Fall 2009

Creation and Implementation of an It Governance Compliant It Asset Management Framework for Wexford County Council

Alan O'Rourke
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Creation and Implementation of an IT Governance compliant IT Asset Management Framework for Wexford County Council

By

Alan O'Rourke

alan_o_rourke@yahoo.com

A Thesis/Practicum Report submitted in partial fulfilment of the requirements for the Degree of Master of Science in Software and Information Systems.

School of Computer and Information Sciences
College for Professional Studies
Regis University
Denver, Colorado

Date: 28th August 2009.

Abstract

IT Governance has evolved from Corporate Governance over time as a means to enforce security and control over information systems and put in place best practices for organisations. There are accredited standards, such as ISO, CobiT, and Information Technology Infrastructure Library (ITIL) to help organisations create, and conform to best practices for information technology security. Currently there is very little IT asset governance specific literature. This study was conducted to research best practices for IT asset management, and proposes a set of guidelines for Wexford County Council to implement for IT asset management. This study also proposes how to physically implement best practices using Microsoft System Center Configuration Manager; and how steps can be taken using the asset governance recommendations to benefit the areas of IT budgeting, risk management and security.

Acknowledgements

I would first like to acknowledge my advisors in MSc SIS, particularly my thesis advisor, Ernest Eugster, who offered all of his expertise in putting the study together. I would also like to acknowledge my colleagues in Wexford County Council IT Section, in particular Michael Redmond, Peter O'Connor and PJ Murphy who helped me all they could with the study and throughout the MScSIS syllabus. I would also like to acknowledge Jim Connolly and Neil McCleane, LGCSB, who provided invaluable advice and expertise when setting up the system. On a personal note, I would like to acknowledge my wife Fiona and my parents, Denis & Sheila, for all their support throughout the course.

TABLE OF CONTENTS

List of Figures

List of Tables

Chapter 1 Background and Assessment of Problem Domain

Wexford County Council is a local government authority providing services for the 131,000+ citizens (Irish Central Statistics Office, 2006) and any visitors to the county. The organisation is the primary local authority for the Wexford County area and is responsible not only for the upkeep and provision of infrastructure in the area but also for providing a diverse variety of public services of the same quality expected from current standards of living (Wexford County Council, 2004). As with the trend for all Irish government organisations, the sector has been in continuous flux with services offered (Friedrichs & Jung, 2007) and how they are delivered over time leading to more and more significant reliance on IT infrastructure. IT solutions for all facets of service within Wexford County Council are always high on priority lists. As well as expanding and developing a more robust networking infrastructure, the organisation has been heavily involved in developing many online services for the public to avail of such as online payment services, planning applications and enquiries, motor taxation enquiries and payments, and sanitary services applications and payments to name a few (Wexford County Council, 2004). The goal has been to deliver better and more competitive services to citizens of the county through investment in IT.

This investment has brought many challenges to information security within the organisation, and there are many best practice procedures and policies employed within the organisation but as of yet there exists no specific IT asset management policy. Plant and machinery and fixed assets are included in the financial accounting service budget but no specific provision as of yet exists for IT specific assets. The corporate procurement plan (Wexford County Council, 2008) and communications policy (Wexford County Council, 2004) are both in place to support the provision of services through IT. These alone have not been deemed sufficient for securing the organisations IT assets now and the management team has been examining other methods to enforce a set of best practices and internationally recognised standards such as those developed through IT governance (ITG). To retain a competitive edge, keep up to date with current information systems practices and comply with ever expanding international and local regulations, the organisation requires a complete overhaul of how the IT assets are managed.

Risk management is performed on individual projects developed in the PRINCE2 methodology (OGC, 2009) but instead of the current risk assessment methodology of managing risks associated with single applications and their underlying assets, it was proposed to asses how each IT asset affects services offered by the organisation (Bustard et al, 2000), (Britton & Bye, 2004 p. 228), given the greater emphasis on the provision of services within the organisation.

1.1 The Problem:

The current state of Information and Communications Technology (ICT) asset management in Wexford County Council is unsatisfactory. It is difficult to trace how many computers and other equipment is in each organisational unit at a given time. No standard asset naming exists. Some assets are given a number in the next automated sequence in the existing database, while others have been named by year of purchase then section name creating inconsistency and data replication.

In addition, there are broken sequences for tracing the life cycle of assets; equipment has disappeared from the organisation, and older or obsolete equipment has been disposed of without noting reasons or date of disposal within the asset records. Furthermore, software licenses are not tracked, rising the potential for significant fines from software publishers. The Finance Department manages all the County's assets including plant & machinery. The poor current state of ICT asset management was acknowledged in an audit in spring 2008. Fixing the problems is now high priority for management.

1.2 Existing Process for Data Collection on Assets:

The existing method for asset data collection involved physically calling to each office and recording serial numbers, product types, associated users, section, location MAC addresses if necessary and other information, all of which is detailed in Appendix A for reference. This was time consuming and left a high margin for error. The process did not identify all areas of IT infrastructure and omitted important details on servers, network devices and devices like UPS batteries which should be inventoried for effective risk management. A Microsoft Access database was the

receptacle for this information and the database was not designed for such a large quantity of data which was another driving factor in the need for a new system and method. The database was incorrectly updated regularly and there were often multiple entries for the same hardware. Accountability or ownership could not be correctly assigned for each asset using this method of management. Licensing for operating systems and software suites is impossible to quantify correctly in this situation which could lead to over-subscribing for products or under-subscribing for products and risking litigation cases.

Being a government local authority, the way asset management within the organisation takes place is slightly different to private organisations and enterprises. Firstly there is a national framework for financial asset management which governs each local authority in Ireland, and the Irish Government enforces legislation regarding the audit of assets through an internal auditor assigned to each public body; as enforced by a subsection of the Local Government Act 2001 (Irish Department of Environment, 2001). There are annual reviews of the internal audit codes of practice and activities carried out during each financial year (Irish Department of Environment, 2000) which then dictates the level of responsibility and control that an IT Section and its associated organisation should assign to asset management.

This problem can be resolved by developing and implementing an ISO 27002 and ITG compliant Asset Management framework. The framework will allow accurate management and quantification of expected life cycles as new IT assets are introduced as well as ongoing tracking of existing assets utilising the framework. In addition to hardware, software is an ICT asset. Licence key management for this software requires implementation, along with defining the physical storage location of the software.

A long term objective of devising this framework is the ability for the administrator to search the container for the oldest number of each type of equipment category in a list by age. How this can be accomplished is demonstrated in 6.3.2. From this list by age report the administrator should be able to derive what equipment requires replacement and the priority level of replacement. IT assets are budgeted for in the annual financial statement and the number of these can be assessed against the asset intelligent reports

from the data container to pick the equipment to replace. This research uses the ISO 27002:2007 framework along with other IT governance techniques to identify and align organizational goals, objectives and measures; to gather asset management data and to measure and demonstrate the value-added contribution of asset management.

Under the IT Governance project initiated between several councils and Espion Consultants, this problem can be resolved by developing and implementing an ISO 27001 compliant Asset Management framework. The framework will allow accurate management and quantification of expected life cycles as new IT assets are introduced as well as ongoing tracking of existing assets utilising the framework. In addition to hardware, software is an ICT asset. Licence key management for this software requires implementation, along with defining the physical storage location of the software. A long term objective of devising this framework is the ability for the administrator to search the container for the oldest number of each type of equipment category in a list by age. From this list by age report the administrator should be able to derive what equipment requires replacement and the priority level of replacement. IT assets are budgeted for in the annual financial statement and the number of these can be assessed against the asset intelligent reports from the data container to pick the equipment to replace.

This researcher will use the ISO 27002:2007 framework to identify and align organizational goals, objectives and measures; to gather asset management data and to measure and demonstrate the value-added contribution of asset management.

1.3 Motivating Factors:

There are a number of issues driving a need for assessment of the problem domain from the perspective of finance and IT management, these are:

- Because of the greater reliance on data, there's a greater need for security at varying levels and on many functions within the IT Section and following on from this, within the organisation.

- Equipment if lost or stolen can damage the organisation's reputation, particularly so if valuable or sensitive data is stored on any equipment that is taken off site

- Increased reliance on communications and the internet for day to day business activities, and an increased reliance on e-commerce increase exponentially the potential for unlawful attack on the network

- The existing register for recording the assets within the domain was out of date in parts, and disposed items were not recorded correctly. Data replication was discovered on audit, and there are instances where equipment was not recorded and as a result not included in the IT assets register which forms part of the fixed assets register once the value of the item is >€5000. Such occurrences were rare but the new method of assessing assets will introduce a more efficient and more accurate method for managing the assets. The reporting features once in place will benefit the areas of budgeting and financial accounting as well as aiding the maintaining of high levels of security to comply with ISO/IEC 27002.

Chapter 2 Primary Research

The project scope as outlined in thesis statement was to follow the path of research within three sections:

- Section 1 was dedicated to research of the Information Technology Governance concepts and technical frameworks and the BS ISO/IEC 17799:2005 which is now to be referred to as ISO/IEC:2007 27002 standard. Governance frameworks considered for this thesis are Control Objectives for information and related technology (COBIT), the Information Technology Infrastructure Library (ITIL), and the entire area of corporate governance which is the parent node in the IT Governance hierarchy. Before implementing an ISO 27002 compliant asset management framework, one must understand the key concepts and requirements of such a project along with assigning due consideration to the significance of previous studies and successful implementations of such a project.

- Section 2 involves research of the practical implementation or physical products that will provide the backbone of such a framework, namely Microsoft SQL Server 2005 in conjunction with Microsoft System Center Configuration Manager 2007. These systems are designed to facilitate an IT Governance project, particularly the area of asset management. The SQL Server 2005 database will host all of the information in tables and the front end application is hosted on a dedicated server set out for System Center Configuration Manager 2007.

- Finally, the completion of research is signified by the results compilation of interviewing members of Internal Audit department within Wexford County Council to ascertain what key areas are of concern with regard to asset management. The experience and past knowledge of the staff will prove invaluable to an IT Governance project for asset management, as both the

finance department and the IT department can liaise on creating a framework that will benefit the entire organisation

2.2 Scope of Project:

- Research the concept of IT Governance and the structured documents available from Control Objectives for Information and related Technology (COBIT) and Information Technology Infrastructure Library (ITIL)

- Follow the asset management guidelines outlined by literature review to identify how IT asset management can add value to the business and save money

- Research the ISO/IEC 27002:2007 Framework, and outline Asset Management Criteria

- Research the SQL server architecture in conjunction with Microsoft System Center Configuration Manager

- Create a SQL 2005 database in conjunction with Microsoft System Center Configuration Manager that holds records of all hardware on the domain

- Check expected life cycle of equipment within the domain, by obtaining list of all permutations and supported operating systems, then devising formulas for measuring average expected life cycle

The research will take place in phases:

Phase 1 involves studying documentation from the IT Governance field and the ISO standards to predict potential barriers. The guidelines for a successful project can be devised from the early literature and documentation studies, along with the conclusions drawn from liaising with Internal Audit Department to define required data from auditing perspective. A final checklist of criteria devised from IT Asset Management guidelines with the ISO/IEC 27002:2007 standard will be developed.

The second phase of research will involve researching the Microsoft Systems Center Configuration Manager (SCCM) which is the software or physical implementation of the framework. Asset management can be conducted through a SQL Server 2005 container in conjunction with this SCCM. The framework will include criteria or details required about each device type. To install and configure the database, information from the Local Government Computer Services Board of Ireland outlining what will be needed to implement the database and software will be obtained. It is proposed to install the software on two DELL Blade servers, one dedicated SQL Server 2005 database server and the other a dedicated SCCM 2007 server. These servers have already been passed as suitable from the Microsoft Hardware Compatibility List and the servers will run on Windows Server 2003 operating systems. The domain within the organisation is a Microsoft Windows domain. The researcher has completed a training course in the SQL server 2005 technology to build the necessary skill set required for managing and maintaining the asset management system. The vendors of each different device type will be consulted to ascertain expected life cycle. Variables in this can affect the life cycle, these will all need to be listed and addressed. Factoring in of these variables will be necessary for correct calculation.

2.3 Primary Research (a)

Annotated Bibliography for IT Governance

Betz, C. (2007). ***Architecture and Patterns for IT Service Management, Resource Planning, and Governance: Making Shoes for the Cobbler's Children*****. USA: Morgan Kaufmann Publishing.**

The author describes how IT Governance needs to be adopted worldwide to address challenges within the IT sector, and first does this by outlining the achievements of IT to date along with describing the problems facing the IT sector – the fact that a lot of organisations view the IT budget as a potential money-pit. In the book the author also asserts that the people who are responsible for managing data processes and how they map to business processes are generally not doing so in a reliable fashion. The author addresses how organisational IT staff can dispel the myths surrounding IT and put in place solid frameworks according to international accreditation that will increase the value of IT to the business. The author asserts that a lot of the problems within the IT sector and organisations begin with project failure, system outages, poor planning and excess expense incurred by overrunning operations and projects, and to address these the concepts of ITG along with corporate governance are utilised to bring in a strategy that benefits the organisation at large through IT. The author describes the origins of frameworks such as COBIT, CMM, and discusses each in detail. The author also provides research links to the creation team behind each different framework. In the process the author provides a critique of the features within these frameworks, concentrating on CMM. This critique is then used to describe how the individual frameworks contribute to the overall value chain of the organisation.

This particular book examines the ITG frameworks in an objective, critical way which will be of great benefit when the process of designing the asset management framework begins; the book encourages the student to think about and analyse the process chain of the organisation, the process chain within the IT Section, and the process chain involved in asset management. The questions prompted by this book all

encourage study of how assets actually add value to the business and what can be done to maximise this.

Calder, A. (2008). ***Corporate Governance: A Practical Guide to the Legal Frameworks and International Codes of Practice.*** **London UK: Kogan Page.**

The author discusses the topic of corporate governance and the frameworks involved and legal requirements of corporate governance. The author first identifies the areas of concern within this discipline and provides a discussion on all of the components, history of corporations and then discussing corporate governance within the EU, United States and the UK. The concept of corporate governance is the parent of many sub-categories of governance, and more importantly for the purpose of an IT asset management thesis, the subject of IT governance is covered over a section of this textbook. The author defines ITG, and defines how each different department in an organisation is involved and has responsibility to conform to the ITG strategy. The author describes how the ITG strategy can prove expensive to implement and involve a lot of labour but is eventually responsible for keeping a competitive edge on an organisation within the marketplace, and the areas of enterprise, and IT risk management are discussed which tie in with an ITG compliant method for managing IT assets. The text also contains many government act references and corporate papers issued by international governing bodies and government departments which are useful resources to refer to when discussing ITG.

As a concept the area of corporate governance should be understood for the purposes of the thesis, as it underpins the design of the framework for asset management. The area of ITG is described in detail in this textbook and can be referred to also as a store of references for applicable legislation with regard to the asset management framework. The author spends considerable time describing the IT Audit process and the audit process in an organisation in general. These audit standards are already in place in the organisation concerned with the thesis but the IT Audit description is highly applicable to the thesis as the criteria of an IT Audit need to be fulfilled in order for the project to be considered a success.

Calder, A, & Watkins, S. (2008). ***IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002, 4ed.*** **London, UK: Kogan Page.**

The authors, both experts in management system standardisation offer a management text for complying with data security requirements in ISO 27001, and the most recent revision, ISO 27002:2007. The authors begin the book by examining the legal requirements and statutory obligations to corporations with regard to governance in the broad sense and then include several examples of reports published by the UK government which were used to develop the governance framework. The authors then describe how IT governance evolved from this and offer advice to managers as to how standard compliance can be achieved. There are many resources external from the book referred to in the text for more information on certification of compliance. As well as advising the reader of these resources, the authors also describe each component of the framework in detail and then break down the subsections individually. For this reason, the text will be a valuable reference in the creation of an ISO 27002:2007 compliant asset management system – the Chapter on Asset management describes all of the concepts required for creating this thesis project and there are areas such as "ownership" that can be neglected in an organisation; the authors describe the legal implications and features of ownership. The asset management compliance is described in all facets and is far more detailed than the framework itself in the description of parameters such as acceptable usage of assets, ownership as already mentioned, and how to correctly classify each different asset and identify its value to the organisation.

This text book sets out exactly what the purpose of IT asset management in an organisation and will be referred to constantly during the course of the thesis. The text breaks down each item in asset management into a manageable individual unit which gives an almost sequential quality to the development of the asset management framework. Another key area within the scope of the thesis is the area of information as an asset in its own right, and how to cope with sharing of confidential information with a contractor or trusted partner, exclusive rules and regulations will need to be formulated and the legal implications and rules are all discussed in the text.

Cater-Steel, A. (2009). ***Information Technology Governance and Service Management: Frameworks and Adaptations.*** **USA: IGI Publishing.**

The author has compiled a set of IT Governance (ITG) literature mainly from organisations within Australia which outlines how IT governance is being implemented within enterprises, what research is being conducted currently in ITG; and a close examination of the mechanisms used within ITG such as the COBIT framework and the ITIL framework and how they function. The author dedicates much of the text (an entire section of the book) to real implementations and case studies of ITG projects in action, and all of these are related to the reader. The author also provides an extensive review of current literature available on each individual discipline within ITG and there are online resources included in the text to expand the reader's knowledge base on completion of a section. All of the key concepts of ITG are given careful consideration and described in detail along with the origins and designers of each framework used by ITG. The author concludes each section with an examination of trends for the future and assesses the credibility and significance of each project discussed within the text.

