LAUREA

Maturity modelling as a catalyst for IT continuity management implementation in a large company

Syrjänen, Kimmo

2009 Leppävaara

Laurea University of Applied Sciences
Espoo Institute

Maturity modelling as a catalyst for IT continuity management implementation in a large company

Kimmo Syrjänen
Information Systems
Thesis
December 2009

Laurea-ammattikorkeakoulu Tiivistelmä
Laurea Leppävaara
Ylempi ammattikorkeakoulututkinto
Tietojärjestelmäosaaminen

Kimmo Syrjänen

Kypsyysmalli jatkuvuussuunnittelun käyttöönoton katalyyttinä suuressa yrityksessä

Vuosi 2009 Sivumäärä 60

Opinnäytetyöni kuvaa jatkuvuuden hallinnan kypsyysmallin sekä esittää kypsyysmallin käytön konkreettisia hyötyjä organisaatiolle, joka on suuri suomalainen teknologia-alan yritys. Koska kohdeyrityksen toiminta on erittäin riippuvainen informaatiojärjestelmäpalvelujen saatavuudesta, panostaa se merkittävästi jatkuvuussuunnitteluun osana toiminnan turvaamista. Jatkuvuussuunnittelun tehtävä on tunnistaa liiketoiminnan tarpeet ja tarjota sellaisia ratkaisuja, jotka varmistavat liiketoiminnan jatkuvuuden vaikka tietojärjestelmään kohdistuisi merkittäviä häiriöitä ja tuhoja. Kun kohteena on laaja IT-organisaatio ja huomattava määrä tietojärjestelmiä, on perusteltua luoda jatkuvuuden hallintamalli johtamaan jatkuvuussuunnittelua tavoitteellisesti ja systemaattisesti.

Opinnäytetyön kohdeorganisaatiossa otettiin vuonna 2007 käyttöön jatkuvuuden hallinnan kypsyysmittaristo. Kypsyysmittaristo on yhdistelmä kansainvälisiä jatkuvuuden hallintastandardeja, prosessien kypsyysmittaristoja sekä IT-hallinnan malleja yhdistettyinä yhteen mittaristoon ja sen käyttötapaan. Opinnäytetyössä esitetään taustat ja tarpeet kypsyysmittaristolle sekä sen periaatteet ja käyttötapaukset. Varsinaisen ytimen muodostaa kypsyysmittariston hyötyanalyysi, jossa mittaristosta saatuja hyötyjä on arvioitu viidellä eri ulottuvuudella: IT-palveluhallinnan, IT-linjayksikköjen, IT-hallinnan, liiketoiminnan riskienhallinnan sekä yksilön kautta.

Tutkimuksessa kerättiin faktoja, missä määrin ja miten jatkuvuuden hallinnan kypsyysmalli on edistänyt jatkuvuussuunnittelua ja toiminnan jatkuvuuden turvaamista. Tämän kypsyysmallin perusteorian mukaan todellinen kypsyys voidaan todentaa vasta, kun voidaan osoittaa rakennettujen ratkaisujen toimivuus käytännössä.

Tutkimuksen tulokset perustuvat toiminnalliseen tietoon: raportteihin palvelutasoista, poikkeamista sekä jatkuvuussuunnittelun tilasta. Myös keskustelut alan asiantuntijaverkoston kanssa on tuonut merkittävää tietoa teorian toteutuksesta. Teoreettinen viitekehys on perustunut alan standardien ja parhaiden käytäntöjen analyysiin (liite 1), sekä systemaattiseen toimintatutkimukseen. Laaja materiaali on mahdollistanut analyysin sille, miten kypsyysmalli korreloi todellisen kyvykkyyden kanssa. Tutkimukseen liittyvän toiminnallisen tiedon luottamuksellisuudesta johtuen esitetyt tulokset on rajattu uuden menetelmän kuvaukseen ja uusien toiminnallisten mallien esittämiseen, joiden käyttökelpoisuus ja hyöty on käytännössä testattu ja kuvattu. Menettely on mahdollistanut opinnäytetyön julkistamisen.

Tämän opinnäytetyön tutkimusmenetelmä on suunnittelututkimus, sekä lisäksi siihen liittyvä toimintatutkimus. Menetelminä suunnittelu- ja toimintatutkimus ovat melko vakiintuneita tietojärjestelmien tutkimusperinteessä, artefaktien, toteutusten ja käsitteistön kehittämisessä sekä uuden osaamisen tuottamisessa erityisesti tietojärjestelmien alueilla.

Avainsanat: Laatujohtaminen, IT-prosessi, kypsyysmalli, liiketoiminnan jatkuvuuden hallinta, IT-jatkuvuuden hallinta, toipumissuunnittelu, riskienhallinta, IT-palveluhallinta sekä IT-governance ja riski

Laurea-university of Applied Sciences
Laurea Leppävaara
Master of Business Administration
Information Systems

Kimmo Syrjänen

Abstract

Maturity modelling as a catalyst for IT continuity management implementation in a large company

Year 2009 Pages 60

This thesis will describe an IT continuity management maturity model and the concrete benefits this model has brought to a company and its IT unit. The target organization is a large Finnish technology company that invests strongly in information technology due to high dependency on information systems availability. The role of business continuity and IT continuity management is to identify business requirements and provide solutions that ensure the continuity of information services and capability to recover in case of disruptions or interruptions. Because of the large size of the target organization and the considerably high number of information services, there is a need to implement target oriented and commonly accepted management models. This applies to IT continuity management processes and maturity models, too.

The target organization developed and started to implement an IT continuity maturity model in the year 2007. The maturity model is a combination of business continuity, IT governance and information risk management standards and best practices built on top of commonly used process maturity models. This thesis will introduce the background and initial triggers for maturity model development. In addition, maturity model principles and usage cases will be reviewed.

The purpose of the study was to find out how much the IT continuity management maturity model has improved overall planning and the level of business continuity in the target organization. The core of this research is the evaluation, the purpose of which is to evaluate the concrete benefits the use of maturity model has brought. The benefits will be analyzed from five viewpoints: information service management, IT line units, IT governance, corporate governance including risk management, and the point of view of the individual.

The evaluation is based on service quality reports, incident analyses and continuity reports. In addition to the extensive report base, open discussions and feedback from the IT continuity community has a significant role while assessing the maturity model value. The theoretical framework is mostly based on industry standards and best practices (Appendix 1) and the methods of canonical action research. Although the extensive source material provides a solid base for the research, the confidentiality of this information limits what and how much information can be shared in this thesis.

This thesis utilizes the premises of two analysis methods, design research and action research. These methods are institutionalized in the context of design artefacts, terminology, information system innovation and development.

Keywords: Quality Management, IT process, maturity model, business continuity management, IT continuity management, disaster recovery, risk management, IT service management, IT governance and risk

Abbreviations used on this thesis

AirMiC	Association of insurance and risk Managers
AR	Action Research
BCM	Business Continuity Management
BCSC	Business Continuity Steering Committee
BS	British Standard
DR	Design Research
CMMI	Capability Maturity Model Integration
CoBIT	Control Objects for Information and related Technology
COSO ERM	Committee of Sponsoring Organizations Enterprise Risk Management
ICT	Information & Communication Technology
IEC	the International Electro technical Commission
IRM	Institute of Risk Management
ISO	the International Organisation for Standardization
IT	Information Technology
ITCM	Information Technology Continuity Management
ITIL	Information Technology Infrastructure Library
ITSCMM	Information Technology Services Capability Maturity Model
NFPA	National Fire Protection Association
PAS	Publicly Available Specification
PDCA	Plan, Do, Check, Act – model
RACI	Responsible, Accountable, Consulted & Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOX	Sarbanes-Oxley Act

Index

1 Introduction to business continuity management

1.1 Finding the rationale

Throughout history man has coped with crisis and uncertainties by taking precautions in order to ensure safety and survival of family, tribe and culture. We can imagine how early continuity plans, verbal or somewhat documented, provided information how to store crops in case famine should strike the village. In the Middle Ages strongholds were designed and located so that food and water supplies were secured. In case walls should fall down under attack, tunnels provided the means for evacuation. We do not have to go very far in history to find similar behaviour, we can simply observe how people today react to union strikes and pandemic alerts. Though planning for the worst has a long history, it was boosted by two major incidents in the beginning of the 21st century: Y2K and 9/11. As a result, crisis and emergency planning developed into a structured and managed process known as business continuity management.

