* Retrieved January, 2004, from http://www. mediaproducts.gartner.com

METASTORM, INC (2002). The case for Business Process Management: Driving Efficiency and Competitive Advantage. Retrieved August 2003 from http://www. Metastorm.com