Section 2 Chapter 5 will prove to be of particular relevance for an asset management thesis, because it is dedicated to a real implementation from Australia of tailoring the COBIT framework to suit the needs of a Public Sector IT Audit, which could mirror many facets of the student's implementation of asset management. This case study will prove a valuable guide along with enabling the student to flag potential troublesome areas in advance. An area addressed within this case study flags how the organisation intends to protect the assets, known in COBIT as Section DS12 Manage Facilities – this corresponds to the Physical Security section in ISO/IEC 27002:2007. The public sectors in Australia and Ireland differ in culture and organisational structure, but this textbook will prove to be very valuable to the student.

Galusha, C. (2001). ***Getting Started with IT Asset Management.*** **IEEE IT Pro Magazine, May | June 2001, 37 – 40. USA: IEEE Computing Society.**

The author describes how in the modern organisation IT staff need to be familiar not only with the technologies and hardware within, but the financial aspects of the equipment also, including service contracts. The author defines what asset management equates to in an organisation, and how IT assets are comprised, from each different category to declare a value to each. The author defines a set of competencies that each organisation must display toward IT assets nowadays – helpdesk, deployment of assets, and managing the ownership of data. The third category is to introduce accountability for auditing of data and associated technologies. The author demonstrates how education of staff and users leads to effective management. This principle will be useful to employ within the thesis situation, the framework derived from the thesis and end product data store of assets will be directly linked to the helpdesk software and integrated to make asset to user tracking more efficient. Finally the author has demonstrated tools in the article that are useful for management of IT assets in different guises, these are quite dated now and the architecture of Microsoft System Center Configuration Manager has already been chosen for the thesis, however the principle ideas of the article can be applied to the asset management framework design.

International Organization for Standardization (ISO) & the International Electrotechnical Commission (IEC). (2005). ***International Standard ISO/IEC 17799:2005, now known as ISO/IEC 27002:2007. Information Technology – Security Techniques – Code of Practice for Information Security.*** **London, UK: British Standards Institution.**

This technical paper is the specification and guide for implementing ISO standard 27002 security practices under the IT Governance framework. The document comprises 15 chapters in total, which cover each individual of information systems security with respect to control levels required, implementation of control, and further information. The topics covered include physical security, access control for information, risk assessment, communications management, and mobile computing

management and compliance levels. The framework document also outlines methods known as "critical success factors" which allow any organisation to gauge the level of compliance within the organisation against recommended paths to execution for compliance. The paper was designed by the ISO and IEC standard bodies to permit organisations to follow a set of internationally recognised and approved best practices. Each category has a predefined scope for implementation and the organisations provide a glossary of terms to explain all topics covered.

This document will provide the backbone of the IT Governance thesis, and in particular Chapter 7 – Asset Management. The end product of the thesis, an IT Governance and ISO 27002:2005 compliant asset management framework, will be derived using this document and the organisational policy outlined by Internal Audit and Finance departments. The framework provides one with a set of concrete, internationally recognised criteria to comply with, and it covers the diverse range of "assets" within an organisation from physical assets to less tangible assets, including: information, physical assets, qualifications of staff, reputation of the organisation as a whole.

IT Governance Institute. (2007). *Cobit Framework 4.1*. Illinois, USA: IT Governance Institute Publishing.

This framework, published in conjunction with multiple vendors of IT services and systems along with IT Governance is the latest revision of the Control Objectives for information and related technology (Cobit) framework which outlines the control areas concerned with IT Governance in an organisation. The extensive text is designed for IT management to place a set of controls or a framework in place to manage IT activities within an organisation. This model allows for tracing through maturity levels and acceptance metrics the major achievements with regard to each phase of the model. The model is concerned mainly with identifying an organisation's business needs and requirements and then linking these into the IT framework within the organisation. The model takes the form of domains and processes of responsibility

for the organisation to conform to, and the IT Governance model is represented as a hexagonal set of components into which CobiT can interlock.

This framework will give the researcher the necessary fundamental knowledge prior to commencing an IT Governance project because the areas of ITG are all examined with regard to success or failure, and there are metrics provided for the researcher to measure how well the system has performed since inception. The organisation within the research problem domain is a service oriented organisation, and the CobiT framework is based upon management of services.

King, C. (2006). ***How Much Does IT Cost : How to Estimate the Time and Cost of Implementing IT Asset Management.*** **Minerva Enterprises Financial Management Magazine, 2, 4. USA: Minerva Enterprises.**

The author outlines the results of interviews and a survey conducted in 2006 with regard to IT asset management and outlines the results and some indicators as to why these results were concluded. The author attempts to rationalise using the opinions of information officers and it managers as to why a lot of organisations do not feel the return on investment is beneficial to an organisation implementing IT asset management. The author then proceeds to issue loose guidelines as to time allotted to IT asset management and suitable areas for an organisation to direct effort towards. The author mentions a point which can be applied to the thesis authors' situation, whereby a main cause of concern was that not enough time was assigned to change management with staff, and this is an area which will impact the research of the thesis. The thesis researcher will need to provide for training and assign appropriate resources for training staff on how to get the most from the asset management system. The author pinpoints several other areas of concern which can be applied to the thesis, such as prior assessment of data: the thesis researcher will need to assess how ready is the data for categorising? Are there manual steps involved before implementing the physical container for holding the assets? The author concludes by advising how to implement best practice with regard to phasing out legacy systems, in this instance a Microsoft Access 2000 database. The researcher has completed the Microsoft SQL

Server 2005 training course which instructs the researcher on import of data from one system to a set of SQL tables.

Leedy, P, D, & Ormerod, J, E. (2005). *Practical Research: International Edition, 8ed.* New Jersey, USA: Pearson Prentice Hall.

The authors of this book cover all areas of academic research and first quantify the concepts of research and how the student can classify what each research tool can be best used for in academia. The authors break the text down into five sections, the introduction of what can be quantified as research, and then follow on with how to perform proper research. This text advises would be researchers to always break problem domains down into sub problems and approach the issue in a component type situation. Most importantly the authors help focus the student/researcher on the major topics to consider in researching and help avoid non-productive situations from arising in research. The authors promote one extremely important mindset for students/researchers to consider – that the researcher should not take other authors' opinions at face value and accept that these opinions are necessarily correct. The authors demonstrate the power behind critical thinking on subject matter, and specifically note how students should read as much as possible and then form opinions based on an objective evaluation of the area.

This textbook is the guide for the thesis author to devise the research plan around. The processes of research are categorically explained within the text and the thesis author is advised on how best to elicit the right information from a set of literature. The authors have an extensive section on how to interpret historical data which will be a very important component of the IT Governance asset management thesis – a lot of the information in existence can be used as the basis for improving the way IT assets are managed within the organisation. If a set of existing data and information are presented along with the problems associated, the thesis author can then design the best ways to avoid these problems happening again. This thesis is the first evolutionary step in how Wexford County Council will manage assets from now on.

McShea, M. (2007). *Communicating IT's Value in a Modern Business Climate.* IEEE IT Pro Magazine, January|February 2007, 42 – 45. USA: IEEE Computing Society.

The author addresses a constantly recurring problem for IT Managers within an organisation, how to demonstrate the benefits of IT accurately and demonstrate the value of investing in IT projects without reverting to traditional financial methods such as return on investment and economic value. The author identifies the common misconceptions and assumptions related to IT, and then reinforces these points with examples. The author also identifies problem domains where an accurate assessment of all IT related tools available to the organisation at a given time is not performed. In this paper the author also explains the traditional finance–oriented methods of measuring the value of IT resources to the organisation and then explores the ways in which improvement of management of resources can help communicate the value of IT assets and possibly to extend the view that IT resources can be considered as valuable and integral to the organisation as all of the critical business functions.

This article communicates the essence of IT asset management, how to think less in terms of purely financial measuring IT resources; the thesis researcher can use this as a platform to formulate accurate metrics for calculating IT value to the company.

Pengelly, J. (2005). *ITIL Service Level Management.* London, UK: GTS Learning.

In this book the author describes the Information Technology Infrastructure Library framework and its components. The author describes the framework from its origins in the United Kingdom in the 1980's to its adoption by British Government Agencies and eventual release into the public domain in its current form. The author provides a guide to devising a service level agreement compliant to ITIL and the steps involved in implementing and maintaining a service level agreement (SLA) within an organisation. In doing this the author identifies the key service areas within the framework and how they can be applied to an organisation of any size or stature. The author describes the process and workflow involved in such steps and provides a detailed description of service level management theory and practice along with why SLM is required within a business and the goals of implementing such a project. In

the book the author also identifies potential pitfalls and problems that can be encountered when adopting SLA through ITIL within any organisation. The author reiterates the importance of striking a balance between business process and IT process and the functions involved in each must be clearly defined. The author concludes with a guide to implementation and constant monitoring of an SLA once it has been designed.

This book will provide the thesis student with an insight into how the asset management framework will fit into the organisation as a whole, adding value to the business by introducing accountability for assets and introducing a method of tracing assets to users. This will prove very valuable for the IT Helpdesk team within the organisation because service level can then be ascertained by a simple query on the database as to calls logged, problems encountered by user and/or network resource. The implementation of service level agreements is still some way off within the organisation but if the asset management framework is in place from the time this thesis is implemented, the framework can be used as the cornerstone of any future evolutions towards SLA.

Redman, T, C. (2008). ***Data Driven: Profiting from Your Most Important Business Asset.*** **USA: Harvard Business Press.**

The author advises system administrators and IT managers on the set of best practices for identifying data as an asset to the organisation. The author strives to show how data is to be considered an independent asset and then outlines criteria for considering how important data is. The author urges the reader to note how rapidly data and information can multiply along with identifying how for each different facet of organisation the value of the data can fluctuate. There are many suggestions for systems administrators within the text future trends expected to take hold in the area of data as an asset management, and the author gives consideration to metadata as an entity on its own within data as an asset.

This textbook can be applied to the asset management thesis for advising the thesis author on how best to recognise data as an asset in its own right and how to consider the extra variants (data storage as an asset and different storage media).

Sisco, M. (2002). ***IT Asset Management. USA: MDE Enterprises Inc.***

This book dates to 2002 and yet the concepts contained within are even more applicable to today's networks with so much importance being emphasised on security and classification of different asset types within a computer network. The author describes all of the components involved in assessing risks involved with and how to manage technical assets within an organisation. The author begins by recommending several tools that assist information officers and IT managers on how to correctly manage the set of technical assets; for this thesis the author will not use these, as the Microsoft SCCM with SQL Server 2005 solution has already been decided upon as the most feasible solution.

The author defines firstly how to identify which assets require management, and this will be consulted to coincide with the thesis secondary research of interviewing Internal Audit staff within the organisation. The author advises the reader on how to correctly identify those components which add value to the business including the intangible categories such as reputation and staff. The author also touches on the subject of vendor contracts which can vary from organisation to organisation, and within the scope of the thesis, the thesis author will focus initially on setting the asset management framework up to manage hardware and network devices, then expand to software, skills, and any other artefacts of value to the business. The information can be classed under hardware storage and again, this subject also comes under the disaster recovery plan of the organisation which will be referred to within the thesis, but is outside of the immediate scope of the thesis. The author describes a method of asset tracking which exists within the scope of the organisation already – asset tagging with labels that detail serial numbers, product numbers, and IP address where appropriate, and asset number which corresponds to the number of the item within the asset management container.

In the course of reading through this book, the researcher notes the templates for use with tracking, and this will be useful for implementing the database and SCCM asset tracking within the problem domain. There are templates for request of change of equipment which will be an excellent way to manage purchasing over the financial year, and in these more strict economic times, the asset management database will be even more important.

Tipton, H, F, & Krause, M. (2007). *Information Security Management Handbook, 6ed.*. Florida, USA: Auerbach Publications.

The extensive text covered in this book contains an introduction to information security and then expands into all facets and sub-sections involved in information security, ranging from the principles of information security and their origins, along with risk assessment and a guide to developing and implementing a risk management plan. While all areas of security management are given considerable discussion over the course of the 3000+ pages, the text covers a lot of subject matter beyond the scope of the thesis. However, Section 1.6 the area that is concerned with Policies, Standards, Procedures and Guidelines can be applied to IT Governance based asset management plans. Issues not directly outlined within the ISO/IEC 27002:2007 framework are discussed by the author within the text such as Human Resources issues, and how to train employees to work within the guidelines of the framework governing information security. The principles outlined by the author and components of security management in information systems can be applied to the thesis and it's particularly useful as a starting point for discovering the ideals that the governance framework and issuing bodies such as ISO and IEC have consulted when defining the frameworks such as ISO/IEC 27002:2007. The project for implementing governance within Wexford County Council has already commenced, and this text will prove essential with regard to implementing the ideals of security through the asset management framework, introducing high levels of transparency and accountability for each individual within the domain.

2.4 Primary Research (b)

Annotated Bibliography for Physical Implementation of the Framework

Kazcmarek, S, D. (2008). ***Microsoft System Center Configuration Manager 2007.*** **Seattle, WA, USA: Microsoft Press.**

The author provides an administrative text book for planning, designing, implementing and maintaining a Microsoft SCCM installation or multiple installations within a domain. The text comprises four sections and each of these is broken into subsections or tasks for the system administrator to accomplish. The author begins by repetitively advertising how important proper planning and design is to the eventual success of implementing such a project. The concepts underlying this software and reasons why it benefits an organisation are outlined by the author and the author also provides online resources and documents to refer to for further information before installing the software. Although the majority of the text is taken up with implementing the SCCM package, the author also dedicates a section to the installation and configuration of Microsoft SQL Server 2005 which hosts the underlying database for the SCCM package. The author is highly instructive with the text and provides a step by step guide for implementing each concept within a test lab environment and for implementing in a live domain. The author emphasises the fact that installation of this management software will be for the benefit of matching the business needs of the organisation.

The SCCM package has extensive asset management functionality and will enable the system administrator to properly manage the IT assets within the domain and report for internal auditors and financial accountants accurately on what assets exist within the domain. The scope for managing assets is extensive and will allow the student to develop a management strategy that complies with all of the criteria within the asset management framework.

Microsoft Corporation. (2007). ***Microsoft Official Course: 2780B. Maintaining a Microsoft SQL Server 2005 Database.*** **USA: Microsoft/MSDN Press.**

This training course will develop the fundamental skills required for the thesis author to devise an asset management container for the organisation. The concepts of installing and configuring SQL Server 2005 are covered initially and the thesis author must then become familiar with all concepts within the SQL server 2005 architecture, mainly from the administrative and maintenance points of view. The initial database for managing the assets will need to be set up and configured and once implemented, monitored and maintained with a view to the highest level of availability. This database will be required all permanently and the disaster recovery plan within the organisation will be altered to factor in the new servers as a result of implementing the project. Security is the cornerstone of the ISO 27002:2007 framework and the SQL Server 2005 database has security features explained in this training course text and practical book that demonstrate how databases within the domain can be set to comply with the standards required. The security features along with the high availability features will be used by the thesis author to maximise the potential success of implementing the project.