The Year 2000 problem (also known as the Y2K problem, the millennium bug, the Y2K bug, or simply Y2K) was a software problem that originated from the days when computer memory capacity was low. Programmers used to save capacity by using only the last two digits of the year information e.g. 1999 were saved as 99. Though memory sizes grew, no efforts were put into updating the software bug. The actual problem was the fact that computers would read year 2000 as 00, resulting in a conflict with the timestamps i.e. earlier days would become later days and year 2000 would turn into 1900. When organizations around the world realized the worst case impacts, a massive world-wide initiative of checking, fixing, and upgrading the computer systems started. (Mahdy 2001, 74-82.)

As Mahdy (2001, 74-82) continues, preparation for the Y2K bug had a significant impact to organizations and corporations as the planning process revealed how dependent they were on information systems. It is only fair to claim that Millennium bug was the trigger for the information systems' systematic disaster recovery planning in large enterprises.

If Y2K was the trigger for information systems disaster recovery planning, 11 September 2001 set a new standard for business continuity planning. When the two planes hit the twin towers the impact was vast as over 2750 people lost their lives. Over 1200 organizations from 28 countries, including American Express, Aon Corp., AT&T, Bank of America, Dow Jones, Deutsche Bank, Morgan Stanley, New York Department of Taxation & Finance, New York Stock Exchange, Sun Micro Systems, and WorldCom suffered major losses. The United States stock

markets halted business for four days and Dow Jones fell 684.81 points immediately in the re-opening days of the stock market. (Jackson 2008, 2.)

The aftermath was profound and a number of studies were made analysing what went wrong. Summary from a Finnish National Emergency Agency publication provides some of the key findings from the World Trade Centre terrorist attack as follows:

- Even the most unlikely risks may actualise causing unexpected and cascaded consequences on a local and global level
- The organizations that had centralized operations in the impact zone were not able to continue their business for a long time and some of them simply closed down their business as all assets and personnel were lost
- The organisations that had continuity plans suffered less damage than those not having the plans
- Organisations who exercised their business continuity plans before the attack survived the best (PTS Publications 2002, 14.)

Tsunami in Asia in 2004, Hurricane Katrina in 2005, H1N1 Swine flu pandemic in 2009, and loss of supply networks due to economy recession in 2009 are just examples of the latest major incidents having serious impacts to nations and businesses globally. Business continuity planning and management does not prevent these things from happening, but may provide assurance that during the next crisis one can prevail.

1.2 Risk and continuity

Risk, by its very definition, always includes uncertainty about the severity of impact and probability if the risk may or may not actualize (Suominen 2003). Risks that have a higher impact on the organization may require special attention. According to the Finnish Financial Supervisory Authority (FIN-FSA) operational risk management publication, financial institutes and organizations should regard continuity planning as an ongoing process and a natural part of their business operations and risk management. Business continuity planning in this context means preparations for interruptions in business activities so that the business can continue its operations and mitigate losses in various business disruptions. Disruptions may be due to damage to the employees, business premises, IT systems or data communications or intentional acts, water damage, fires or utility outages. (Management of operational risk 4.4b 2004, 20-21.)

The British Standard (BS) 31100 is a standard for risk management established by the British Standard Institute. It describes how to develop, implement and maintain effective risk man-

agement within business by providing clear framework components as to how risk management governance should be arranged, what is a good policy, processes and instructions on how to evaluate outcome of the risk management framework. The standard is aligned with several other risk management standards e.g. ISO 31000 (in preparation), Enterprise Risk Management COSO, and the risk management standard developed by the Institute of Risk Management (IRM) and the association of insurance and risk Managers (airMiC). (BS 31100 2008.)

BS 31100 (2008, 11) emphasizes that, as part of risk management function, there are specific risk areas where a detailed management or control framework is needed. Standards list the following as areas of specific risk management: Compliance risk, operational risk, health and safety, information security, and business continuity management. This Standard keeps information security and business continuity separate management entities for specific risk management purposes. What is interesting in the above standard is that it does not stress the role of IT as a separate risk management topic. IT as it is understood as a larger function is listed as a critical asset on several occasions and standards.

British Standard Institute has published the Business Continuity Management standard BS 25999 which can be applied for various types and sizes of organisations. According to the standard, Business Continuity Management (BCM) is complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks. By focusing on the impact of disruption, organizations can recognize what needs to be done before an incident occurs to protect its people, premises, technology, information, supply chain, stakeholders and reputation. (BS 25999–1 2006.)

According to Westerman and Hunter (2007) the first logical step in improving the foundation of the information risk management is to address availability risks. This can be done by addressing business continuity management as base of availability risk management. This powerful engine lays the ground work for managing in every layers of 4A where the A means risks related to: availability, access, accuracy and agility. (Westerman & Hunter 2007, 60-68.)

The examples above demonstrate that business continuity management is an important part of risk management practice. One can say that in order to extend an organization's capability to manage the risks which cannot be simply insured, transferred or compensated by money, implementation of business continuity management will secure organisation's mission and continuity.

1.3 Business continuity management system

BS 25999 defines the business continuity management system as a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework. System should proactively improve an organization's resilience against the disruption of its ability to achieve its key objectives. The basic assumption is that the system should include a rehearsed method how to restore an organization's key products and services to an agreed level within an agreed time after a disruption. So as an end result business continuity management system may at its best deliver a proven capability to manage a business disruption and protect the organization's reputation and brand against threats. (BS 25999-1 2006, 6.)

ISO standard 21827 (2008, 117) for technology security capability maturity model refers to Dr. W. Edwards Deming's observation as follows:

"In a manufacturing plant, a manager observes problems with a certain production line. All he knew, though, was that people on the line make a lot of defective items. His first inclination might be to plead with the workers to work harder and faster. But instead, he collected data and plotted the percentage of defective items. The plot showed that the number of defective items and the variation from day to day were predictable." (ISO 21827 2008, 117.)

Moen & Norman (2009) introduce the history of the PDCA model development. The PDCA model became well-known through W. Edwards Deming, although Deming called the model the Shewhart Cycle after its inventor and form. It is also known as Deming's Wheel. Deming published the methodology in his book Out of Crisis (1982). Deming regarded the PDCA model as "a flow diagram for learning and for the improvement of a product and a process". The PDCA model corresponds to the general principle of managing a system according to general systems thinking, systems dynamics, or cybernetics. A modern application of the PDCA model is the Six Sigma methodology for an organization's performance improvement (Brue 2002). Its most general activity phases are DMAIC – Define, Measure, Analyze, Improve, and Control. As an example of other application area Figure 1 provides comparison between the information technology service management ISO standard 20000 and BS 25999 business continuity management system standard. Snap shots (figure 1) of the given "Life cycles" provide a good example on how the PDCA model is used in different contexts in business continuity and IT service management.