2.5 Original Brainstorm Diagram & Project Plan Timeline

Fig. 2.1 Brainstorm Diagram:

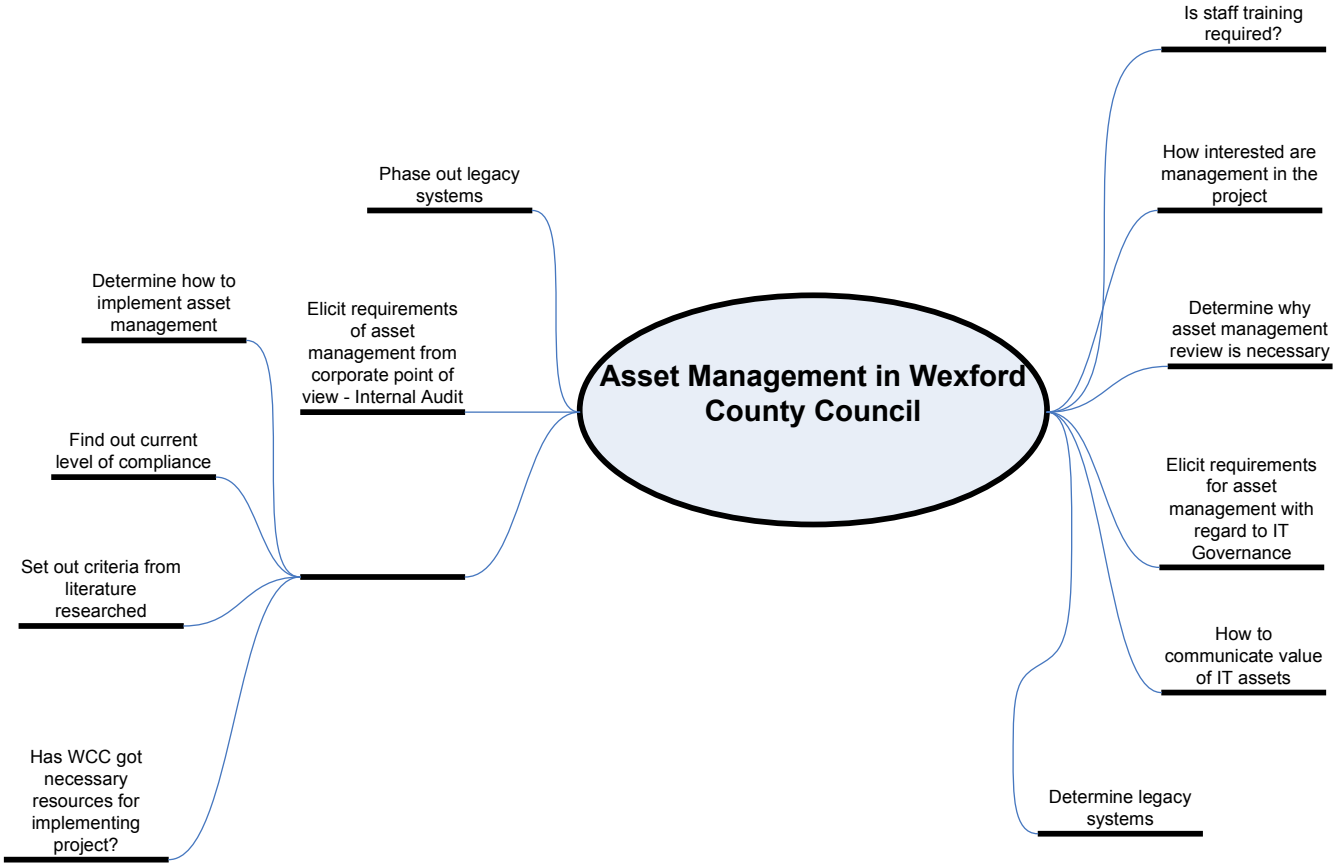


Table 2.1 Proposed Project Plan Timeline:

Interview Internal Audit staff	10 days	09/02/2009	20/02/2009
Review legacy system with management following guidelines	1 day	02/03/2009	02/03/2009
Elicit requirements from ISO standard with Internal Audit guidelines	1 day	03/03/2009	03/03/2009
Prepare for installation of SQL Server	1 day	04/03/2009	04/03/2009
Prepare for installation of MS SCCM	1 day	05/03/2009	05/03/2009
Install and configure software	1 day	06/03/2009	06/03/2009
Implement asset intelligence to gather extensive information	5 days	09/03/2009	13/03/2009
Define information classification - Appendix	1 day	16/03/2009	16/03/2009
Define information ownership - HR & Internal Audit. Devise actual framework and document	30 days	17/03/2009	25/04/2009
Link assets to acceptable use of assets policy	15 days	24/04/2009	14/05/2009
Train co-workers on asset management framework at work	7 days	15/05/2009	25/05/2009
Identify scope of devices to be recorded initially	4 days	26/05/2009	29/05/2009
Contact vendors to elicit expected life cycle of common hardware in domain	20 days	01/06/2009	26/06/2009
Documentation	?	29/06/2009	27/08/2009

Chapter 3 Primary Research Findings

3.1 IT Governance Historic Context

Examining the history of IT governance, the researcher can demonstrate how it fits into the parent discipline of corporate governance. Corporate governance exists to enable organisations to elicit control and direction over their operations (Calder & Watkins, 2008). The associated corporate governance frameworks consist of many elements that vary between statutory requirements to non-statutory or organisation specific elements. (Calder, 2008)

Corporate governance originates back to 1979 and the publishing of a report in the United Kingdom (Calder, 2008) which consisted of a set of papers set out to examine "boardroom responsibilities" within organisations. Corporate governance as an entity was defined to differentiate between how business activities were carried out within an organisation and the roles and activities that the board of directors are faced with regularly – interaction with all other stakeholders in the business (Calder, 2008). Since 1979 many papers and books have been published devoted to the discipline of corporate governance, one of the most prominent being the Organisation for Economic Co-operation and Development (OECD)'s publication – "Principles of Corporate Governance" (OECD, 1999).

Information technology governance is the "framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives" (Calder & Watkins, 2005). Governance exists to give leaders of public companies a responsibility and framework to adhere to, and gives organisations the means to provide sufficient management of their IT assets, information, and information related assets. There are other definitions available for IT governance, the IBM definition states that a combination of political and organisational roots for governance influence how governance is perceived (Cantor & Sanders, 2007). Governance can be described as a method of devising

external requirements for an organisation and then enforcing these on the organisation (Cantor & Sanders, 2007), or as a process in its own right.

Governance should also be considered as a long term oriented process for organisations, and the process of managing and controlling the many benefits of an IT infrastructure (Cater-Steel, 2009). This approach reflects the greater reliance of organisations on IT infrastructure to support the ever evolving business needs and requirements. IT assets should be managed with the same level of responsibility that is assigned to all other facets of an organisation – "responsibly, efficiently and effectively" (Cater-Steel, 2009). Governance is very important to an enterprise; it is responsible for promoting a sequence of events or actions (Magee et al, 2008) eventually reaching an end result. Governance is concerned with security, in the form of responsibility chains, and the establishing of standards, controls, roles and mechanisms to support security (Magee et al, 2008). Governance has the following considerations within its remit: (Brown et al, 2009)

- A strategic IT plan
- IT investment plan and budget
- IT Processes and relationships to organisational policy
- Management strategy and direction
- Quality management
- Assessment and management of risks
- Project management
- Domain security
- User training and education
- Continuous monitoring and evaluation for improvement
- Human resources plan

IT governance can be derived from the corporate governance framework or addressed and devised as an entity in its own right. Corporate governance has introduced the fundamentals of the organisation and how they are controlled; IT governance is a way of setting in place a framework that allows control of information and all of its

associated entities to achieve the organisational strategic goals and objectives (Calder & Watkins, 2008).

Many variables are responsible for driving the need for IT governance, and the concept has been described as a way to develop leadership and accountability within the confines of an organisation which can then aid development and delivery of the business capabilities of the organisation. The governance strategies and goals can be used to align business functions with IT functions and allow the business to effectively and efficiently achieve its objectives (Mueller et al, 2008). IT governance is most concerned with security, high availability, asset management and disaster recovery.

3.2 Types of ITG Techniques and their Areas of Concern

One of the main driving forces behind the evolution of IT governance as a process was the publishing of the Sarbanes-Oxley Act in July 2002 (Chorafas, 2009). This act was published to set out financial accounting and audit requirements for organisations. IT governance is included in the correct method for audit, and the Act defines how IT is used to support it. There are several frameworks for implementing IT governance within an organisation. The most commonly employed variants are (Cater-Steel, 2008):

1. ISO/IEC 27002:2007 Information Security Standard
2. Information Technology Infrastructure Library (ITIL)
3. CobiT Framework
4. Software Process Improvement and Capability Determination (SPICE)
5. ISO 20000 – IT Service Management

For each of these a set of constraints were assessed to see which method would be most suitable, or a hybrid could be developed using parts of each to perform accurate asset management. Before the project could be initiated, the criteria outlined in Chapter 1 concerning estimation of time and cost (King, 2006) with regard to IT asset management had to be satisfied. These involved estimation of the following:

- Time to develop the knowledge base within the organisation - the knowledge base was in existence in the organisation in many shapes and forms, from policies of internal audit, fixed asset management in financial accounting to the communications policy signed by every employee who avails of the telephones, email and IT infrastructure of the organisation

- Time taken to diagnose a solution (assessment of available solutions) – these are all assessed in Chapter 5 whereby a set of requirements are outlined and the available software solutions were tested against these for compliance. The end decision was arrived at mainly because of the organisations leaning toward Microsoft products and the existing knowledge base of staff could be used optimally with implementing

- Get senior staff to commit to the project – the project leader of the technical services section and the Head of Information Systems were both consulted prior to setup, and this lead to sign off for costs associated with the project, in PRINCE2 terms, the project had 3 "champions"

- Define opportunities where improvement would be immediate – in the current economic climate this was a very important point to consider when budgets have been shrunk and the organisation has an onus to only replace or purchase when deemed absolutely critical to the provision of services. Licensing is costing the organisation hundreds of thousands of Euro each year and this situation required more stringent control. One of the requirements of designing a framework for asset management was the assessment of security, licensing for desktops, and replacement of obsolete equipment (posing potential security risks using outdated operating systems and security settings). There were several metrics designed for enforcing these which are all covered in Chapter 6 which demonstrate how the framework for asset management is physically implemented. Other benefits include (ITGI, 2007 pp48) prioritisation within IT budgeting through targeting potential security risks for upgrade first, and more efficient cost management.

- Assign accountability and "ownership" (ISO, 2007) – this was accomplished through examining the communications policy of the organisation with regard to IT assets and then assessing the ISO 27002:2007 standard to outline where these overlapped. This is demonstrated in detail in Chapter 4, where the derived framework is presented according to ITG principles and the ISO 27002 standard in conjunction with corporate and government policies concerning the organisation.

- Consider the use of a prototype solution – a rapidly introduced management method for assessing security with regard to software licensing, updates and non-compliant software was designed, this is presented in Chapter 6 along with screenshots outlining how the prototype solution facilitated the identification and replacement/upgrade of any potential risk associated hardware
- Provide a critique and identify faults of existing legacy system – this is presented in Chapter 1 where the problem domain is assessed along with the drawbacks of existing current practice for asset management. The research was geared toward the successful projects initiated and demonstrated by case study, such as the Ontario Pensions Board

- How long does could it take to develop new policies from existing policies? – this point did not involve as much time consumed as was initially estimated, the original figure, presented in chapter 2 with the literature review was inaccurate

- Cost incurred by supporting technology

3.3 Asset Governance

Asset governance comes in as a sub section of many of the ITG frameworks – under the ISO 27002:2007 the subject is approached in Chapter 7. This chapter was used to

formulate the rules defined in the framework applied to the problem domain. The main research question posed by the researcher involved assessing how a study could improve the standard practices for IT asset management within WCC. The system in place was proven to be obsolete and incomplete when compared with best practices. The researcher was presented with the challenge of devising an asset management framework that complied with Irish local government rules and the criteria outlined in IT governance literature.

To begin with, the researcher had to investigate previous success stories and case studies of asset governance in enterprises, the numbers of these were few and far between. One of the main issues with conducting the study was the researcher could access many sets of documents and literature concerning ITG but there is very little asset governance literature available as its own entity. Of particular interest to the author was the report of a successful ITG implementation used by the Ontario Pensions Board (OPB, which outlined how the CobiT framework principles were applied to put in place best practices for IT management in several areas. The area of risk assessment and management was the main area of interest for the researcher because of the strong foundations for asset management within security and risk management (ISO, 2007).

3.3.1 CobiT and Asset Management

The principles of the CobiT framework were highly applicable to an asset governance only project; the framework contains the following metrics and controls within its specification:

The CobiT Section "Plan and Organise, PO4.14" (ITGI, 2007 p48) demonstrates the necessary actions for first implementing how a set of practices and policies should be in place governing contracted staff. This approach was applicable to the project by applying the communications policy and internal audit fundamentals to the project to ascertain how best to introduce maximising information integrity through protection of all the organisations IT assets (ITGI, 2007 pp111). This is done through many mechanisms, establishment of defined roles within the IT section, assigning accountability and responsibility through ownership of assets, and the use of existing policies and standards within the organisation. The use of a "centralised tool" (ITGI, 2007 pp111) to monitor and manage each asset of the organisation is advised as best

practice with regards to securing information via IT assets. This is the favoured approach and is enforced using Microsoft SCCM, detailed in Chapter 6. The framework complies with the principles evoked in CobiT (ITGI, 2007) of delivering value from IT systems by maintaining security and in conjunction, system "up-time", and provisioning for more efficient risk management with regard to IT services.

3.3.2 ISO 27002:2007 & ISO20000 - Asset Management

ISO 27002:2007 and previous ISO iterations with regard to information systems security feature asset management functions and best practices with control mechanisms in some shape or form. The following controls are offered for implementation of asset management within the ISO standards:

- Declaration of responsibility for assets
- Creation of an inventory or "stock take"
- Classification methods for assets
- Delegation of accountability and responsibility through ownership
- More transparent auditing – accuracy of inventory
- Acceptable use of assets schema
- Classifying information as an asset
- Information labelling
- Risk assessment best practices
- Identification of risk types – threats, vulnerabilities
- Eliciting control
- Linking the best practices to the corporate policies, and disaster recovery plan
- Correlation of the relationship between IT assets and their objectives/business activities they support
- Risk impact analysis

3.3.3 ITIL and Asset Management

ITIL main area of concern is service management, and the service desk (helpdesk) within the organisation is designed around the fundamentals of ITIL and the provision

of services. In this capacity it is possible to link the service desk to an individual computer or asset associated within the inventory. The ITIL framework offers many insightful best practices for asset governance and IT governance, including areas beyond the scope of this research such as provisioning for staff training, the centralisation of a service desk, and creation of service level agreements (SLA) to allow users within the organisation to interact with service desk and IT staff to name a few. Points of note with asset governance for consideration within the research:

- Use of an IT procurement policy to complement the corporate procurement model or offer improvements for implementation where possible
- Asset configuration through inventory, regular assessment of the current state of the inventory and continual improvement process in place (Cater-Steel, 2009)
- Guideline for asset inventory scope is defined clearly
- Service descriptions are associated with assets
- Recommendation of storing assets by evaluating them for replacement, prioritising in this instance
- Assess business value of assets with consideration to the current condition, age and decide whether to "leverage, maintain, replace or terminate" (Allen, 2006)
- Asset inventory is considered a very important component of the configuration database for ITIL (Allen, 2006)
- The asset inventory is the cornerstone of ITIL service management, and is used for provision of service delivery, service support, service analysis and service management (Allen, 2006)
- The ITIL maintains that metadata for assets is as important as the assets themselves within the inventory (Allen, 2006)

3.3.4 SPICE - Asset Management

SPICE advocates the best practices of the ISO standard ISO15504 (Cater-Steel, 2009). The SPICE framework is divided into several major categories, and the asset management component is described in the Organisational Life Cycle processes and is managed by a reuse process group. This group is employed in the framework to research areas of reuse, particularly in asset management by assessment of the assets

in place (Cater-Steel, 2009). The main focus is improving business performance through constant review of the predefined library of documents and methods (Dorling, 2006). Although geared more toward the development of standard process assessment methods for software development, the asset management area within the framework, with regard to reuse, must be considered for this research and this fundamental concept can be used to devise asset replacement policies and expected life cycles.

Chapter 4 Framework derived from ISO27002:2007 and other ITG best practices

"Account for and protect all IT Assets" (ITGI, 2007 pp65)

The focus of this chapter is to present the proposed framework and describe how the framework was derived. The researcher will present the physical implementation of the framework using SCCM and associated demonstrative screenshots in Chapter 6. Appendix D contains all of the relevant details for installing and designing the SCCM database and software application for managing the assets.

Areas of concern for scope of the project are

- security,
- subset specifically securing assets,
- identifying risks associated with assets and
- compliance with communications policy.

The communications policy is derived from corporate policy, and complies via inheritance from Irish Local Govt internal audit guidelines.

Motivations for the study as mentioned in 1.3 are:

- improve valuation process of assets,
- improve stock taking procedures,
- And improve security on each level: physical, data level, and through enforcing all security controls on the information systems architecture.

CobiT as outlined by the ITGI (ITGI, 2007 pp30) advised on devising a strategic plan involving IT and the rest of the organisation. This issue for the researcher was not applicable in the context of the study – a corporate and strategic plan is already in place for provision of business operations and services and how IT best serves these areas. Creation of principles to be enforced on asset governance meant that the researcher had to first examine how IT services and assets are viewed currently in the organisation, and then prove how improvements to the asset management process can benefit the organisation at large on different levels: budgeting and financial

accounting, auditing, procurement and requisition procedures and introducing individual and sectional level accountability (ITGI, 2007 pp30).

The end product of this framework was a repository for housing, facilitating management and monitoring of all IT assets. A measurement of compliance to security baselines is taken periodically from the repository (Microsoft SCCM). The percentage of assets successfully monitored is measured and adjustments to security can then be enforced resulting from this. The principles involved in measuring this percentage are demonstrated in detail in Chapter 6 and the requirements for information on each asset are listed in Appendix A.

4.1 Risk Management and Asset Governance

The goal of this research was to derive how best to protect the organisation's IT assets and comply with the legal and corporate requirements in place. Using fundamental principles of CobiT (ITGI, 2007 pp65) and ISO27002:2007 (ISO, 2007 pp20-21), the researcher was required to concentrate on risk assessment regarding the IT assets and management of the risks – how to report risks and the process of associating risks with business processes. CobiT (ITGI, 2007 pp65) provided a set of activities and metrics for measurement of risks and assessing how to manage and guard against each. The metrics for assets risk management involved assessing critical objects and assets within the organisation and "establishing clarity on the business impact of risks" (ITGI, 2007 pp65). Another document which proved highly valuable for this purpose was the ISO/IEC 13335-3 Standard (ISO, 1998). Under this plan, all assets were proposed to be accounted for, and protective measures employed depending on the criticality (ITGI, 2007 pp65). The researcher was then posed with a challenge, how to differentiate between assets and their importance? Business processes and the impact of a security breach on an asset were the first topics to be assessed for this (ITGI, 2007 pp117). The following method is proposed by the CobiT framework (ITGI, 2007 pp117):

'Control over the IT process of

Ensure systems security

That satisfies the business requirement for IT of

Maintaining the integrity of information and processing infrastructure and minimising the impact of

Security vulnerabilities and incidents

By focusing on

Defining IT security policies, plans and procedures, and monitoring, detecting, reporting and

Resolving security vulnerabilities and incidents

is achieved by

- *Understanding security requirements, vulnerabilities and threats*
- *Managing user identities and authorisations in a standardised manner*
- *Testing security regularly*

And is measured by

- *Number of incidents damaging the organisation's reputation with the public*
- *Number of systems where security requirements are not met*
- *Number of violations in segregation of duties'*

(ITGI, 2007 pp117)

Risk management metrics on IT assets are defined in Appendix C. An individual within the organisation, job title "Administrative Officer" in the Finance Section is employed to manage risk assessment and insurance policies for the organisation and these recommendations for risk assessment in Appendix C can be proposed to the officer. Best practices for asset governance were researched in Chapter 3, and the resulting principles can be applied in conjunction with the assertions proposed.

Implementation guidelines were decided using the IT governance principles and specifically asset governance principles along with the corporate plan of the organisation and its communications policy (Wexford County Council, 2004 – see Appendix F). The following proposed best practices were devised to manage assets and the risks associated with assets, the guidelines were all based around the actual best practices proposed by ISO 27002:2007 (ISO, 2007 pp20-21). Use of ISO standard best practices promotes the use of continuous improvement both through assignment of roles within the security spectrum; ITIL also promotes the same fundamentals when deriving best practices (Tipton & Krause, 2007), along with Service Management approach, ISO27002:2007, CobiT and SPICE. These were discussed in detail in Chapter 3, section 3.3.

4.2 The Derived Framework

Objectives of the Framework:

(a) "To achieve and maintain appropriate protection of organisational assets" (ISO, 2007). All assets must be inventoried and have an assigned owner within the organisation. Responsibility: asset protection, maintenance and controls are assigned to each owner. Certain controls deemed beyond the remit of owners are delegated to a specified owner within the IT Section. The inventory is required to ensure that all assets are effectively protected and secured.

(b) Ensuring that the organisations information is adequately protected according to its value to the business activities. Classification metrics for assessment of importance must be detailed, these appear in Appendix B. Both of these points comply with the communications policy of Wexford Local Authorities (Wexford County Council, 2004).

SCOPE:

For the purposes of this study, the only objects considered were IT assets and outlining a framework for their governance within the organisation. Any other security functions and procedures are outside of the scope of this study but are mentioned because of their importance. The best practices below would be best

applied to all communications media related to Wexford Local Authorities and staff performance of daily tasks and duties.

(i) Inventory of Assets:

Organisational IT assets need to be clearly identified as property of the organisation. A repository for storage of asset information must be created and updated/maintained. Metrics should be put in place for assessing importance of assets and classification performed. The assets should be included in the disaster recovery plan of the organisation and any information specific to individual assets required for recovery should be included in the plan. Appendix A contains the listing of data required for each assets detail. Classification of assets is listed in Appendix II and metrics proposed for assessing the value of an asset to the organisation. The inventory of assets must be made available on request from other non-IT organisational units, particularly in the instance of health & safety, human resources, or insurance issues. Where possible, a business value should be attributed to assets. A fixed assets schedule exists within the organisation but this does not account for intangible assets detailed in Appendix B. This is standard practice currently in public sector organisations; once the IT asset inventory has been created, it must be cross checked against the fixed assets schedule maintained by the finance dept. The new proposed procedure for adding assets to the domain and the inventory is in Chapter 6 – the physical implementation of the framework best practices.

(ii) Ownership of Assets:

"Each user carries sole responsibility for security access to his/her computer." (Wexford County Council, 2004)

The following Irish Government Legislation enforces regulations on the communications policy (Wexford County Council, 2004 – see Appendix F):

‘

- Employment Equality Act, 1998

- Equal Status Act, 2000
- Data Protection Act, 1988 & 2003
- Freedom of Information Act, 1997
- The Companies Acts, 1963 - 2001
- Copyright and Related Rights Act, 2000
- Child Trafficking and Pornography Act, 1990 ‘ (Wexford County Council, 2004)

The definition of an owner (ISO, 2007) must be clearly demonstrated, and the importance of this definition must be stressed so that confusion does not arise over what constitutes an “owner” in the context of the information systems infrastructure. The word owner does not imply property rights on any device or piece of equipment. An owner is an individual assigned to a position that implies or entails responsibility for “production, development, maintenance, use and security of the IT assets” (ISO, 2007). The fact that WLA is a service oriented organisation means that ownership may be equated to a group of assets being owned by a services, such as online payments database and web application servers. Delegation of tasks in using assets is permitted, but the responsibility of care of the asset still terminates with the owner. When co-ordinated with the communications policy (Wexford County Council, 2004 – Appendix F) the following points are noted:

Relating to use of the term “ownership” attributed to each asset, the WLA communications policy (Wexford County Council, 2004 – Appendix F) clearly states that the word “owner” implies no individual property rights on equipment purchased by WLA, the equipment is sole property of WLA. All software used within the organisation is licensed by WLA and therefore the property of WLA. The software is provided to enable employees to conduct their day to day work in the provision of public service. Software is to be inventoried within the asset repository and subjected to the same governing rules as hardware assets. Software metering and computer compliance should be measured regularly and if non-permitted software is found installed on computing equipment, it should be removed as it poses a security risk, a licensing risk, or cause incompatibility with assets running in the domain. Any

software policy breach will be dealt with in accordance with the WLA grievance and disciplinary corporate policy in place.

An owner may be attributed to the following (ISO, 2007):

- A set of business activities
- A business process
- An application
- A set of data

Expanding further on ownership, the staff member's seniority should be appropriate to the value of asset(s) that the individual "owns" (Calder & Watkins, 2005). A recommendation of ISO 27002:2007 is that each member of staff signs a corporate document such as an appendix to the signing of the communications policy indicating that they accept responsibility for the asset(s). Best practice is to keep this signed document on the individual's personnel file and/or with the assets schedule or register (Calder & Watkins, 2005). Detail in the document shall include asset(s) in the person's ownership, location of asset(s), and security controls for the asset(s).

The following are to be the final instructions in accordance with ISO 27002:2007 Asset Inventory Guidelines (ISO, 2007):

1. The SCCM administrator is responsible for implementing and maintaining this asset register
2. Owners of assets are responsible for advising the administrator of changes and to help maintain an up to date repository
3. Inventory is to be broken down into hardware, software, communications and intangible assets as instructed in Appendix B – Classification of Assets
4. Risk assessment shall be calculated on this inventory (see Appendix C)
5. All required details regarding each asset are to be defined
6. An owner is to be defined and notified of ownership for an asset
7. All new assets are to be correctly labelled and added to the repository

8. The repository should be maintained and updated as assets are changed or disposed of
9. The best practices listed should be made available for all staff to read as an accompaniment to the corporate policies library

(iii) Removal of assets

Removal of any asset from the premises requires prior authorisation from a line manager and the responsibility for the safe keeping and security of the asset is on the owner in the same capacity as it is within the organisational premises. This should be particularly noted in the case of laptop or portable devices belonging to WLA. In the instance that a device stored sensitive data the organisation is at risk on security level, a trust level, and any incident arising from sensitive data being misplaced could damage the organisations reputation irreparably. This applies to a software asset also, as stated, the software is the sole property of WLA and removal of software or applications without prior approval from a section head, or the head of information systems is in breach of the communications policy.

(iv) Acceptable use of assets

This consists of a set of rules defined by the IT Section and Personnel section, covered by the communications policy (Wexford County Council, 2004 – Appendix F). Acceptable use of assets is covered in ISO/IEC 27002:2007 Section 7.1.3. Acceptable use includes all IT communications assets including mobile and handheld devices. Each owner must not put the organisation, fellow employees or customers at any risk due to breach of the rules governing these assets. These rules govern the employees of the organisation and any consultants or visitors to the site with regard to appropriate use of assets and minimising security risks by correct use of assets. The email and telephone infrastructure are to be treated the same way as any written communication on behalf of the organisation. Company email policy is covered within the communications policy in Appendix F.

Software assets include the following (ISO, 2007):

- Application software used to perform daily duties, either developed in-house or vendor supplied
- System software
- Development tools and libraries
- Software utilities licensed for operating systems

The organisation pays an annual subscription to software and operating systems and the licensing fee is decided by the inventory of assets and their associated numbers of software, and the inventory will maintain a regularly maintained list of software and hardware associated with each asset. A requisition form can be issued electronically and/or in hard copy to identify any non-networked (off-site, standalone) computers and their associated software. This would typically arise for instance, in the case of a civil engineer based on a roads site office somewhere with no direct WAN access.

In accordance with ISO27002:2007 (ISO, 2007):

1. Every employee, direct and indirect is responsible for ensuring they comply to proper use of the organisation's email and network infrastructure
2. The responsibility for setting mailbox policies in place is with the IT Technical Services team
3. The HR training officer is responsible for ensuring all employees have the required skills to use the infrastructure correctly
4. Each employee is responsible for not increasing risks to the organisation through misuse of email or communications
5. The technical services project leader is responsible for "responding to and managing" security incidents (ISO, 2007)
6. Email may not be used to breach any HR policies
7. Infrastructure is used to send and receive confidential information; the IT technical services team is responsible for ensuring adequate security is in place for this purpose
8. All email attachments are to be filtered by external consultancy service and legitimate attachments related to business may be retrieved

9. Any incidents of virus/spam warnings should be reported to the technical services team
10. This document complies with the Communications Policy (Wexford County Council, 2004 – Appendix F), which contains more guidelines on personnel issues with email

(v) Replacement of Assets

Replacement of assets will take place on a regularly scheduled review, the frequency of which is at the discretion of the Head of Information Systems and Head of Finance department. All of the inventoried assets will be subjected to age analysis and compatibility for upgrade or replacement. A fixed number of equipment to be replaced will be defined in the annual budget process and software associated for these should be accounted for. The method for replacement of assets is described in Chapter 6, demonstrating the physical implementation of the framework. With the existing system, there was no provision for replacing assets until one failed or broke down. The new framework presented will introduce more stringent control over such situations. If a minimum amount of equipment can be targeted each quarter/half or annually at least, the equipment provided to staff to perform daily duties should always comply with to recommendations by vendors. This form of estimation is more feasible than the linear depreciation method or any other fixed method because a simple RAM upgrade may suffice in some cases than replace a computer; whereas the linear depreciation may not facilitate such estimation.

(vi) Classification of information:

1. Information is classified according to value, sensitivity, and how critical it is viewed within the organisation
2. Information classification can and should be revised periodically, particularly when new applications and services are introduced to the organisation
3. Asset owners are responsible to inform the SCCM administrator of any changes to be made to asset or information valuation and classification
4. Classification of an asset determines the level of protection applied to it
5. Assign a business impact to each class of information

6. Classification labelling should be considered for information, in the form of confidential, restricted, and access control lists already in place are to be revised to implement this classification
7. The existing system of Access Control Lists defined from organisational unit shall remain in place but more stringent control should be elicited over departmental access levels where appropriate

(vii) Labelling

1. All assets must be clearly marked property of WLA with an emblem sticker and identifying serial number corresponding to the asset repository
2. Software assets can be labelled in a catalogue and if packaging exists for the software it should be labelled clearly in the same way as a physical asset
3. Classification of assets should be consulted to link each class of asset back to the repository
4. Labelling should include facility for classification of sensitive or confidential material
5. In the case of database information, metadata should be used to classify the information

(viii) Resultant procedure for adding new hardware to the organisational domain:

1. Equipment arrives on premises and is unpacked, labelled immediately as property of WLA using labelling software
2. Asset is set up/installed and configured
3. If asset is networking equipment (e.g. switch, hub, router), it is also added to an IT spreadsheet for any changes to network
4. Add asset to domain, give asset a meaningful name relevant to physical location in domain, e.g. if in roads department, asset is to be called ROADS001 and so on in sequence
5. SCCM administrator runs heartbeat discovery or schedules to run within 1 hour to update asset repository

6. All asset details should be checked when the repository is updated, cross checked with physical characteristics, identify classification if required (as per Appendix B)

Chapter 5

An Assessment of Available Technologies for Implementation of the Framework

In order to assess the proposed technologies the researcher must present the predominant factors in the selection process. These include cost (time and monetary), corporate policy, licensing, suitability to the ISO framework in respect of asset management, and staff training. Non-organisational requirements such as government policy, internal audit requirements and project management techniques in place were also dominant determining factors in the selection process. The literature review in Chapter 2 involved assessing the IT governance disciplines and associated technologies to gain an accurate set of outlines for managing IT assets. Once completed, the researcher used the findings to define the framework and then implement the framework in the physical form of Microsoft SCCM 2007 and SQL Server 2005.

One of the first major points for consideration by the researcher was the fact that there is now a growing trend in public organisations toward e-business more than traditional applications. Government departments worldwide are also involved at this level of business and more and more authorities are solely running their day to day business activities around e-government. This is significantly happening across the European Union and the e-government projects are based around the concept of the provision of services rather than designing applications alone. Services are now geared to be "citizen-centric" (Friedrichs & Jung, 2007). This trend is evolving rapidly with the idea of shared services in e-government: various departments or county local authorities combine their effort in a joint-venture or co-operative project and these types of project lean toward and show strong bias to the SOA architecture and framework. Authorities then develop architecture for a service that's platform and vendor independent and allows the authorities to provide a "uniform and integrated user experience" (Bosch, 2007). To facilitate the more effective management of the assets once the framework was devised, the researcher had to decide on how to best enforce the best practices for risk assessment – do the assets get linked in groups to services and business processes, or were they best served by linking assets to the applications they support? The conclusion drawn was to use each asset as service-

centric which is the approach advised by the ITIL (Bajada, 2008); and the following were found to be true in the case of Wexford County Council:

- There is a large dependency on IT services, one example being the web application server and the Citrix Secure Gateway allowing secure access to the LAN
- Visibility and transparency are required by internal audit and for accurate risk assessment – each IT service can be linked to points of failure and in turn hardware or assets
- Complexity is increasing as newer projects are added to the organisation

All of these factors helped determine how to link assets to services, and a recent addition to the organisation was Service Desk Express, a helpdesk software solution which supports ITIL best practices and facilitates efficient service management (BMC Software, 2006).

5.1 Technology Solution Baselines for Testing:

The following baselines had to be established for assessment of the potential technologies used to physically implement, store and manage the asset data.

1. Did the solution offer support for IT governance best practices?
2. Was the solution cost effective and did it involve extensive training (highly important given the time frame)?
3. The domain is Microsoft-centric, was the solution suitable in this respect?
4. Could the solution be used on existing hardware in place if made available, or would new hardware be required?
5. Is the solution scalable?
6. Would the solution fit in to the disaster recovery plan?

Software Solutions:

5.1.1 Solution 1: Altiris Service & Asset Management Suite (Atiris Inc, 2006)

1. On first impressions of testing the application the researcher found that the solution did indeed support aspects of IT governance best practices, in particular from the perspective of ITIL. The solution is based around the fundamentals of service management within ITIL and the asset classifications and management concur with the principles of ITIL and indirectly to ISO 27002:2007. Of particular interest in this solution were the options available to implement security controls as described in ITIL and ISO 27002:2007, and the support included for the financial procurement process. IT purchases, like all other purchases in the organisation must be passed through a procurement process when over a threshold value (Irish Department of Finance, 1994); the solution offered a level of support for this.

2. The organisation currently pays licensing to Symantec for back up exec, the program used to perform backups and physically implement the disaster recovery plan, so an additional costing could have been added to this annual licensing fee. Training on the product could be conducted through built in tutorials and use of the product vendor's website.

3. The solution was very adaptable to integrate into a Microsoft Windows domain environment – the data store behind the application was designed to run on a Microsoft SQL Server 2005 environment. The client computers had a small package component deployed throughout the domain which took place in all subnets, and the application agent could then be used to manage computers/devices remotely. The minimum requirements were all realistic expectations to have when deploying to a desktop computer oriented domain.

4. Existing hardware which was in place already in the form of DELL Poweredge 1955 Blade servers (DELL, 2006) was compatible with the minimum requirements of the software, and could be installed immediately

with either both the application and the SQL database housed on the same server or on separate servers.

5. The solution was highly scalable, SQL server 2005 back end to the software meant that depending on the version of SQL server, enterprise or standard (WCC uses standard) the data could grow and evolve exponentially with no limit other than physical disk size (Microsoft Corp, 2006) as new assets are added and old asset records get modified. This software involved installing a client component on each computer that derived information for the database, and offered a method of filing each component of equipment in organisational units such as is done in Microsoft's active directory component. Assets could then be assigned by location, department, or whatever way each individual IT section wished to store this data.

6. Through research it was noted that the disaster recovery plan in WCC includes backing up daily an image of each DELL blade server using Altiris (Altiris Inc, 2006). If the server were to experience a failure, hardware or software fault the downtime for this solution would be an estimated 20 minutes, depending on the amount of data on the drives at the moment of time. In this particular case, the Altiris software was 100% compatible with the solution and was developed by the same vendor.

With this solution one major selling point was the idea of software metering – the monitoring or setting up of an access control list to define what was acceptable software for installing within the domain. In this way the security of the assets internally was facilitated by ensuring that no unauthorised software could be installed without prior approval.