Even though the content of the life cycles are different, both approaches highlight the importance of continuous improvement using the key phases of the PDCA model. Both processes start with the planning and understanding of the current situation. Second phase is the plan execution by taking controlled steps after which one move on to the third phase, learning from the results. Checking the results provides the insight into which actions are needed in order to improve the process and, by that, to reach the optimum result.

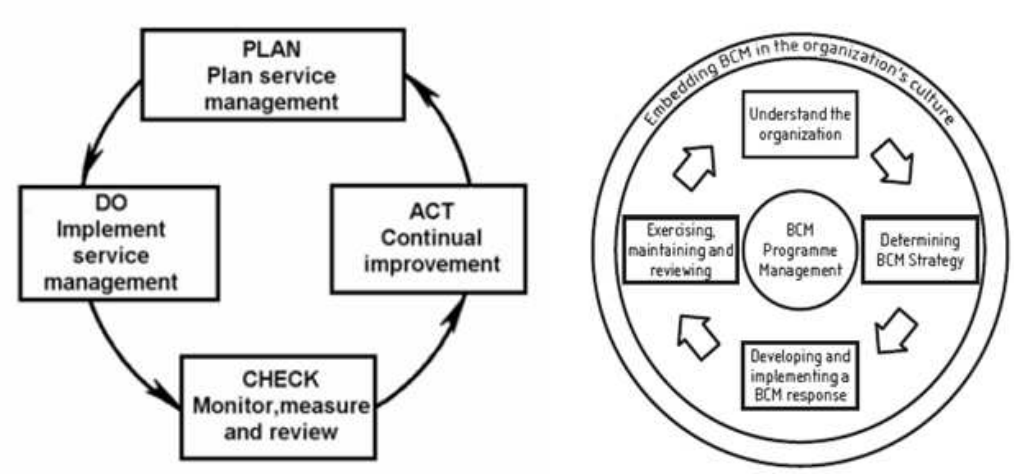


Figure 1 Comparison of Plan, Do, Check, Act model adaptations between International Organization for Standardization and International Electro Technical Commission (ISO/IEC) 20000 (2005, 5) and BS 25999-2 (2007, 3.)

Consistent link to quality models enables BS 25999 to be integrated with related management systems standards, such as BS EN ISO 9001:2000 (Quality Management Systems), BS EN ISO 14001:2004 (Environmental Management Systems), BS ISO/IEC 27001:2005 (Information Security Management Systems) and BS ISO/IEC 20000:2005 (IT Service Management). (BS 25999-2 2007, 3.)

Even though the standards provide common models agreed on by the different industry representatives and standardizing bodies, it is important to keep in mind that each country's standardizing bodies and institutes often promote their own approaches and this applies also to the BS 25999 as it is not the only standard related to business continuity management. When the number of available standards may start burdening the implementation, it is good to recap what is the ultimate goal of the business continuity planning. Graham and Kaye (2006, 11) summarize the essence of business continuity management into four key points that apply to all relevant systems:

- BCM is not just about response, it is also about building resilience to strengthen an organization
- BCM is not just about fighting fires, it is about understanding what might be at risk and developing strategies if things go wrong
- BCM is not just about having plans to recover a business that are over-elaborate, it is about having plans that suit the nature of your business
- BCM is not an extension to the business, and for it to be effective, it must be an embedded management process – as part of risk management, and in turn, as part of business management (Graham & Kaye 2006, 11.)

BCM “life cycle” provides a solid structure for developing the business continuity management in organization, whether this is private or public. Implementation of a high level management process apart of current organization processes may become challenging if it is not understood by those who should carry out the actual implementation. One way to solve this problem is to provide a tailored model of how business continuity management principles can be applied to in specific areas, such as information technology (IT).

1.4 IT Continuity management

U.S. Federal information processing standard (FIBS PUB 87 1981) introduced fundamentals of contingency and disaster recovery planning in automated data processing almost 30 years ago. At the time the standard development group identified the key topics that contingency planning should cover in order to have a working plan against adverse situations. The list below summarizes the content of the FIBS PUB standard.

- Risk analysis and management role in planning
- Preliminary planning scope, objectives and roles
- Preparatory actions related to people, critical assets, data and infrastructure
- Action plan for emergency response, backup operations and recovery, and
- Expectation for testing the plan

Even then the FIBS Publication 87 emphasized that contingency planning should be an integral part of the program for any data processing operation. As the standard continues, minor problems may become major and major problems may become catastrophic without a tested and effective plan how to respond to and recover from unexpected and sudden disruptions of service. (FIBS PUB 87 1981.)

Since FIBS PUB 87, IT contingency and recovery planning has evolved into a managed process in which BS 25777 established by the British Standard Institute in 2008 represents the latest approach to IT continuity management. BS 25777 provides a common approach for information and communications technology (ICT) continuity management. The primary objective is to ensure that the organization has plans in order to continue information and communications technology services at an acceptable predefined level in case incidents and disruptions should occur. The cornerstones for BS 25777 (2008, 3-4) are the six key principles in ICT continuity management:

1) Protect: Protecting the ICT environment from incidents, failures and disruptions by improving the resilience of ICT services

2) Detect: Detecting incidents at the earliest opportunity and minimize the impact to services
3) React: Reacting to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime
4) Recover: Identifying and implementing the appropriate recovery strategy will ensure timely resumption of services and maintain the integrity of data
5) Operate: Running in ICT disaster recovery mode until return to normal is possible
6) Return: Devising a strategy for every ICT continuity plan that allows an organization to migrate back from ICT disaster recovery mode to a position where it can support normal business

As these six principles demonstrate, today's ICT continuity management is not only limited to response and recovery phases but is extended to cover also pre-work and actions for prolonged interruptions and for returning into normal operation. In order to promote managed implementation of the given principles, BS 25777 applied BS 25999-1 business continuity management lifecycle model (figure 2). This model consists of six elements which should be implemented phase by phase starting with understanding business needs and moving from strategy determination to implementation and testing the strategy. Outer circle represents the implementation of continuity management into the organization culture.

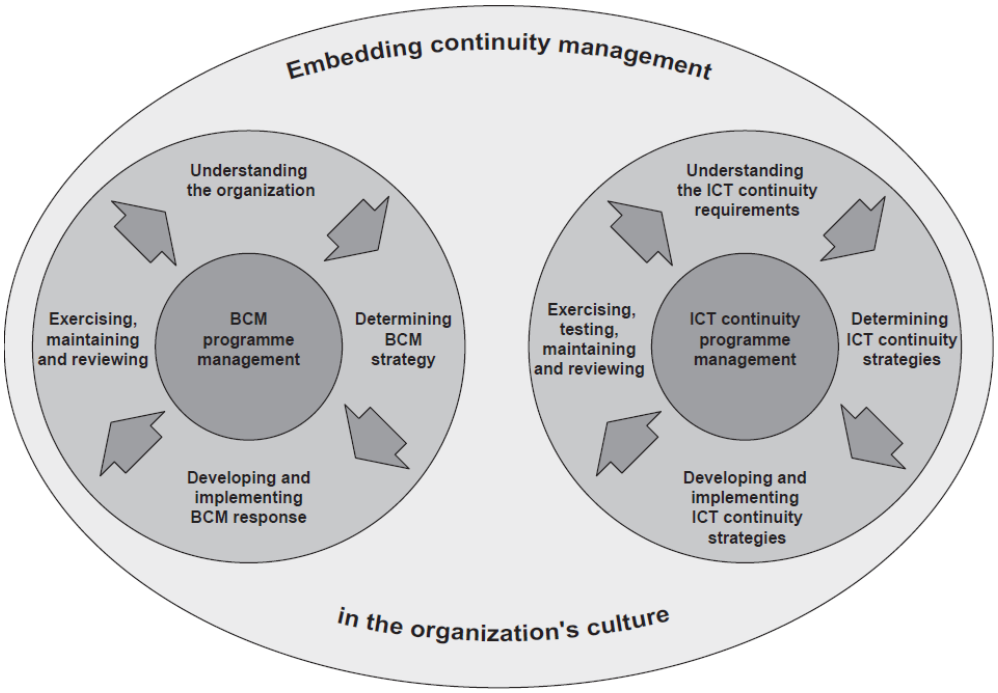


Figure 2 Relationship between ICT continuity management and business continuity management (BS 25777, 3.)