5.1.2 Solution 2: Symantec Control Compliance Suite 9.0

1. This product supported ITG from the perspective of risk management and measuring compliance to best practices within a domain. The product was developed with several mechanisms to reinforce the governance policies of an

organisation; and offered a provision for development and evolution over time of policies. Many security functions such as domain group policies and template deployment were supported in this product. This product supplies customisable monitoring tools for measuring compliance with regard to software and assets within the domain. Template policies compliant with ITG policies are included.

2. As above, the licensing paid to Symantec could be modified to include this product. Training on the product could be conducted in the same way, but staff would require good experience and knowledge of security functions within a domain.

3. This solution was designed for Windows and Linux/UNIX variants and offered the client the option of using SQL server or Oracle as the repository of choice. The built in asset repository was customisable and could be implemented in a Microsoft dominant domain.

4. The existing hardware in place met the minimum requirements for this software solution.

5. Because of the nature of the databases, the scope for growth and scalability over time was facilitated, this is a solution geared toward large enterprises and offered a method for a team to manage and implement a security plan within the domain.

6. This database could be easily implemented into the DR plan – the database could be backed up to disk in a task and then exported to tape once complete or even replicated servers could be implemented. The nature of the database change frequency would dictate the level of backup type but the product was designed to conform to all DR necessities.

5.1.3 Solution 3: Microsoft System Center Configuration Manager 2007

1. This solution complies with the ITIL framework offered by the office of government commerce and is supported through the use of the "Microsoft Operations Framework" (Kaczmarek, 2008 p507). The product and its fundamental ideas are based around the provision and management of IT services and service level agreements.

2. The product is an add-on to the Microsoft Licensing agreement through the local government framework and because of the existing knowledge base of IT staff, and the fact that the product is based around technology already in use in the domain, this solution was deemed the most appropriate solution. Training would be easier to implement within the domain for this product, as the staff have a solid foundation in Microsoft technologies and most software development projects are implemented using SQL server and the .net framework.

3. Microsoft designed and developed this product so it would make implementation much more smooth and streamlined, an existing SQL server database instance on a DELL blade could be the basis for the repository and another DELL blade had been assigned to host the application itself.

4. The existing hardware fully complied with the requirements of this software solution.

5. Scalability was not an issue with this solution, as with all of the others examined; the software runs on an enterprise capable database instance and supports concurrent transactions and multiple connected users. The front end reporting tool simply uses the client web browser. This solution, like the others examined supported virtualisation.

6. The DR plan could be modified to back up the database to disk, like Control Compliance Suite, then a disk to disk and LTO tape backup could be

performed. The server is of critical importance once an asset repository has been set up, and will be treated as such in the DR plan. All of the organisations data is backed up to several places.

Chapter 6 Physical Implementation of the Framework

The purpose of this research was to define the best practices for asset governance, then show how these could be physically implemented in an SCCM & Windows dominant environment. This chapter presents how the SCCM software and its underlying SQL Server 2005 database support the points proposed in the framework in Chapter 4. All points were considered, and in Appendix A the existing labels system and required information of the legacy access database are detailed.

6.1 Ownership and Asset Inventory

Straight after server side SCCM installation (described in Appendix D) is the gathering of the inventory phase. This is done by deploying a client installation across the domain through all of the resources located in the Microsoft Active Directory database. Computers are identified, and the client deployment is pushed to these computers. This conforms to the requirement, “account for and protect all IT assets” (ITGI, 2007 pp65). A compliance percentage updates as new clients are successfully added, and this is the same for deploying critical operating system and security updates as they are released. For more detail - see Fig 6.1 below:

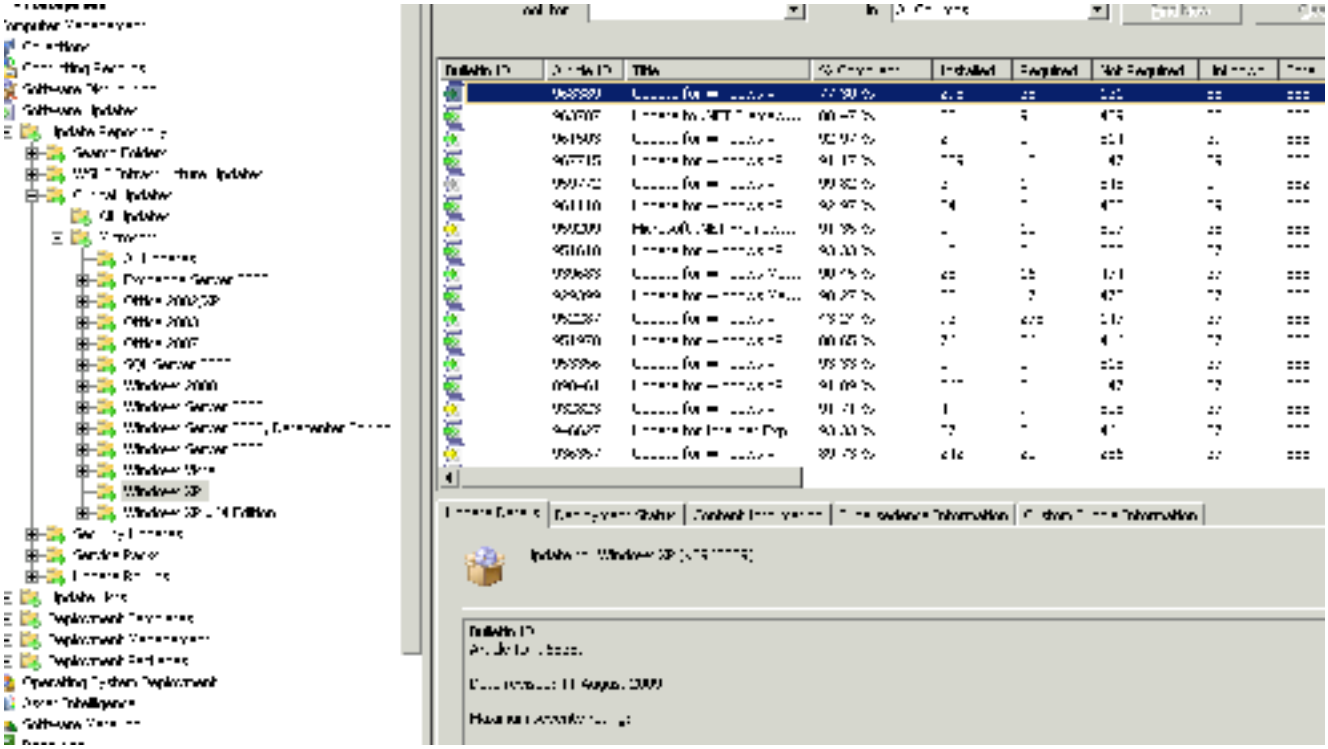


Fig 6.1 – SCCM details of software update. Compliant percentage is calculated for each deployed package.

Points (i) and (ii) in Chapter 4 refer to creating an inventory of all assets and identifying then assigning “owners” to each of these assets. The database houses the “population of client computers” and devices in the chosen environment for managing (Kaczmarek, 2008 pp268). Population of the database is accomplished once the initial configuration client install has been completed. Each record derived from hardware is known as a Discovery Data Record (DDR) (Kaczmarek, 2008 pp268). The information returned to the database from discovery over the network varies depending on the asset type; computers will return far more information than a network hub.

6.1.1 Discovery Methods

Discovery is performed using many different methods; the most important for the purpose of this research were Heartbeat (initial, default method), Network and Active Directory discovery methods. Each of these is scheduled to run and has differing features depending on the requirements of the organisation.

Heartbeat discovery is used to perform regular scheduled maintenance on the database and keep DDR records up to date (Kaczmarek, 2008 pp279). The default schedule runs this discovery weekly. To facilitate heartbeat discovery, the client package must be installed on the computers the SCCM administrator wishes to manage. Network discovery was implemented for this research after the initial installation – the researcher had to disable heartbeat discovery and enable the network discovery method instead. This involved adding the subnets in use within the WLA networks and scheduling a discovery then. Any networked device with its MAC address and details were returned on completion of the discovery. Active directory discovery was the final discovery method to update any user accounts that had not been associated with an asset previously. Active directory discovery retains user information, security group information, and system client information.

6.2 Inventory

The inventory is collected and an information hierarchy is defined within the database to hold all related information about each asset to highly granular detail levels. Fig 6.2 below shows the initial list of the assets within the domain. This report is generated through a web browser and is also available in the reports console on the SCCM server. These reports can be customised and redefined; this report is simply an inbuilt report that demonstrates all hardware, or “hardware-general” in the reporting console. The hostnames and primary domain are listed below for demonstration.

RATES-001	WEXFORD_DOMAIN
RATES002	WEXFORD_DOMAIN
RATES003	WEXFORD_DOMAIN
RATES004	WEXFORD_DOMAIN
RECEPTION	WEXFORD_DOMAIN
REGISTER_002	WEXFORD_DOMAIN
REGISTER_003	WEXFORD_DOMAIN
ROADS001	WEXFORD_DOMAIN
ROADS002	WEXFORD_DOMAIN
ROADS003	WEXFORD_DOMAIN
ROADS004	WEXFORD_DOMAIN
ROADS005	WEXFORD_DOMAIN
ROADS007	WEXFORD_DOMAIN
ROADS008	WEXFORD_DOMAIN
ROADS009	WEXFORD_DOMAIN
ROADS010	WEXFORD_DOMAIN
ROADS010	WEXFORD_DOMAIN
ROADS011	WEXFORD_DOMAIN
ROADS-020	WEXFORD_DOMAIN
ROADS-PC-001	WEXFORD_DOMAIN
ROADS-PC-002	WEXFORD_DOMAIN
ROADS-PC-003	WEXFORD_DOMAIN
ROADS-PC-004	WEXFORD_DOMAIN
ROADS-PC-007	WEXFORD_DOMAIN

Fig 6.2 – Computer names report and their primary domain

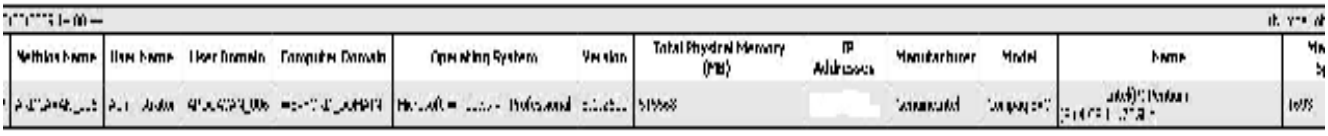


Fig 6.21 – Individual computer details, and the arrow button directly left of Netbios Name is expandable, to show more detail on the individual asset. The User Name field is used to assign ownership in this case. In the case of a server the associated service is noted in the DR plan as the owner. The discovery method to perform this initial default scan is “heartbeat” discovery described in section 6.1.1 (Kaczmarek, 2008).

6.2.1 How useful is the Inventory?

The database is only as useful as the value the organisation places on it. How useful this type of inventory is depends on the application and domain it is set within. This inventory for the purposes of the research and supporting the guidelines listed in Chapter 4 is highly useful and informative from an asset management perspective. This database enables the researcher to discover any device connected to the LAN and assign ownership of the assets discovered to individual users within the organisation. In future work beyond the scope of this research, the researcher aims to implement a system whereby each asset is linked back to a financial management system database and interconnects the assets in SCCM to the rows in requisition and purchasing tables in the FMS. In this way an exact valuation on each asset can be discovered at any given time. The research can also go in the direction of linking the service desk application, also a SQL server 2005 database into the assets in SCCM – asset owners contacting the helpdesk can see how many calls they have logged with the same piece of hardware and so on. The opportunities for implementing this SCCM solution can be explored further beyond the scope of putting in place a best practice and procedures for maintaining and securing the IT assets of the organisation.

6.2.2 Securing the inventory

The inventory, once collected can be secured using several mechanisms to ensure compliance to the framework. These include:

- Is there any unsolicited software or unlicensed software installed that places the organisation at risk? This can be measured using software compliance reporting and if any risks are identified they should be catalogued, and reported to the head of information systems – see fig 6.3 for details of software metering
- Are all computers and servers in the domain secured against potential virus attacks? Again, the software compliance can be reported against each computer to check have all client versions been updated on each asset and any risks identified, logged, and updated as priority. Each computer can be

remotely managed and a client package deployed to a client computer in a silent install where even a system restart can be suppressed.

- Have all computers in the domain been catalogued in the inventory? Computers based away from the LAN and WAN still need to be initially installed within the environs of the organisation so instances of this should be rare
- A value or weight can be attributed to high priority equipment derived using the risk management metrics described in Appendix C and a collection of critical assets can be designed as demonstrated in Figs. 6.4 – 6.. A collection is a group of assets which holds related assets depending on the meaningful name attached to the collection. As a priority, critical assets should be defined and collectively organised.

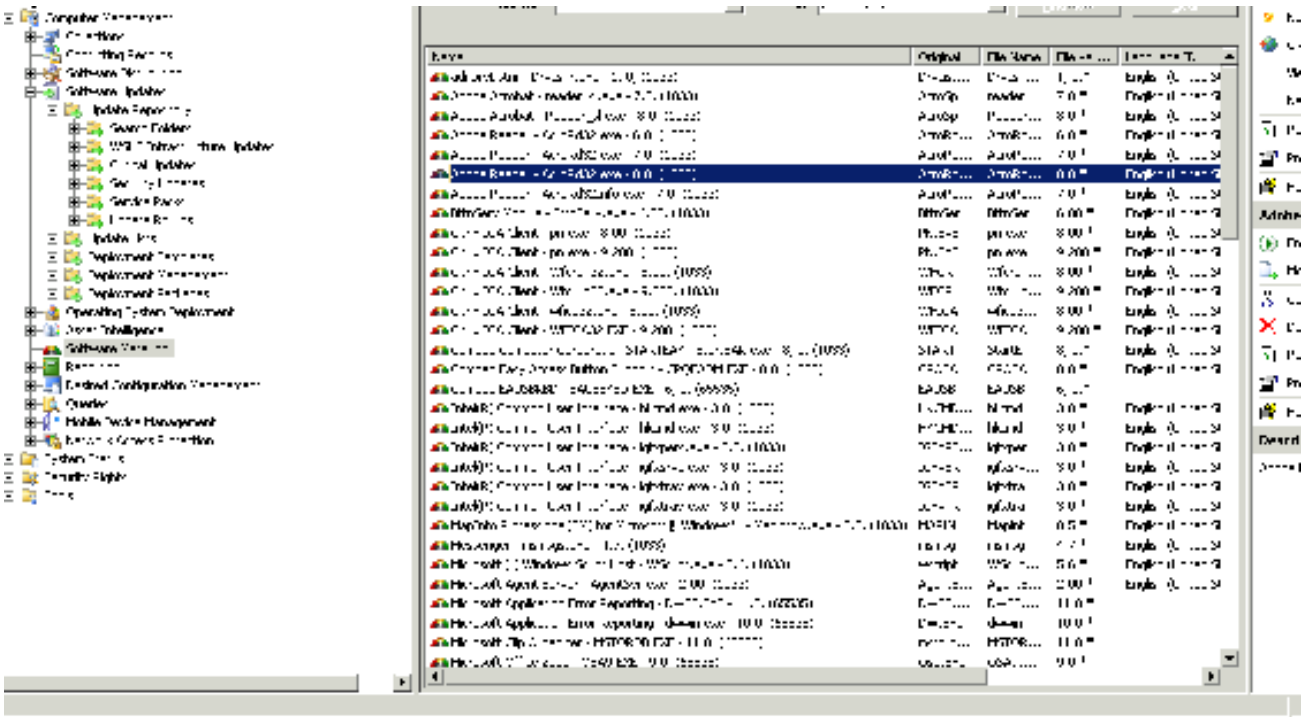


Fig. 6.3 – Software metering search for all installed exe files on assets

Fig. 6.4 Right click the collections to select new collection

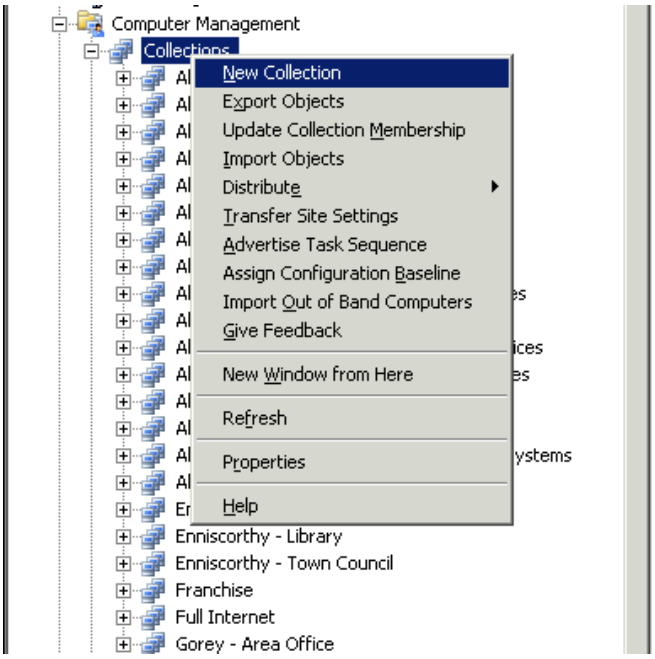


Fig. 6.5 – Name the collection

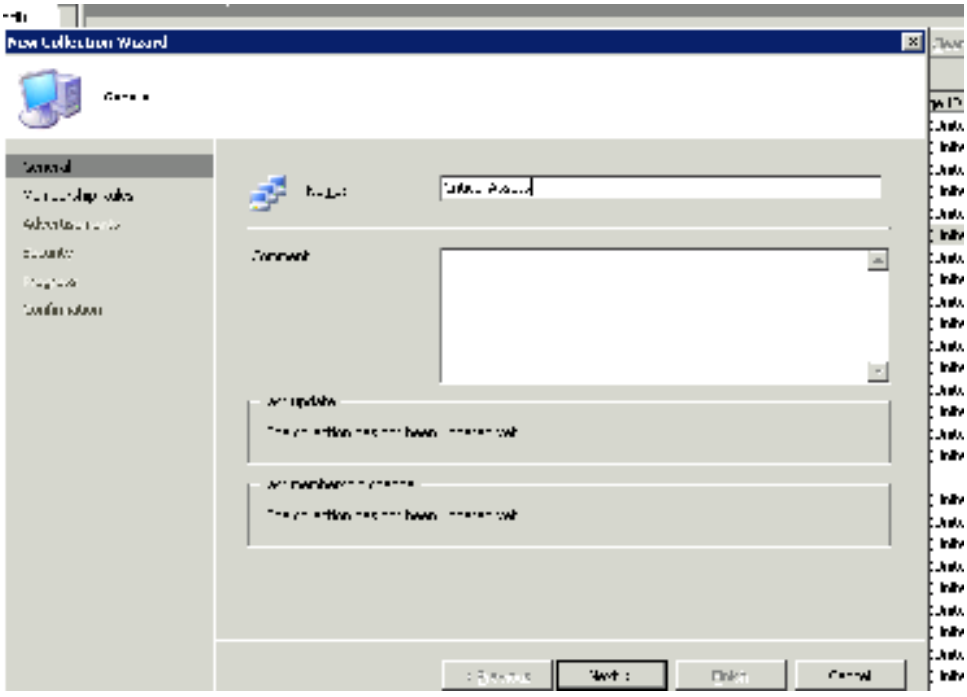
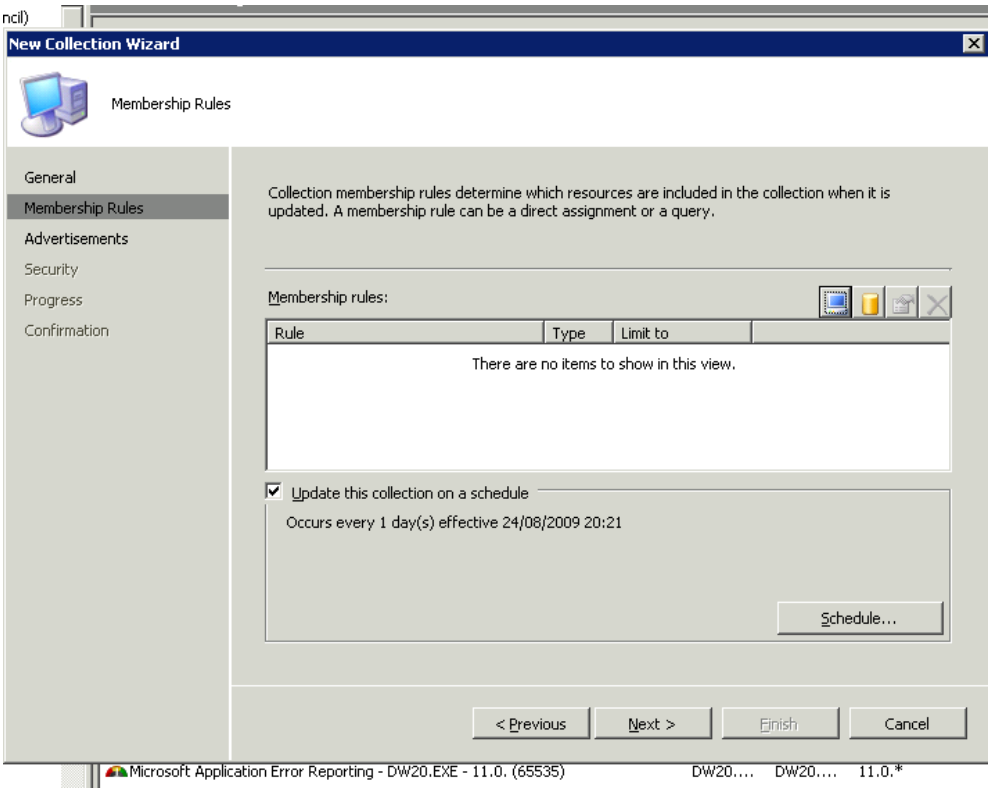


Fig. 6.6 Click computer (membership rules button) icon to add in member assets



For demonstration, the system resource, and netbios name variables have been selected, to allow all computers with finance prefix to be identified as critical assets in this example. A wild card character % can be used, as shown in Fig. 6.7

Fig. 6.8 Select a predefined collection such as all desktops and servers or all windows XP systems to populate the new collection; this will catch all assets that have been detected during the inventory phase.

Fig. 6.8

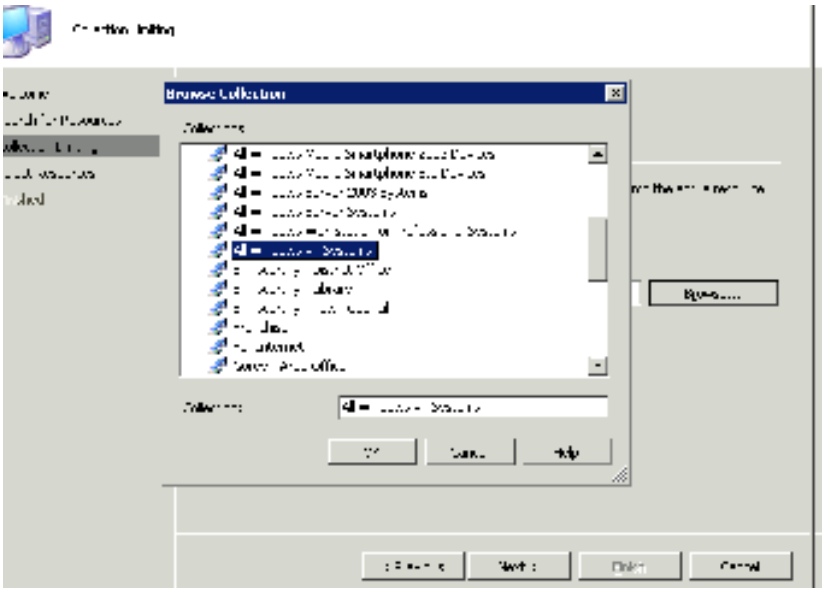
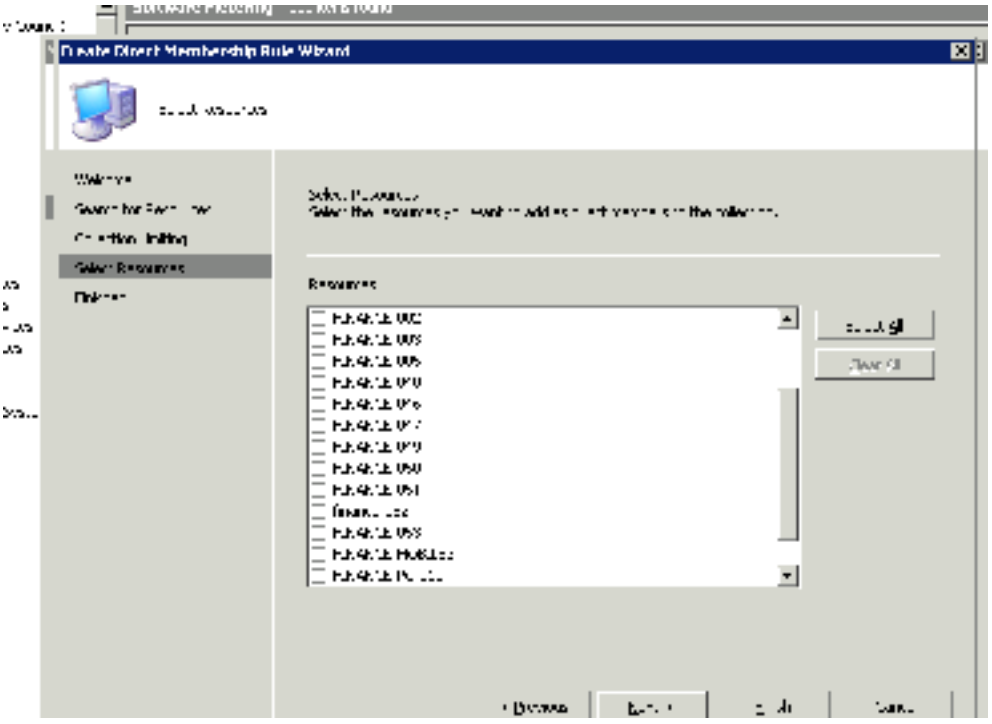


Fig 6.9 – all assets detected with the wildcard prefix can then be added to the new critical collection:



6.2.3 Creating Inventory of Networked Devices

To add an inventory of all networked devices (switches, hubs, routers, embedded printer jet direct cards), the procedure is the same except for the following details:

- Prior to creation of the collection, a network discovery must be turned on and left on for a scheduled period, 24 hours would be advisable in case there are power outages or network node lag times during the inventory phase. The administrator must enter manually the subnets in use in the domain to search, by entering the default gateway IP address for the inventory to search

- Once the network discovery has collected for minimum of 24 hours, the new collection of switches can be created for the inventory

- In the previous computer example, membership rules were set to system resource and netbios name; in the method for network device inventory, the following must be selected – system resource, then SNMP community name (it's common practice for networked devices to have an SNMP community name associating them with a particular domain or organisation)

- Once next is selected, the list should populate immediately once the network discovery was successful, and the list of devices will organically grow and contract over time as devices are added or removed

6.3 Deriving Value for Money from SCCM

6.3.1

The first point in deriving value for money with SCCM and the underlying framework is that, as stated in 1.2, licensing vendor software needs to be 100% accurate because

inaccurate figures can cost the organisation unnecessary expense either way. It also puts the organisation at higher risk when a level of incompleteness exists over the inventory. This can be assessed now, as the software metering component within SCCM inventories every .exe file on client computers in the inventory and this updates automatically via the client component deployed to each computer. Licencing can be addressed in this way, and accurate numbers mean better budgeting and better risk management from software perspective.

6.3.2

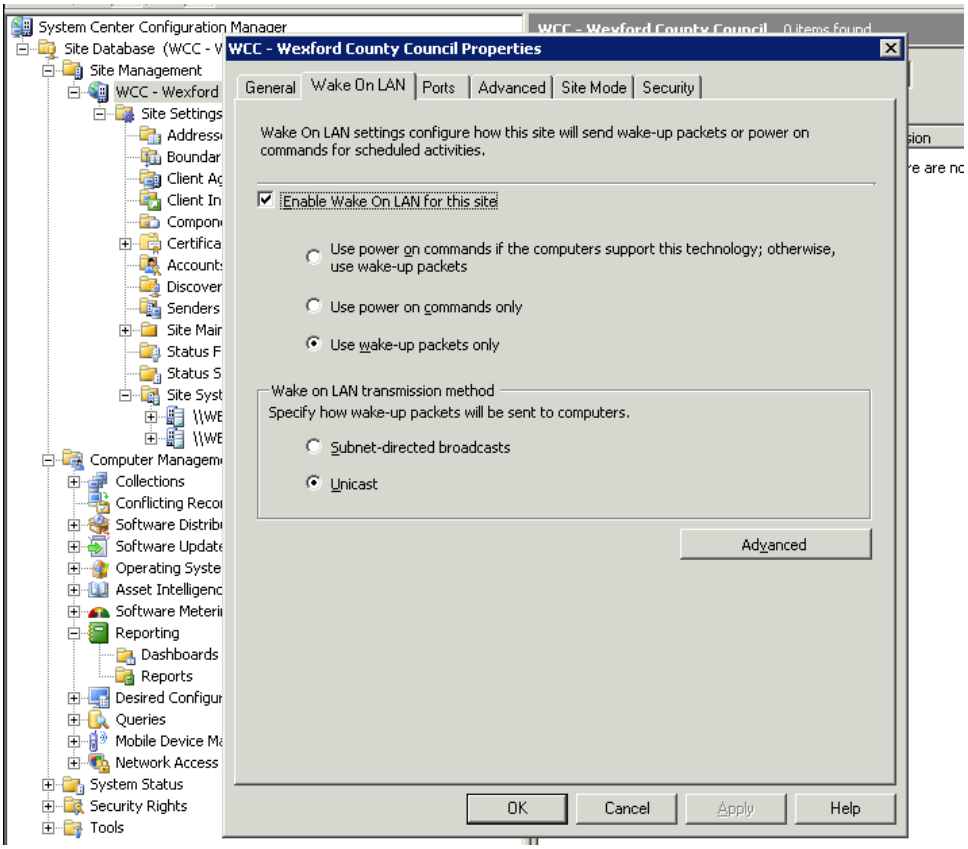
Secondly, the reporting tools in SCCM, particularly the asset intelligence and hardware reporting interfaces allow the researcher to build a list each quarter or however more frequently demanded which details all hardware in the inventory. From this inventory the contents can be customised and exported in comma separated value format so that the report can be ordered in different orientations. One simple way to budget for replacement of user hardware in an inventory has been exercised with success to date. It involves:

1. Run the hardware report on summary of computers in site
2. Run a custom report by joining physical memory custom report(set it to below a certain threshold, for instance 512MB RAM) with a report on processor type
3. Export the results to a spreadsheet (CSV file)
4. Order the file by RAM and then cross check the least amount of RAM against the processor type
5. If a computer has a P4 chip processor or dual core and is only running 256 – 512MB RAM they can be upgraded with little issue, it's far cheaper to replace RAM than needlessly replacing a computer
6. A fixed number of computers could be targeted for upgrade each quarter as standard practice, then replace/upgrade every quarter this set amount
7. Budgeting will benefit, more cost effective way of managing procurement of assets

6.3.3 Wake on LAN and Value for Money

The use of SCCM network discovery enabled the site to be prepared for remote wake up and shut down by using Wake on LAN technology. WOL works by sending a remote "magic packet" via unicast address (Kaczmarek, 2008) to all networked computers, which wakes them up at a set time.

Fig. 6.10 Configuring the site for Wake on LAN



The implementation procedure for Wake on LAN involves first defining a script to shut down any computer running Windows XP, Windows 2000 desktop or any other desktop operating system. This script was kindly shared with WCC by Neil McCleane, an ICT Consultant in the Local Government Computer Services Board, Dublin. Neil's script tells all computers in the domain to shut down except those with "noreboot" in their Active Directory computer account description field. There are two programs required for executing these scripts – psshutdown (Russinovich, 2006)

to shut the computers down, and WOL.exe (Gammadyne Technology, 2009), which facilitates the wake up of the computers.

The shutdown script is set to run as a scheduled task at 7pm every week evening as the premises close to staff shortly after this time. Each weekday (Monday-Friday) morning there is a program executed as a scheduled task at 08.20 on the SCCM server, which sends a magic packet to every computer in the domain and wakes them before employees start arriving for work at 08.25. There are huge savings experienced on electrical and power costs for the equipment being turned off for the night, and all users are now advised to shut off printers and any other devices when they leave the premises in the evening.

Chapter 7 Conclusions and Future Work

7.1 Conclusions

This research was set out initially to define a set of best practices that can be enforced and put in place in the IT Section of Wexford County Council with the idea of better managing IT assets. The research has succeeded in creating a new procedure for adding equipment to the repository, created an underlying set of best practices to reinforce the data repository functions and regarding securing the network. As a result, budgeting long-term and short-term will benefit; the methods described for assessing hardware for upgrade in 6.3.2 can be presented to the financial accounting team for approval. Risk management for the assets can be revised and refined to include IT assets down to a high level of granularity. These findings will be presented to the Administrative Officer responsible for risk management and insurance.

The main aims of the research had initial scope for computers, servers and networking devices; the research can be expanded further and evolving from this study the researcher can investigate and add methods to manage other IT assets such as fax machines, phone exchanges, and any communications related devices. There is a program in use for printer management manufactured by Hewlett Packard, called JetAdmin. This program runs a Java applet with a database at its back end, which will be investigated by the researcher to see if it can be ported into the asset repository.

7.2 Future work following on from Research

- Increase scope to take in more devices
- Integrate jet admin to SCCM for printer support
- Investigate and implement methods to manage computers on remote sites
- Refine the software metering reports generation process

References

Allen, P. (2006). *Service Orientation: Winning Strategies and Best Practices.* UK: Cambridge University Press.

Altiris Inc, (2006). *Service & Asset Management Suite Software Specification Whitepaper. USA: Altiris/Symantec Publishing.*

Bajada (2008) – Bajada, S. (2008). *ITIL v3 Foundations Certification Training.* USA: GTS Learning Courseware.

Betz, C. (2007). *Architecture and Patterns for IT Service Management, Resource Planning, and Governance: Making Shoes for the Cobbler's Children*. USA: Morgan Kaufmann Publishing.

Bosch, J. (2007). *Service Orientation in the Enterprise.* IEEE Magazine, Nov 2007. 51 – 55. USA: IEEE Computing Society

Britton, C, & Bye, P. (2004). *IT Architectures and Middleware, Strategies for Building Large, Integrated Systems, 2nd ed.* USA: Pearson Education.