The central governance element in both BS 25999 and BS 25777 is continuity programme management. The purpose of continuity programme management is to ensure ongoing development and implementation by steering all the planning phases consistently and in a goal-oriented manner. Goals and objectives should be carried out so that they fit the organisation's objectives as well as possible within the given timescales, resources and the budget. BS 25777 (2008, 9) provides examples of what successful ICT continuity management programme should achieve:

- The ICT continuity management objectives are clearly stated, understood and communicated
- Top management's commitment to ICT continuity management as part of business continuity management is demonstrated
- Necessary resources are allocated, and
- Those with ICT continuity management responsibilities are competent to perform their roles

As the programme evolves and the organization becomes more aware of the continuity management benefits it may become a part of the normal management process. In order to secure this change successfully it is imperative for the overall governance structure that a business continuity steering committee (BCSC) is appointed. The implementation of this steering committee ensures that the organization's continuity plans are regularly considered, reviewed, tested, and updated when organizational change occurs. This group should be comprised of the most senior managers from the organization and each key unit should be represented. (BS 25999 -1 2007, 13-16.)

Brue (2002, 36) refers to the famous William Thomson a.k.a. Lord Kelvin: "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind. It may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science".

Brue (2002, 36) states that if you do not have measurements, you cannot make progress because you do not know where you are. This underlines the common management problem which applies also to business and IT continuity management, that is, how to measure change? Continual monitoring of progress against organization's objectives ensures that actions and resources can be allocated accordingly. This can be done by having relevant and valid measurement methods that reveal issues and deviations on the process before they escalate into major problems. Basically, measuring change is one way to carry out risk man-

agement as the target is to predict and prevent incidents that would weaken the achievement of the business objectives.

BS 25999-1 (2006, 11) requires that business continuity capability should be measured and BS 25999 part 2 specifications for business continuity management underline the importance of continual improvement based on objective measurement. U.S. National Fire Protection Association (NFPA) has created a standard for disaster, emergency and business continuity management. This NFPA 1600 standard (2007, 5) states that performance measurements should be established and periodically reviewed as a part of continuity management program. The problem is that this standard does not provide principles on what the performance indicators for successful programme management should be. From the continuity management point of view a common relevant and reliable measurement model would bring significant benefit when assessing an organisation's continuity capability, especially when managing large scale operations both in business and in IT.

2 Background for the research

2.1 Initial state at target organization

The company in scope (referred herein simply as Company) operates globally in the field of telecommunication. Because of this position, external expectations from the shareholders and the Company community are relatively high, especially in matters of business continuity. The Company puts high priority to enforce practices and controls balanced with informed risks which will protect both shareholders' and Company community's interests in the most optimal level.

The Company has a robust crisis management program that has proven its effectiveness in real life situations; still, further development was seen necessary in order to be able to work more proactively against the risks. The Corporate risk management unit started to formalize practices towards business continuity management collaborating with company security, infrastructure services and IT units. After exploring all relevant possibilities, the publicly available specification 56 (PAS 56 2005) was seen as a framework that could be best adapted into the current operation model for the Company. One reason for the selection was the fact that PAS 56 had a strong development community behind it and was linked to the respected British Standardizing Institute. Since that the PAS 56 has evolved into the BS 25999, which today is the globally recognized business continuity management standard.

The Company already had established risk, information security and crisis management policies when the business continuity management policy was under development. Business continuity management policy statements were embedded to other relevant management poli-

cies, as the objective was to keep the number of policies as low as possible. As a general guideline each business unit was responsible for ensuring business continuity in their own area at a level that fit the mode of operation best. Since operations in a large organization differ considerably from one business unit to another, the policy was written in a manner that allowed business continuity plans to be delivered in either a project or a program mode. Delivering business continuity plans in a project mode was seen beneficial for those units which had limited resources for a dedicated management system. The approach was especially successful in situations where fast actions were needed due to a sudden change of risk level e.g. pandemic outbreak, natural hazard, political restlessness or technological vulnerabilities.

The program approach was seen best for situations where the business unit had a critical role in other company operations in a large scale. This role would set a high standard for maintaining a high preparedness and response level. When the scale of continuity planning increased inside the unit, continuity management program provided an effective method to steer and control several planning streams at the same time. Continuity management program subject matter experts facilitated the planning process in order to make sure that plans were consistent and overlaps with other plans could be avoided. Continuity program was seen as a first step in a process in which the long term objective was – and still is – to embed continuity management seamlessly into the organization's normal operations and management.

2.2 Building the IT continuity management system

The initial step was to define and agree on the IT continuity management scope and relation to business continuity management. As a result, it was agreed that IT will take responsibility for all information services' continuity management, including the infrastructure such as data centres, network connectivity and IT personnel. This scoping resulted to business continuity management in which IT continuity plans are a subset for business continuity plans, allowing business units to focus on their response in case IT plans should fail.

The second phase was to define and agree on the level of implementation as that would affect the whole management concept. Basically it was question of which IT subunit should act as the primus motor and who should take the responsibility of each system's continuity plans. As each IT service already had responsibility of the business requirement and information systems management, it was only natural to include IT service continuity planning as part of their role. IT service and computer managers' role became critical for continuity management as they were responsible for managing applications' life cycle and collecting requirements from business owners. To support IT managers and to ensure consistent implementation of the IT continuity process, a team of continuity management specialists was established. The objective of the team was to develop the process and the tools, to provide train-

ing and consult when needed, to communicate common objectives and to follow the planning progress.

At the time PAS 56 provided the structure for continuity management but the terminology was seen too confusing and vague for practical implementation in IT. In order to solve these problems the terminology and the model were modified in such a way that the user would understand better the given action and the main deliverables in each phase. Table 1 shows the changes between PAS 56 and the Company IT continuity planning model planning phases (Table 1).

PAS 56 (BS 25999 Nov. 2006)	**Company IT continuity planning model**
Understanding the organization	IT Continuity risk and impact analysis
Determining BCM strategy	IT Continuity management strategy development and business approval
Developing and implementing BCM response	IT Continuity strategy deployment and plan delivery
Embedding BCM in the organization's culture	IT Continuity plan communication and training
Exercising, maintaining and reviewing	Maintain & exercise IT Continuity Plan

Table 1 Comparison of PAS 56 and Company IT Continuity planning implementation

As the example above shows, the planning process included several phases. In order to ensure that continuity planners would understand that each phase needed to be completed before starting the next one, a simplified process flow was created (Attachment 1). Continuity plan exercising was seen as the most important part of the process, so the PDCA lifecycle was integrated as a part of the whole process. Using the PDCA lifecycle the importance of continuous improvement by rehearsing and exercising the plans became visible to planners. It was also clear that information systems are under constant change pressure due to new business initiatives and mandatory configuration updates. This change pressure was covered in the process by adding a clear loopback from the continuity plan maintenance phase back to planning and creating phases in the beginning of the process. The overall objective for drawing a single IT continuity planning process was to enhance communication and steer the continuity planners' actions into a desired direction.

2.3 IT continuity maturity model

IT continuity management can be part of either the business continuity management or the IT governance discipline, depending on how responsibilities are shared between the organiza-

tions. Regardless of the responsible entity, management needs to have information about progress and capability from the processes and other activities in order to be able to steer the organization. As an example, British Standard for Information technology service management (ISO/IEC 20000-1 2005, 6) states that the service provider shall apply suitable methods for monitoring and, where applicable, measurement of the service management processes. These methods shall demonstrate the ability of the processes to achieve planned results. From Company IT unit continuity management point of view it was necessary to capture the current continuity planning status across the IT and be able to follow the progress. In order to build a working maturity model for IT continuity management and IT governance purposes, following expectations were set by the senior management after recognizing and specifying the problem area to be researched:

- The model must be simple and easily understandable for those implementing the process
- Key performance indicators must be scalable with the organisation and measured subjects
- The model must support senior management decision making
- The model must direct actions so that users will understand what they are expected to achieve
- Key performance indicators must reveal changes in order to identify possible gaps and forthcoming issues
- The model should support rewarding system and,
- To demonstrate the level of assurance in the organization's ability to respond and react during events that cause an interruption or a disruption

In order to comply with industry standards and internal expectations, the need for a maturity model was obvious. For this purpose the IT continuity planning process model provided a foundation for creating maturity measurement. The planning process was translated into a roadmap for IT services system development as a part of standard planning cycle used by the IT. In practice this means that the IT service team could plan how to allocate resources between the1st and the 2nd half of the year (Table 2). This approach allowed IT services that managed several information systems with different service level requirements to set balanced continuity objectives between the business critical systems and the standard systems. The fundamental part of this model was the decision that the unit of maturity measurement was not the IT service or the team but the information system itself. The rationale for this approach was the fact that failures in the information systems would cause an interruption directly to business process. Due to this direct dependency measuring the systems' resiliency and recovery capability was seen more important than the organization's capability to re-

sponse and work under problem situation. (Company IT Continuity management process 2007.)

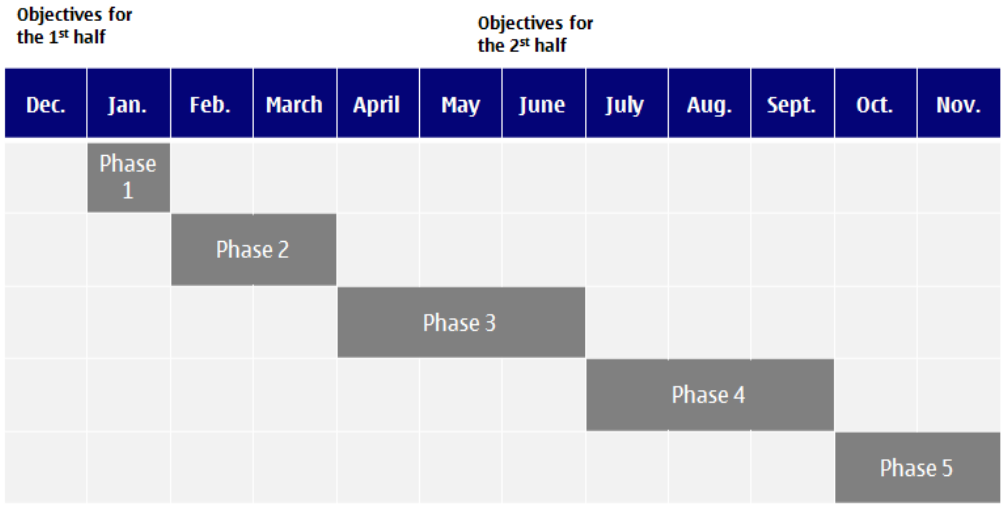


Table 2: Example of the common planning cycle and how IT continuity planning phases are connected (Syrjänen 2009.)

In order to ensure that each planning phase would be completed accordingly, a simple success criteria model was established based on PAS 56 planning phases. The rule was that each criterion of success must be complete and validated by the continuity specialist team before the planning process could progress to the next phase. (Company IT Continuity management process 2007.)

The purpose of phase 1 is to build the rationale why the continuity planning process must be initiated by conducting the Business impact and risk analysis. Business impact analysis aims to identify and quantify impacts to business in case an interruption or a disruption should occur in the information systems. It is essential to understand and prioritize information about interdependencies between the business processes and systems in scope. Outcomes of business impact analysis are recovery time objectives for the system and recovery point objectives for the data. Risk analysis aims to identify any operational risks which may cause extreme damage to the information systems which would then cause a failure or extended outage of the business operations. Based on the risk analysis findings and the business owner's risk tolerance, decision of further continuity development will be made. (Company IT Continuity management process 2007.)

The target of phase 2 is to identify available continuity solutions for the information system in scope. When selecting the solutions, the costs/benefits calculation must be completed in a balanced manner. In this context balance means the cost of solution versus how effectively

the solution can reduce the risk of failure or to ensure fast and controlled resumption back to business. The final stage is to propose solutions to business owners and get approval for the implementation for the selected one. (Company IT Continuity management process 2007.)

The success criteria of phase 3 contain two key actions, continuity solution building and documenting the IT continuity plan. Solution building is done following the standard project management and system development practices, and therefore this has not been defined separately. The criteria for the success are that the solution is implemented according to the risk and the business requirements and that the IT continuity plan document is available for validation by subject matter experts. (Company IT Continuity management process 2007.)

The target of phase 4 is to ensure that the plan is shared between all relevant teams and units; i.e. those who have a role in continuity solution management and possible recovery actions in case it is necessary to invoke the IT continuity plan. This phase also includes IT service team training for the IT continuity plan use so that each team member understands their role and the role of other team members in case there is a need to initiate recovery and restoration actions. (Company IT Continuity management process 2007.)

Phase 5 is demonstrates whether the continuity solution and agreed recovery actions will work as planned. The term technical exercise is used here as it combines both the crisis management and the technical capability testing. Even though exercise methods vary depending on the solution in use, all of these exercises aim to validate whether response, recovery and restoration can be done within the time objectives set by the business. (Company IT Continuity management process 2007.)

As remarked earlier, continuous improvement of continuity management was based on information systems' recurrent technical exercises conducted by the IT service teams. Successful technical exercise provided evidence about the capability to recovery and restore information systems and data if needed. This result demonstrated the highest level of assurance of mitigated risks and, by that, justified retaining the maturity level 5. (Company IT Continuity management process 2007.)

Failures in technical exercises revealed weaknesses and deviations that would require special attention leading to corrective actions and dropping the maturity level down on the scale. As an example, technical exercise might reveal that the back up process did not work promptly due to a technical mismatch. This finding would initiate reconfiguration of the back up process that would be done on maturity phase 3. Even though a technical exercise is normally required for maintaining the highest maturity level, there is one exception. In case the continuity solution has worked as planned during a real incident, technical exercise does not need

to be completed. This is regarded a proof of a working solution; therefore maturity level can be kept on level 5 until the next review round. (Company IT Continuity management process 2007.)