Brown, W, A, Laird, R, G, Gee, C, & Mitra, T. *SOA Governance: Achieving and Sustaining Business and IT Agility.* USA: IBM Press.

Bustard, D, Kawalek, P, & Norris, M. (2000). Systems Modeling for Business Process Improvement. USA: Artech House Publishing.

Calder, A. (2008). *Corporate Governance: A Practical Guide to the Legal Frameworks and International Codes of Practice.* London UK: Kogan Page.

Calder, A. (2005). *A Business Guide to Information Security: How to Protect your Company's IT Assets, Reduce Risks and Understand the Law.* UK: Kogan Page.

Calder, A, & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002, 4ed.* London, UK: Kogan Page.

Cantor, M, & Sanders, J, D. (2007). *Operational IT Governance.* Retrieved from http://www.ibm.com/developerworks/rational/library/may07/cantor_sanders/

Cartlidge et al (2007) – Cartlidge, A, Hanna, A, Rudd, C, Macfarlane, I, Windebank, J & Rance, S. (2007). *An Introductory Overview of ITIL V3, Version 1.0.* UK: London Chapter of iSMF.

Cater-Steel, A. (2009). *Information Technology Governance and Service Management: Frameworks and Adaptations.* USA: IGI Publishing.

Central Statistics Office (CSO). *Irish Census 2006.* Retrieved from http://www.cso.ie/census/Census2006Results.htm

Chorafas, D, N. (2009). *IT Auditing and Sarbanes-Oxley Compliance: Key Strategies for Business Improvement.* USA: Auerbach Publications.

Dell Inc. (2006). *DELL Poweredge 1955 Blade Server Specification.*

DoEHLG (2000). *Local Government Value for Money Report. Department of Environment, Heritage and Local Government.* Ireland: DoEHLG Publishing.

DoEHLG (2002). *Local Government Code of Audit Practice. Department of Environment, Heritage and Local Government.* Ireland: DoEHLG Publishing.

Dorling, A. (2006). *SPICE User Group Notes.* Retrieved from http://www.isospice.com/categories/SPICE-User-Group/

Ferguson, D, Storey, T, Lovering, B & Shewchuk, J. *Secure, Reliable, Transacted Web Services.* IBM Architecture and Development Network Publishing. USA: IBM.

Friedrichs, S, & Jung, S. (2007). *New Paradigms for Next Generation E-Government Projects.* IEEE Magazine, Nove 2007, 53 – 54. USA: IEEE Computing Society.

Galup, S, Dattero, R, Quan, J, J, & Conger, S. (2007). *Information Technology Service Management: An Emerging Area for Academic Research and Pedagogical Development.* SIGMIS '07, 46 – 52. USA: ACM Press.

Galusha, C. (2001). *Getting Started with IT Asset Management.* IEEE IT Pro Magazine, May | June 2001, 37 – 40. USA: IEEE Computing Society.

Gammadyne Technology. (2009). *Free DOS Utilities – WOL Tool.* Retrieved from http://www.gammadyne.com/cmdline.htm

Greiner, L. (2007). *ITIL: The International Repository of IT Wisdom.* NW Magazine, December 2007, 9-11. USA: IEEE Computing Society.

International Organization for Standardization (ISO) & the International Electrotechnical Commission (IEC). (2005). *International Standard ISO/IEC 17799:2005, now known as ISO/IEC 27002:2007. Information Technology – Security Techniques – Code of Practice for Information Security.* London, UK: British Standards Institution.

ISACA Inc. (2006). *Ontario Pension Board – COBIT and IT Governance Case Study.* Retrieved from: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/ContentManagement/ContentDisplay.cfm&ContentID=35998

IT Governance Institute. (2007). *Cobit Framework 4.1.* Illinois, USA: IT Governance Institute Publishing.

Jackson, L, A & Al-Hamdani, W. (2008). *Economic Acceptable Risk Assessment Model.* InfosecCD Conference '08. USA: ACM Press.

Kazcmarek, S, D. (2008). *Microsoft System Center Configuration Manager 2007.* Seattle, WA, USA: Microsoft Press.

King, C. (2006). *How Much Does IT Cost : How to Estimate the Time and Cost of Implementing IT Asset Management.* Minerva Enterprises Financial Management Magazine, 2, 4. USA: Minerva Enterprises.

Klosterboer, L. (2008). *Implementing ITIL Configuration Management.* USA: IBM Press.

Laplante, P, A, & Costello, T. (2006). *IT Best Practices: CIO Wisdom.* IEEE IT Pro, January|February 2006, 17-23. USA: IEEE Computing Society.

Leedy, P, D, & Ormerod, J, E. (2005). *Practical Research: International Edition, 8ed.* New Jersey, USA: Pearson Prentice Hall.

McShea, M. (2007). *Communicating IT's Value in a Modern Business Climate.* IEEE IT Pro Magazine, January|February 2007, 42 – 45. USA: IEEE Computing Society.

Microsoft Corporation. (2007). *Microsoft Official Course: 2780B. Maintaining a Microsoft SQL Server 2005 Database.* USA: Microsoft/MSDN Press.

Microsoft Corporation. (2008). *System Center Configuration Manager Asset Intelligence Whitepaper.* USA: Microsoft Corp Publishing.

Office of Government Commerce (OGC). (2009). *PRINCE2 Methods.* Retrieved from http://www.ogc.gov.uk/methods_prince_2.asp

Ontario Pensions Board. (2006). *Engaging in Good Governance.* Retrieved from http://www.opb.ca/portal/ShowBinary?nodePath=/OPBPublicRepository/OPB/Publications/Shared/Booklets/en/Engaging In Good Governance

Pengelly, J. (2005). *ITIL Service Level Management.* London, UK: GTS Learning.

Redman, T, C. (2008). *Data Driven: Profiting from Your Most Important Business Asset*. USA: Harvard Business Press.

Russinovich, M. (2006). *PSShutdown V2.52 Documentation.* Retrieved from http://technet.microsoft.com/en-us/sysinternals/bb897541.aspx

Senft, S, & Gallegos, F. (2009). *Information Technology Control and Audit, 3ed.* USA: Auerbach Publications.

Sisco, M. (2002). *IT Asset Management. USA: MDE Enterprises Inc.*

Tiako, P, F. (2009). *Designing Software-Intensive Systems: Methods and Principles.* USA: IGI Publishing.

Tillquist, J & Rodgers, W. (2005). *Using Asset Specificity and Asset Scope to Measure the Value of IT*. Communications of the ACM January 05, 48, 1, 75 – 80. USA: ACM Press.

Tipton, H, F, & Krause, M. (2007). *Information Security Management Handbook, 6ed.*. Florida, USA: Auerbach Publications.

Wexford County Council. (2004). *Staff Communications Policy*. Ireland :Wexford County Council.

Wexford County Council. (2008). *Corporate Procurement Plan 2008-2010*. Retrieved from http://www.wexford.ie/wex/YourCouncil/Publications/Policies/Thefile,7456,en.pdf

Wexford County Council. (2004). *Corporate Plan 2004-2009*. Retrieved from http://www.wexford.ie/wex/YourCouncil/Publications/CorporatePlans/Thefile,515,en.pdf

APPENDIX A

The following fields are used in the existing Microsoft Access database, and the fields marked with an (r) are the fields to be retained in the new SCCM based regime for asset management.

Asset Number – an automatically generated unique identifier number from the database
Asset Type* *(r)*

Serial Number (r) – maintained in new asset repository; the vendor serial number for warranty information
Product Number (r)– the vendor product range identifier; maintained in new asset repository

Computer Name (r) –Netbios name for identification on the network. This was previously assigned using the section and a number depending on the next available number, e.g. IT-001 and so on; maintained in new asset repository

Make (r)- Manufacturer; maintained in new asset repository

Model (r)– any other model details; maintained in new asset repository

User (r)– Person accountable for or main user of the asset (in the new framework deemed the "owner" of the asset) maintained in new asset repository

Username (r) – domain username – replacing user

Section (r)– Organisational unit (OU) the asset is assigned to, which will be specified, see Chapter 6, section 6. for details of how computers are arranged by location

Location (r) – Location within the organisations environs and area; maintained in new asset repository, but identified by OU

IP Address (r) – not required, this was previously required when static IP addresses were issued but Dynamic Host Configuration Protocol is now in use enforcing a 3 day lease on each IP address maintained in new asset repository in the capacity that SCCM reporting retains the last used IP address for a piece of equipment, regardless of it being a leased or a reserved DHCP address

Operating System (r)– manual entry not required as the System Center Configuration Manager database will host this information
MAC Address (r) – manual entry not required as the System Center Configuration Manager database will host this information

Carepack Number / Warranty – if associated extended warranty has been purchased – store details of this in spreadsheet linked to FMS but do not retain in current SCCM solution

Carepack / Warranty Expires – expiration date of the extended warranty

VT320 License Number – terminal services software, licencing was a serious issue within the domain, and this needed to be monitored. The software is now almost completely phased out.

Date Installed – date of installation at destination.

Notes

*Note - Asset Type Pc, Printer, Screen, Laptop, Scanner, Server, Router, Switch, Hub, Camera, PDA

APPENDIX B

Information Classification

ISO Objective: "To ensure that information receives an appropriate level of protection" (ISO, 2007 pp21)

Classification of information in the organisation is dictated by many variables. To calculate the classification for each and devise a set of meaningful categories, several controls should be implemented to ensure accuracy and maintain just enough detail without overcomplicating the matter. Each business need varies and so a different classification can be applied to the information generated by and input to each business need (Calder & Watkins, 2005).

"Owners should make decisions about classifying information and systems and protecting them in line with this classification" (ITGI, 2007 pp42).

Responsibility for calculating the class of information or information asset should be shared between IT representatives - most likely a senior technical services team member, the officer charged with management of risk assessment in the finance section, and each asset's owner or owners. If any radical changes or new services are introduced that increase the value attributed to a particular asset, it is up to the owner to inform the risk assessment officer and IT representative of this. As soon as a business function is added or removed from an information asset the asset's classification should be modified. The criticality of the asset to the business fluctuates when functions performed using the assets fluctuate.

The following should be assessed regularly to decide how to classify information and information assets:

1. Value of the information/asset
2. Is the information/asset legally required?
3. Are there extra risks to the information due to information sharing?
4. Is the information constantly in demand from customers/users?

5. Do external consultants access the information/assets?
6. How sensitive is the information?
7. How critical to the daily business activities is the information?
8. Does the information contribute to one or many applications? (ITGI, 2007 pp33)

The CobiT framework (ITGI, 2007 pp34) also advises on the creation and regular maintenance of an enterprise information architecture model to reflect all of the systems, applications, information sharing and how business activities relate to these. Other recommendations that should be implemented in best practice for information classification are the creation and upkeep of an enterprise data dictionary which incorporates business rules and has constraints assigned to it so that all applications and user defined data elements are designed to be shared in the same format (ITGI, 2006 pp34). One extra point for classification of information raised by the CobiT (ITGI, 2007 pp34) is the area of archiving and encryption which are extremely useful controls for applying to information that is either obsolete but legally required, and highly sensitive data. The classification scheme should be a combined effort between management, IT management and finance management to facilitate creation of a universal enterprise data dictionary.

A classification scheme should be introduced as a manner of measuring sensitivity of data, and an appropriate Access Control List schema should be implemented at domain and group policy level for each organisational unit and staff grades. Three such categories could be “Confidential, Restricted, and Private” (Calder & Watkins, 2008).

APPENDIX C

Proposed Risk Assessment Methodology for submission to Finance Office

The following observations have not been included in the main research because there are already risk management metrics and methodologies in place in the organisation devised by the Finance section. Risk assessment is a legal requirement of the internal audit framework in place already so these proposed modifications to how IT assets are assessed should benefit the organisation and make the audit process even more transparent. These proposed metrics for measuring IT asset risks are part of the research, but a dedicated Administrative Officer within the organisation is already charged with risk assessment and handling of company insurance so the research may or may not be implemented.

The four objectives for general risk management outlined by Calder & Watkins (2008) are:

1. elimination of risks
2. reduction of risks that cannot be eliminated to manageable levels or considered sufficiently low
3. to elicit control over the manageable tolerated risks to maintain their status as acceptable
4. transfer where possible of risks via insurance to become another organisations' responsibility

The recommended management metric for risk assessment involves measuring the level of impact a risk can cause to a company asset and then devising thresholds to adhere to when measuring potential impact (Calder & Watkins, 2008). The level of risk assessment depends on the business area each organisation is involved in. The following observations are the recommendation to the Finance Administrative Officer regarding IT assets:

- A designated member of IT staff should be delegated to calculation of risk assessment and formulating how this risk assessment can be implemented as part of the corporate plan

- "Senior corporate officers" (ITGI, 2007 pp6) should be made aware of and understand the risks and responsibilities toward these information and asset related risks

- Once the member of IT staff is identified, adequate professional risk management training should be a priority for this individual

- A member of the IT security staff or technical services team should liaise with the IT risk management delegate. The risk management scheme for information should overlap with the corporate risk management plan.

- There are a number of risk assessment and management tools certified by the ISO and BSI (Calder & Watkins, 2008), these should be considered for implementation

With the points discussed and researched in this Appendix, the following is the Recommended Procedure for Risk Analysis for submission to the Finance Section (Calder & Watkins, 2008), and Senft & Gallegos, (2009):

- Develop a risk management plan, and devise this using relevant staff, this plan needs to be flexible and open to modification as regulations change

- Assess and define the scope for the IT asset risk management plan clearly – what constitutes an IT asset?

- Perform “quantitative” risk analysis – using probability formulae calculate the possibility of an event occurring, then correlate with likely loss incurred by the event

- A potential loss cost is calculated by multiplying potential loss in monetary terms by the percentage probability of the event occurring, a decision as to the importance of the risk is made if the result is high or low; high being more serious to the organisation

- A map of how risks interrelate should be drawn up, but care must be taken not to allow the list to become too complex

- Identify changes quickly in risk areas – if a particular asset changes specification by upgrade or has more confidential data stored on it, the risk status changes

- Identify new risks quickly – if a discovery is made such as a server not connected to an uninterruptable power supply, this is a new risk, and risk management should account for it

- Manage compliance to legal requirements efficiently – auditors and government departmental requirements constantly change, particularly with data retention and information classification, these need to be monitored by owners of assets, IT management and internal audit staff

- Use the best physical security to minimise physical risks; use a sign in log book of any works in the premises and request identification and papers confirming any works on data or assets

- Secure networks against internal attack by using controls such as permission lists and access control

- Always use audit results to modify and improve risk assessment

- Categorise risks according to the weighting system suggested by Senft & Gallegos, (2009):

    1. Critical assets, where loss of assets would incur severe monetary and reputation loss or even result in bankruptcy
    2. important – damaging and the organisation could struggle to fund replacement of the asset/information
    3. unimportant – replaceable

APPENDIX D

Installing and configuring Microsoft SCCM for implementing the research is detailed in this appendix.

Hardware Used:

The hardware used to run both the SCCM installation and the Microsoft SQL Server 2005 database were both DELL Blade Poweredge 1955 servers (Dell, 2003). The SQL database server is also connected via HBA fiber optic cables to an IBM DS3400 SAN unit which hosts the log files and backups before they are backed up to disk as part of the nightly DR procedure. There were several prerequisites on both the SQL server and the windows server hosting the SCCM installation that had to be prepared in advance of installation and setup of the database. Static IP addresses were assigned to each piece of hardware and the SQL server database hosts other databases along with the SCCM back end database so it was critical that the installation be performed during a quiet time. The database server had to be rebooted twice before the installation completed which meant that the service desk (helpdesk) and several other dot net applications were unavailable until the server reloaded. The installation was initiated and supervised by Neil McCleane and Jim Connolly, both ICT Consultants with the Local Government Computer Services Board.

Issues noted during initial install

SQL server required SP2 for the SCCM database to be created; SP2 was not initially deployed to the server so this was the first installation necessary. This is where the first problem was encountered in the domain. The structure of the architecture in place is:

- A SAN unit used to house the log files and bak files for SQL Server
- The system databases (master, model, msdb, distribution and others) had been relocated to a partition mapped to the SAN unit

Because of this last point, the SQL database engine would not restart when the SP2 installation and system restart had been completed. Microsoft technet forums revealed that SQL server will not function post SP2 install if the system databases have been moved away from the partition that houses the initial SQL server installation, in this case the C:\program files folder. The system database locations had to be moved manually back to their original container on the C: drive of the server and a restart was necessary to begin the SCCM installation. The database architecture fulfilled the prerequisite of minimum SQL Server 2005 Standard Edition SP2. The full client components suite is installed on the server and not on client computers within the site, so a console or remote desktop session needs to be established under the correct credentials to open the SQL Server management console.

Prerequisites for SCCM are categorised between site server prerequisites, database server prerequisites listed above, console prerequisites, client installation prerequisites, and finally configuration manager setup prerequisites. In more detail these contain: (Kaczmarek, 2008 pp31-39)

1. Database server prerequisites – MS SQL Server 2005 Standard Ed or higher, running SP2
2. Site server prerequisites – all of the computers to be managed in the site must be part of a windows server 2000 (minimum) active directory domain. Both the IIS and BITS server components had to be installed on the server also from add/remove windows components before commencing installation.