Even though IT continuity management has a long history in the Company IT, the maturity model development did not start until 2007. The initial stage consisted of diagnosing and reflecting the key problem: how to measure and lead IT continuity management implementation in a large IT organization. After action planning, the first six months the model was adjusted to the organisation's management and it passed several iteration rounds between the specialists and the stakeholders. Implementation of the desired model began after common agreement on what would work best in the target organisation.

The model has now been used for three years and it is time to analyse and reflect how well original expectations were met. According to Järvinen & Järvinen (2004, 103) scientific research can be divided into two main areas, basic research and applied research. The objective of basic research is to observe and analyze environment in order to create and test new theories. Applied research uses results from basic research as scientific foundation to create new innovations for everyday use. According to Pirinen (2009, 10) the diversity of ways to generate innovation is huge and the nature of innovation generation is multidisciplinary. Pirinen provides a concept of six perspectives on research and development in integrative action which are not exclusive and all of which are needed to successfully consider processes of integrative action. This concept sets the framework for the following two chapters, which will reflect the journey of the IT continuity maturity model innovation in the context of design research and action research.

2.4 IT continuity maturity model in the context of design research

The aim of design research (DR) is to solve identified problems by delivering practical solutions and innovations (artefacts). An additional target is to provide new information for solving problems in horizon. To decide whether IT continuity maturity model belongs to the premise of design research, one must understand the concept of artefact. According to Hevner, March, Park & Ram (2004) both_design research and behavioural sciences are inseparable as technology and behaviour are not dichotomous in an information system. The fundamental of this idea lies on the fact that an information system research is at confluence of people, organisations and technology so it is more than a product. Based on this, IT artefacts can be defined broadly as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems).

IT artefacts are implemented in an organizational context i.e. information systems are for people and organizations, not an end in itself. This is the rationale for the object of study in information systems behavioural science research. Behavioural science research objective is to predict or explain phenomena that occur with respect to the artefact use, perceived usefulness and impact to individual and organisation. Most of the behavioural science is focused on instantiations i.e. information systems but is used also with the evaluation of constructs and methods. As a conclusion, even though the design research focus is on technology-based design, its link to behavioural science allows us to cover also organisations, policies and work practices as design artefacts. (Hevner, March, Park & Ram 2004.)

Effective design research must provide a clear contribution in the area of the design artefact. According to Hevner at al. (2004) design research may provide three types of contributions based on the novelty, generality and significance of the designed artefact. One or more of these must be found in a given research project. The first contribution is related to the design artefact itself as it may solve the initial problem. From this perspective IT continuity maturity model has solved the initial problem of improving the implementation of the continuity management practice. The second contribution is the foundation, i.e. the creative development of novel construct, model, method or instantiation that extends and improves the existing foundations. IT continuity maturity model is a method that was a novel approach as it was a totally new approach in the field of continuity management practice in the target organization. The third contribution is methodologies, i.e. the creative development and use of evaluation methods and metrics for design research contribution. Results of this research did not reveal that the maturity model or the research method created new methodology for the purpose of design research. Finally Hevner at al. (2004) mention that artefacts must be implementable and contribute business environment. The IT continuity maturity model was implemented and its outputs improve the level of business continuity from the information system viewpoint. (Hevner, March, Park & Ram 2004.)

When one considers these design research definitions, a loose connection between the maturity model development and the premises of design research can be seen. As an example, the IT continuity management maturity model is an outcome of a design process. However Hevner, March, Park & Ram (2004) clearly state that design is both a process of (a set of activities) and a product (artefact). Even though there seems to be a link between the design research and method development it is evident that the outcome of the process must also produce something tangible.

Building the artefact for a specific problem may solve the initial problem, but the basic question is how well does it work? The evaluation of the artefact provides feedback information and a better understanding of the problem and improving the quality of the product and de-

sign process. Hevner, March, Park & Ram (2004) provide a guideline for design evaluation. According to them, the utility, quality and efficiency of a design artefact must be rigorously demonstrated via well-executed evaluation methods. IT artefacts can be evaluated in terms of functionality, completeness, consistency, accuracy, performance, reliability, usability fit with the organization and other quality attributes. The core of this thesis is the value evaluation of the IT continuity maturity model. Design research provides the premise for the maturity model evaluation.

2.5 IT continuity maturity model in the context of action research

Action research (AR) is, by definition, active and tightly bound to real life problems in organizations and may provide a practical means to reflect theory and practice on a highly pragmatic level. In order to have a working connection to real life problems, research test subjects are all the actors related to research problem e.g. developers and tools. This method provides a structured approach for problem solving; finding innovations and solutions for developing organisational capabilities. As action research progresses gradually from problem identification to implementation and testing closely with the users of the solution, this relationship may also change the way the community is thinking and the way they are working which might affect the research results. For the researcher this means that in practice he must be able to make theoretical interpretations about the new findings and the reasons behind them and, at the same time, to be able to contribute to the practical use of the research results. (Järvinen & Järvinen 2004, 128 -131.)

According to Baskerville and Meyers (2004) there are four premises to consider in order to conduct a pragmatic action research. The first is the necessity to establish a theory beforehand of any action. The rationale for this is to avoid actions that are not relevant or valid from the research point of view. The theory behind the IT continuity maturity model innovation originates from the learning and improvement models like PDCA model (Moen & Norman 2009) and Six Sigma (Brue 2002). The assumption was that the capability to measure continuity planning and delivery process utility would lead to concrete improvement actions in IT continuity management. The second premise is the problem setting that must be pragmatic. As stated earlier (chapter 2.3) the identification of the most tangible problem related to IT continuity management led to strict requirements set by the senior management. The third premise requires that the action must inform the theory. According to this, the theory must be validated by its practical outcome. The validation of the IT continuity management maturity model value is the core of the thesis objective. Findings are discussed in chapters 5, 6 and 7. The fourth and last premise is related to social situation. This means that the action researcher must be a participant in action and at same time be an observer. Due to this reason there must be a collaborative team participating during the action. This will ensure that

there are reasoning and social realities while the problem is solved. (Baskerville & Meyers 2004.)

Looking at the downside of the action research, the critical success factor is how well the researcher co-operates with the actors i.e. customers and co-workers. This implies that actors must trust and be willing to share information with the researcher. This challenge puts the researcher's social and communication skills to test as failure in communication and getting the commitment will probably lead to failure of not reaching the research targets. (Järvinen & Järvinen 2004, 128 -131.)

According to Järvinen & Järvinen (2004, 128 -131) instead of just observing the process and the response, researchers are expected to work closely with the actors and participate in the problem solving. In order to meet this expectation, the researcher has to participate in the actual use of new solutions or at least be present when the theory is put into practice. Close relation with the actual work may not fit for all personalities and may lead to motivational problems. Other challenges are the high expectations of the client or the end user. Client may give a lower priority to theoretical part of the action research as concrete results matter the most. As a result, the research may turn into a routine and original scientific research targets are lost.

Davison, Martinsons & Kock (2004) introduce the five principles of the canonical action research which may mitigate the risks like Järvinen & Järvinen demonstrated:

- the Principle of the Researcher–Client Agreement
- the Principle of the Cyclical Process Model
- the Principle of Theory
- the Principle of Change through Action
- the Principle of Learning through Reflection

The first principle underlines the importance of the agreement between the researcher and the client. The agreement represents consensus of the goals, planned actions, and implementation of the changes and evaluation of the change. At the time there was no separate agreement between the author and the target organization of how to conduct the research and development of the IT continuity management maturity model. Basically the agreement was replaced by individual objective settings that included the goal, expected actions and schedule for the delivery. Objectives were reviewed every sixth month and, when needed, corrections were made so that the ultimate goal of overall improvement of IT continuity management remained intact.

The second principle is the cyclical process of sequential actions that, according to Davison, Martinsons & Kock (2004), should ensure that an action research project is conducted with systematic rigor (figure 3). It is possible to complete a project satisfactorily in a single cycle, but very often additional cycling through the stages is needed. Davison at al. underline the importance of flexibility, e.g. supplementary planning may be necessary if an intervention cannot be completed as intended. Variations from an unidirectional flow through each of the five stages should be justified but these should be taken into account while defining the research project plan. (Davison, Martinsons & Kock 2004.)

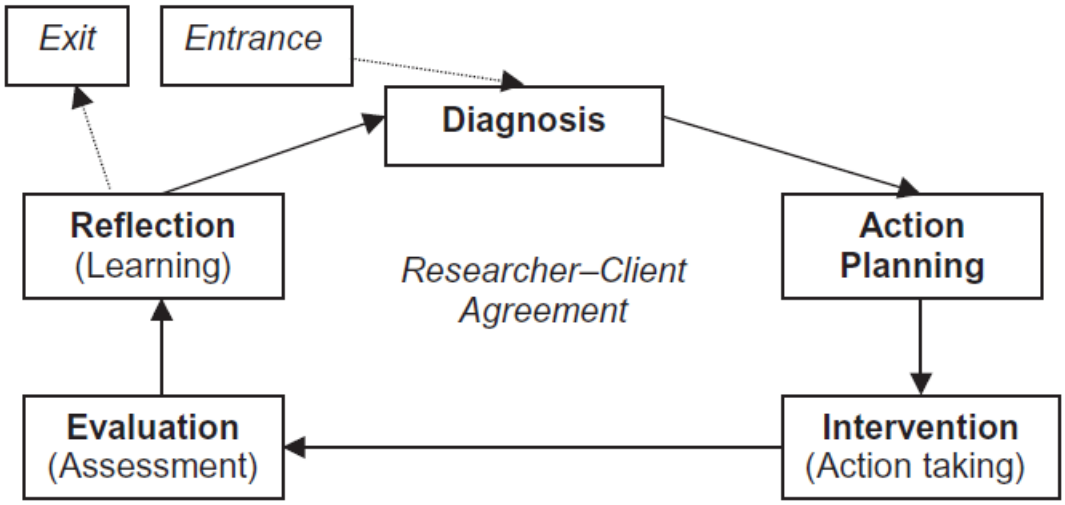


Figure 3 Canonical action research model (Davison, Martinsons & Kock 2004, 7.)

Table 3 provides a comparison of phases between the IT continuity maturity model development and the canonical action research model. The content of the IT continuity maturity model development steps include only a few examples per phase reflecting the canonical action research steps.

Theory	Reality
Canonical action research model (Davison, Martinsons & Kock 2004)	**IT continuity maturity model development steps (Kimmo Syrjänen 2009)**
Diagnosis and reflection i.e. reflection on the work or the work environment from the perspective of the three statutory tasks; raising questions; and recognizing and specifying a problem area to be researched and treated with new forms of action or changed actions.	The problem was identified on collaborative mode between the author and the stakeholders of the IT continuity management. The problem was the inadequate capability to capture the current continuity planning status across the IT and ability to set performance-based objectives.
Action planning involves learning about a problem and planning for a change by introducing and being self-motivating in the co-creation of strategies, scopes, plans and implementations that use the organizational bottom-up model.	The objective was to improve IT continuity management and ensure that information systems were built based on business needs and risk tolerance. This work was lead by the author with the support of other IT continuity team members. The plan was to create a maturity model that would direct and lead IT continuity planning

	process among the IT teams. The purpose of this model was to measure progress and performance using common language
Interventions i.e. taking actions in order to change the current situation and its unsatisfactory conditions. The intervention might require the assistance of catalytic change agents.	- Roles and responsibilities were implemented - The planning process was translated into a roadmap for IT services system development as a part of standard planning cycle used by the IT - Workflow for continuity planning was simplified - Each maturity level was validated by the continuity specialist team before the planning process could progress to the next phase. The author's role was to facilitate the process, review the performance and gradually improve the model based on the received feedback.
Evaluation, which is the assessment of the effects of change. After the planned actions are completed, the intervention needs to be evaluated with outcomes being compared to project objectives and expectations.	The objective of this research is to evaluate the value of the IT continuity maturity model. Maturity model relevancy and value is reviewed from five different process and management view points that reflect the key stakeholders and the users of IT continuity management maturity model: - Service management - Line unit organisations - IT governance - Corporate governance, and - Individual At this stage the author's role was to collect the data, analyze the result and document the findings.
Specifying learning, which reflects on what has been learnt and how the whole effort has been reported and updated to the relevant knowledge base and the body of knowledge documented. It should enable the action researcher to reach a decision as to whether or not to proceed through an additional process cycle. Eventually, the action researcher has to exit the project. The exit of the researcher should be related to the achievement of the specified objectives or to another explicit justification.	This thesis provides the premise for the learning of the maturity model usability, utility and reliability in IT continuity management in the target organization. From academic point of view this thesis was written in a form that allows publishing in a public forums, e.g. journals.

Table 3 The comparison of canonical action research phases and the IT continuity maturity model development (Syrjänen 2009.)

The third principle highlights the role of theory in canonical action research. Davison, Martinsons & Kock (2004) acknowledge that a canonical action research project may begin with theory-free action learning. However, akin to the traditional scientific method, the diagnostic stage provides a starting point of comparison for the post-implementation evaluation. Action researchers need to rely mainly on one or two theories as these will guide their activities and keep the research objectives on the track. The theory behind the IT continuity maturity model introduced earlier on this chapter supports Davision at al. viewpoint, even though the model was initially created based on the real life experience and benchmarking the industry best practices.

The fourth principle reflects the necessity of action and change, with intervention seeking to produce change. In order for meaningful action and change to occur, the researcher and the client must have a common understanding of the organizational situation which doubles as the research context. The target organization situation during the initial stage on the maturity model development was favorable as the initial trigger for the activity was business-driven (Chapter 2.1). Even though the target organization is under a constant change, the conditions remained favorable for IT continuity maturity model development as continuity management was seen critical for the operations and securing the revenue.

Davison, Martinsons & Kock (2004) assert that the explicit specification of learning is the most critical activity in action research. The rationale for the fifth principle, the Principle of Learning through Reflection, stems from the multiple responsibilities of the action researcher: to clients and to the research community. This is consistent with the common call for research reports to specify the implications for both practice and (further) research. Clients will focus on practical outcomes while the research community will be interested in the discovery of new knowledge. Since the beginning of the IT continuity maturity model development the collaborative arrangement between the author and the client organization was clear, regardless of the author's dual role between the target organization and in the field of academic. From the viewpoint of the target organization the author's responsibilities included both the key developer and the change agent roles. In the beginning of the maturity model development the author worked as a specialist in the field of IT continuity management. Gradually the initial responsibilities changed from a specialist to a member of a senior management at the same pace than the maturity model was implemented across the IT organization. As a result, the role of facilitator of change turned into overall management of the IT continuity. One could say that the implementation of the maturity model grew also the author's own professional maturity. Throughout the whole process the author was also a member of an academic community, completing master studies in the Laurea University of Applied Science. The dual role as a researcher and the change agent provided an opportunity to share knowledge over the boundaries of academics and business.