3. For this research, the architecture was windows server 2003, and

    - A single server was used for the install of the site server, following the best practice offered by the vendor
    - minimum of .NET 2.0 installed
    - IE 5 or later installed

- IIS 6.0 or later installed on the server

3. Configuration manager console prerequisites –

   - Windows XP pro sp2 or any later operating system
   - Microsoft management console is installed, v3.0
   - Minimum of .NET framework 2.0 installed

4. Client installation prerequisites –
   - There is a library of approx 88 files to be downloaded before the client installation can be pushed out across the site, containing cab files, xml files and Windows Management Instrumentation (WMI) updates so the client computers can be contacted and browsed/managed by the server.

Installation Options Selected for the Research

The server software was installed as a single configuration management server for the site, code WCC, and there are no partitions on the server. For disaster recovery, the server is part of a 10 server array of blades that are managed by an Altiris server. The Altiris server takes an image each night of the server and dumps it to a file repository on the network, and this is backed up to LTO tape. The software is installed on the C: drive of the server, and all the associated kits, windows updates and client software packages are housed on the D: drive of the server. There is a hidden share for deploying the client updates to each computer so they can be managed by the configuration manager.

When installing the software, the following options were selected for the reasoning explained with each point:

- The site is running in Mixed Mode, and this was selected because the domain to be managed still has client computers and servers running the Windows 2000 and Windows Server 2000 operating systems, these are fully supported within Mixed Mode.

- Update check was run beforehand as the software release had not been checked for up to date libraries

- The server is the only server in the site and so is set as primary site

- Using the setup wizard, a custom install was deployed because the credentials associated with the SQL server instance had to be manually entered

- The site was named WCC to represent the organisation and is the only site within the county's network

- If the national root domain in Dublin decides to implement a main site to manage the countrywide sites, mixed mode will enable the server to be managed

- Software & hardware inventories, ability to deploy advertised programs as updates, windows updates, software metering for compliance , remote tools and configuration management were all taken options as each feature would be used to back up the points proposed in the framework

- Ports to be opened for the server were 80 for HTTP client requests, 443 to support HTTPS protocol communication, and Port 9 had to be opened to allow Wake on LAN (see Appendix E) to be configured to shut down and

wake up client computers remotely and implement proper power management

- Computers when added to the domain are deployed the client configuration package and are then approved as members of the domain once passed by the administrator

- There are no planned secondary sites as of yet

APPENDIX E VB Script to Shutdown all Computers in Domain Provided by Neil McCleane, LGCSB

```
'#####################################################################
############
' THIS IS A SCRIPT TO SHUTDOWN ALL VISTA XP AND 2000 CLIENTS IN
CURRENT DOMAIN (OU=IT Lab)
' note: there is an exception if "NOREBOOT" is in place in the
description field
'               of the computer AD account
'
' UPDATED BY NEIL MCCLEANE 31/10/2008
'#####################################################################
############

Const ADS_SCOPE_SUBTREE = 2
Const ForAppending = 8

On Error Resume Next

'       #### NAME text file for appending
FileLog = "C:\ScriptLog_ShutdownComputers.txt"

'       #### CREATE text file for appending
Set objFSO = CreateObject("Scripting.FileSystemObject")
objFSO.CreateTextFile(FileLog)
Set objTextFileLog = objFSO.OpenTextFile(FileLog, ForAppending)

'       #### Find out the current domain
Set WshShell = WScript.CreateObject("wscript.shell")
strDomain = WshShell.ExpandEnvironmentStrings("%USERDNSDOMAIN%")
n = InStr(strDomain, ".")
strDom1 = Mid(strDomain, 1 , n-1)
strDom2 = Mid(strDomain, n+1 , n+99)
'Wscript.Echo "LDAP://OU=,DC=" & strDom1 & ",DC=" & strDom2
strDNSDom = "LDAP://OU=,DC=" & strDom1 & ",DC=" & strDom2

Set objConnection = CreateObject("ADODB.Connection")
Set objCommand =   CreateObject("ADODB.Command")
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"

'       #### Places all Vista XP and 2000 Pro computers where
description field does not equal "NOREBOOT" into array
Set objCommand.ActiveConnection = objConnection
objCommand.CommandText = _
    "Select Name, operatingSystem, operatingSystemServicePack from "
& "'" & strDNSDom & "'" & _
    " where objectClass='computer' and description<>'noreboot'" & _
            " and ((operatingSystem = 'Windows XP*') or
(operatingSystem = 'Windows 2000 Professional*') or (operatingSystem
= 'Windows Vista*'))"
objCommand.Properties("Page Size") = 10000
objCommand.Properties("Searchscope") = ADS_SCOPE_SUBTREE
Set objRecordSet = objCommand.Execute
objRecordSet.MoveFirst

Set objShell = CreateObject("WScript.Shell")

Do Until objRecordSet.EOF
```

```
    strCommand = "%comspec% /c ping " &
objRecordSet.Fields("Name").Value
    Set objExecObject = objShell.Exec(strCommand)
    strText = objExecObject.StdOut.ReadAll
    n = InStr(strText, "[")
    m = InStr(strText, "]")

    If Instr(strText, "Reply") > 0 Then
        'Wscript.Echo objRecordSet.Fields("Name").Value & ", " &
objRecordSet.Fields("operatingSystem").Value & ", "_
        '& ", " & Mid(strText, n +1 , m - n -1) & ", reachable by
ping & SHUTDOWN attempted."
        '       ##### write to log file with all succeeding pinging
computers
        objTextFileLog.WriteLine(objRecordSet.Fields("Name").Value &
", " & objRecordSet.Fields("operatingSystem").Value & ", "_
        & Mid(strText, n +1 , m - n -1) & ", reachable by ping &
SHUTDOWN attempted.")
        '       ##### call the sub function
        ShutdownComp

    Else
        'Wscript.Echo objRecordSet.Fields("Name").Value & ", " &
objRecordSet.Fields("operatingSystem").Value & ", "_
        '& ", " & Mid(strText, n +1 , m - n -1) & ", COULD NOT BE
REACHED."
        '       ##### write to log file with all failing pinging
computers
        objTextFileLog.WriteLine(objRecordSet.Fields("Name").Value &
", " & objRecordSet.Fields("operatingSystem").Value & ", "_
        & Mid(strText, n +1 , m - n -1) & ", COULD NOT BE REACHED.")

    End If

    objRecordSet.MoveNext
Loop

'=====================
'= Shutdown computer =
'=====================
Sub ShutdownComp ()
    strCommand1 = "%comspec% /c psshutdown -f -c -k -t 300 -m " &
Chr(34) & "!!!WARNING!!! THIS MACHINE WILL POWER OFF IN 5 MINUTES" &_
     Chr(34) & " \\" & objRecordSet.Fields("Name").Value
    Set objExecObject = objShell.Exec(strCommand1)
End Sub
```

APPENDIX F

COMMUNICATIONS POLICY
WEXFORD LOCAL AUTHORITIES
VERSION 1.2 - March 2004.

Policy on Communications

Scope

This policy applies to all electronic communications systems provided by Wexford Local Authorities including, but not limited to internet, intranet, e-mail, personal computers and laptops, analogue telephones, mobile telephones and fax machines. It is the responsibility of both management and staff of the Local Authority to ensure that all such tools are used in accordance with this policy.

All users are expected to use common sense and to conduct themselves in a manner, which is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of the Local Authority under many enactments including, but not limited to the following:

- Employment Equality Act, 1998
- Equal Status Act, 2000
- Data Protection Act, 1988 & 2003
- Freedom of Information Act, 1997
- The Companies Acts 1963 - 2001
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1990

Other documentation that is relevant to this policy includes the Local Authority's policies and procedures on:

- Grievance and Discipline
- Harassment and Sexual Harassment
- Bullying in the workplace
- Equality and Diversity

General Computer Usage

1. Security and Passwords

All equipment provided by Wexford Local Authorities' for use by staff remains the property of the Authority. Employees must not remove any such equipment (computers, laptops, mobile telephones, etc.) from the Authority's premises without prior authorisation from their Town Clerk, Section Head and/or Head of Information Systems/I.S. Department as appropriate.

It is the user's responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

Users must not engage in conduct which interferes with other's use of shared computing resources and/or the activities of other users.

Users must not utilise any other person's access rights or attempt to gain access to resources or data for which authorisation has not specifically been granted. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.

No staff member may misrepresent himself / herself as another individual.

Passwords must remain confidential to each user and must not be relayed to any other person. The IT Department may provide the option to alter any passwords as necessary. Each user carries sole responsibility for security access to his/her computer.

2. Software Ownership

All software which is provided by any Wexford Local Authority to an employee is licensed and owned by the organisation and may not be downloaded, stored elsewhere or transferred to another individual by any employee of the local authority. No software may be downloaded from the Internet and used on the Authority's machines without prior authorisation from the Head of Information Systems or Authorised Officer. Any breach of these requirements may result in disciplinary action in accordance with the grievance and disciplinary procedure.

3. Confidentiality.

When a user registers with a site or a service in the name of the local authority the resulting spamming of information may tie up the authority's communications system. Therefore, to avoid the release of confidential Local Authority information to third parties and to avoid interference with the communications systems, users must not register with an electronic service over the website without prior permission from their Line Manager and from their I.T Department.

Users must maintain confidentiality while carrying out their duties and while on Local Authority business.

4. Legal implications of storing electronic data.

All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include but are not exclusive to Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation.

All data must be stored in an up-to-date format. Personal information may contain only information relevant to the individual and to the purpose for which it is being stored. Data must not be used for any other purpose. This data must be maintained in an accurate format and must be altered if the user/authority becomes aware of inaccuracies.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Employees should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by the employer and / or disclosed to third parties.

5. Monitoring Policy

It is the policy of Wexford Local Authorities to monitor e-mail content and Internet usage on behalf of all employees in order to protect the Authorities and their employees from liability under equality, data protection, pornography and copyright legislation. This does not constitute infringement of any individual rights to personal privacy under the Data Protection Acts 1988 and 2003.

6. Virus Protection

Viruses can enter an organisation a number of different ways:

(a) On diskette or CD from an external source, particularly “home PC’s”.
(b) Via email (usually an attachment).
(c) By browsing certain Internet sites or by downloading infected files.
(d) From infected laptops / notebooks that are brought into the organisation.

All desktop and laptop/notebook computers connected to the Local Authorities’ LAN must have appropriate anti-virus software installed on them. This software must be enabled and have up-to-date “signature” files. Therefore, you must not introduce C.D, diskettes, downloaded files or personal laptops/notebooks without first getting clearance from the I.T. department in consultation with the appropriate Director of Service(s) and/or Section Head. Please contact the IT Helpdesk for further details on this.

7. E-mail

Many employees have a personalised e-mail account to facilitate the sending and receiving of business messages between staff and between the Local Authorities and their clients and suppliers.

Risks associated with e-mails.

- Messages can carry viruses that may be seriously damaging to the Local Authorities' systems.
- Letters, files and other documents attached to mails may belong to others and there may be copyright implications in sending or receiving them without permission.
- It has become increasingly easy for messages to go to persons other than the intended recipient. If E-mail messages contain confidential or commercially sensitive information, this could be breaching Wexford Local Authority's security and confidentiality.
- E-mail is speedy and, as such, messages written in haste or written carelessly may be sent without the opportunity to check or rephrase. This could give rise to legal liability on the part of the Local Authority.
- An e-mail message may legally bind the Local Authority contractually in certain instances without the requisite/appropriate internal authority/approval.
- All personal data contained in e-mails may be accessible under Data Protection legislation and, furthermore, non-personal and personal data may be accessible under Freedom of Information legislation.
- E-mails should be regarded as potentially public information which carry a heightened risk of legal liability for the sender, the recipient and the organisations for whom they work.

Rules for e-mail use

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly any written, stored or forwarded and disseminated information must adhere to the guidelines within the Data Protection and the Employment Equality legislation and in accordance with the equality policy of Wexford Local Authorities.

In order to avoid or reduce the risks inherent in the use of e-mail within the Local Authorities, the following rules must be complied with:

♦ The following signature format and text must appear at the end of every e-mail sent from your Local Authority address to a recipient external to the Local Authority's domain.

Name & Title
XYZ Local Authority
E-mail: *abc@xyzcoco.ie*
Web: *http://www.xyz.ie*
Ph: *Number*
Fax: *Number*
****

This message is intended only for the use of the person(s) ("the intended recipient(s)") to whom it is addressed. It may contain information which is privileged and confidential within the meaning of the applicable law. If you are not the intended recipient, please contact the sender as soon as possible. The views expressed in this communication may not necessarily be the views held by Wexford Local Authorities.

Any attachments have been checked by a virus scanner and appear to be clean.
Please ensure that you also scan all messages as Wexford Local Authorities Do not accept any liability for contamination or damage to your systems.
****

- The Local Authority name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation. Therefore, e-mail messages must be appropriate and professional.

- Correct spelling and punctuation should be maintained in all communications.

- E-mail is provided for business purposes.

- Occasional and reasonable personal use of e-mail is permitted provided that

  1. This does not interfere with the performance, work duties, responsibilities and customer service of the Local Authority,
  2. It does not support any business other than the Local Authority and
  3. It otherwise complies with this policy.

- An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or

other inappropriate remarks whether in written form, cartoon form or otherwise is forbidden.

- E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.

- Any e-mails received from an unsolicited or unknown source must be reported to the IT Department to be checked for viruses prior to opening.

- Distribution lists may only be used in connection with Council business. There may be a few exceptions to this as authorised by the IT Department (e.g. Sports & Social Club notices), but for all other mails, names must be selected individually.

- Particular care should be taken when sending confidential or commercially sensitive information. If in doubt please consult your Section Head.

- Care should also be taken when attaching documents as the ease with which employees can download files from the Internet or 'cut and paste' materials from electronic sources increases the risks of infringement of the rights of others particularly to copyright, intellectual property and other proprietary rights.

- Where important, you should obtain confirmation that the intended recipient(s) have received your e-mail.

- Documents prepared internally for the public or for clients may be attached via the e-mail. However, excerpts from reports other than our own, may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt consult your Section Head.

- Do not subscribe to electronic services or other contracts on behalf of the Local Authority unless you have express authority to do so from the appropriate Director Of Service(s) in consultation with the Head of Information Systems.

- If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your Town Clerk, Section Head or HR Department as appropriate.

- Chain mails or unsuitable information must not be forwarded internally or externally.

- The Local Authority reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.

- Notwithstanding the Local Authority's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior written approval from the employer. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message.

8. The Internet/Intranet

Access to the Internet / intranet is provided to staff as necessary solely for the purpose of conducting Local Authority business.

Rules for internet use

- The Local Authority's Internet connections are intended for activities that either support the Local Authority's business or the professional development of employees. Web surfing or internet access unrelated to these activities is strictly forbidden.

- General internet access will only be provided to authorised personnel. Authorised personnel will have responsibility for Internet access under their account and hence will also have responsibility for illicit use of their account with or without their consent.

- Internet usage is monitored on a systematic basis and as deemed necessary by the Local Authority.

- If you have any doubt as to the content of any item you wish to download you should contact the I.T. Section.

- Internet use is not permitted for personal gain or profit, to represent yourself as someone else, or to post or download messages that contain political views, or contrary to the ethics and other requirements of the Local Government Act 2001.

- It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom.

- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom.

  If an employee is downloading pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment by offended parties. Such incidents should be reported to the relevant authority. Apart from any potential offence caused and the inappropriateness of such activity, the Local Authority may be vicariously liable for any claims arising from such behaviour.

Because of the serious criminal implications of accessing child pornography, any employee found to be accessing such information may be summarily dismissed and the matter referred to An Garda Síochána. Furthermore, should an employee be prosecuted under the Child Trafficking and Pornography Act, 1998, by engaging in such activities outside the remit of the workplace, the Local Authority may find it fitting to invoke disciplinary action.

- The internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.

- The internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.

- Public messaging systems on the Internet must not be used by staff save with the prior written permission of the appropriate Director of Service(s) in consultation with the Head of Information Systems. Public messaging systems include user groups, chat rooms, special interest forums and bulletin boards.

9. Laptops and remote computers

The rules applying to use of the internet and e-mail messaging systems apply also to any laptops, remote computers or other electronic processors in use by the staff member and supplied by the local authority. Express permission must be obtained from the relevant authority to remove such equipment from the Local Authority

premises. All such equipment will be subject to the same monitoring procedure as that which is retained on-site.

10. Telephone Usage

Access to telephones is intended for Local Authority purposes only. While reasonable making and taking of personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. The Local Authority reserves the right to monitor the use of the telephone system.

Personal mobile telephones must be switched off during normal business hours. Some mobile phones are provided to staff members for Local Authority business. Personal calls from such phones are generally not permitted, and where such personal calls are necessary staff should seek to use an analogue telephone where possible.

11. Other Electronic Tools

Other electronic equipment (e.g. fax machines, photocopiers etc.) remains the property of the Local Authority and as such must be treated with care and used only for Local Authority purposes. Abuse of equipment for personal use or gain may result in disciplinary action in accordance with the grievance and disciplinary procedures.

12. Infringements of Policy

Any staff member abusing this policy may be subject to use of the disciplinary procedures and disciplinary action, up to and including dismissal. Serious breaches of policy may result in criminal or civil charges being brought against individuals.