3 Framework of the evaluation

3.1 Evaluation objectives

IT continuity planning process with success criteria has now been in use for 3 years in Company IT. Continuity management objective settings and status follow up are based on this maturity model throughout the IT organisation. Although the practice may represent the best practice approach and is linked to industry standards, there are still some questions to be asked:

- How well is the model adapted into the organization's governance model and management?
- Does the approach support actual implementation of IT continuity planning?
- Has the model increased awareness of continuity management?
- What concrete impacts does this have for service delivery promises and,
- Does the maturity model really build assurance that information systems and services can be recovered and restored as required?

Summarizing all questions above has the Company really gained such concrete benefits that this maturity model can be regarded as a reliable approach for IT continuity management performance measurement and should be used in the future? Can we verify the theory that the maturity model will work as a catalyst for IT continuity management implementation and improvement of the real capability to react and respond on continuity related incidents?

Objective for this analysis is to evaluate the IT continuity maturity model development, implementation and implications in the Company IT department between 2007 and 2009. As an outcome, this study should provide insight into the role of measurable maturity model in continuity management implementation in IT organisations' management frame work. The ultimate objective is to verify if the model work as a catalyst for improved IT continuity management.

3.2 Data source of the evaluation

Järvinen & Järvinen (2004, 145 – 166) introduce several methods of collecting information for empiric research. According to Järvinen & Järvinen, the most common methods are interviews, observations, surveys and documentation reviews. All these methods can be divided into subcategories based on the tools used during the research and the role of the researcher. The role between the author and the organization made it possible to use several methods for data collection. The most important data sources for this analysis were reviewing the documents and observing the process and its progress.

According to Järvinen & Järvinen (2004, 154-157) data collection using the observation is based on the notes taken by the researcher. In practical terms this means that the quality of the data is fully dependent on the researcher's own experience and training. Even though research subject's behaviour may increase uncertainty, flexibility of this approach allows capturing the events and details that could not be found by other means. According to Järvinen & Järvinen observation as a data collection method fits well for situations in which the research subjects are social groups and processes. This method allows the researcher to be a part of the research subject e.g. participate in the process implementation or its development. Based on the author's role in the maturity model development and the research subject itself, observation as data collection model was an obvious choice.

During the IT continuity maturity model evaluation, data about the use of the maturity model and its perceived value was collected from the following research subjects with the help of discussions and observation:

- 20 IT service teams (10 of these managing critical information systems)
- IT continuity specialist team
- IT Service management team
- senior IT management team
- corporate and IT assurance related specialists (total: 15 people)

According to Järvinen & Järvinen (2004, 154-157) perhaps the biggest challenge in collecting the data by observation is the researcher. The reason for this is the fact that the researcher's own perception about the research subject will have an effect on the interpretations he will make. Basically there are no controls that prevent the researcher from collecting the wrong data and from making wrong interpretations. Another challenge is how to observe people so that the researcher's presence will not affect research subjects' behaviour. In order to mitigate the known issues related to observation method, the author reviewed relevant documentations and reports on IT continuity maturity model.

Järvinen & Järvinen (2004, 156) underline that any documentation that is not designed for the purpose of the research is a secondary data source. Regardless of this statement the available documentation concerning the IT continuity maturity model analysis were mostly statistical reports about the process implementation and recovery capability. So even though the documentation was not designed for the research, evidence for the maturity model evaluation was available. Following document types were reviewed and analysed by the author:

- documented statistics from information services' quality and trends
- critical incident reports and business impact analysis

- continuity maturity monthly reports
- documents about on-going continuity development actives
- individual incentive score cards
- IT score cards

3.3 Measuring the maturity model

Hevner, March, Park & Ram (2004) provide a guideline for design evaluation. According to them, the utility, quality and efficiency of a design artefact must be rigorously demonstrated via well-executed evaluation methods. IT continuity management maturity model evaluation is based on both qualitative and quantitative measurements. The qualitative measurement is based on the perceived value of the maturity model for the users and the stakeholders. In practise this is based on how well the IT continuity maturity model serves the users' and the stakeholders' objectives. The analysis is based on the author's observations and impressions of how the users and stakeholders utilize the IT continuity maturity model. In this context users are all individuals, teams and units who utilize the IT continuity maturity model partly or fully in their work and objectives. Stakeholder in this context refers to the people in charge and representative of governance and management models related to IT continuity management. Based on this the taxonomy of the organization entities and subjects represents the users' and the stakeholders' viewpoint:

- service management
- line unit organisations
- IT governance
- corporate governance, and
- individual

The quantitative analysis is based on statistics derived from the incident and maturity level reports. Following chapters will introduce only the concept of quantitative analysis used while estimating the value of the IT continuity management maturity model for the organisation. Quantitative analysis is based on the:

- documented statistics from information services' quality and trends
- critical incident reports and business impact analysis
- continuity maturity monthly reports

Concrete outputs from continuity planning are the solutions that are not only reactive controls but will also increase the level of information system resiliency. All incidents cannot be avoided but if the IT environment is designed to be fault tolerant and resilient, incidents

should not escalate to a critical level as controls will prevent this from happening. The theory is that there should be a positive correlation between the number of critical incidents and continuity maturity levels. The basic assumption is that when IT service has a tested plan how to respond to a different situations they should be able to limit the damage so that the incident will not escalate to a critical level. As a result, the number of critical incidents should decrease when maturity levels get higher (Figure 4).

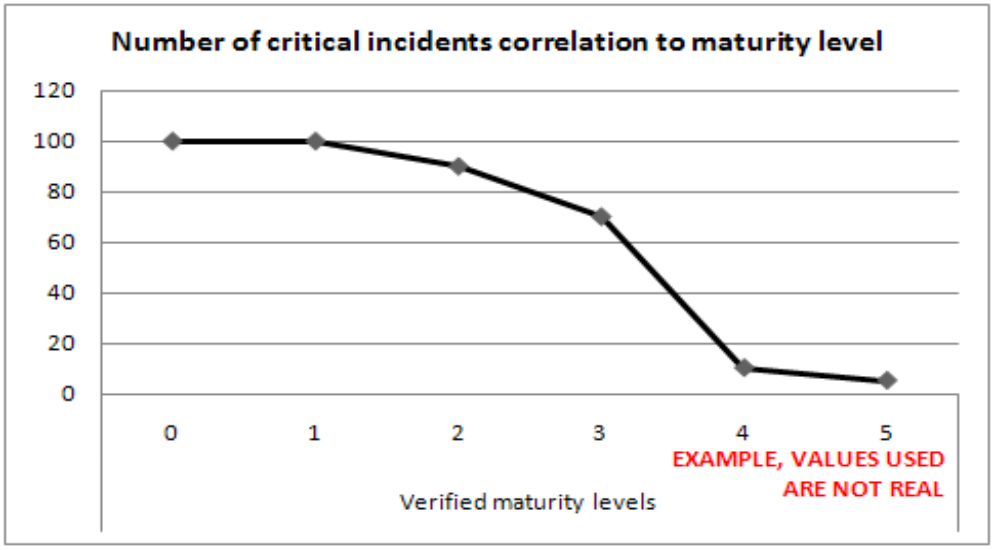


Figure 4 Example of how the number of critical incidents occurred should correlate with the IT continuity management maturity levels (Syrjänen 2009.)

The total time of service recovery and restoration is dependent on the incident respond time so it is important to keep this time as short as possible. One way to assess the success rate is to collect actualized incidents and evaluate the speed of incident response. The basic theory is that there is a positive correlation between the short resolution time and continuity maturity levels because testing and exercising should improve the response time. If this assumption is true then all maturity level 5 IT services should be able to meet or even to exceed the agreed time to resolve incidents. Figure 5 demonstrates assumed correlation between the rate of successful responses and the maturity level.

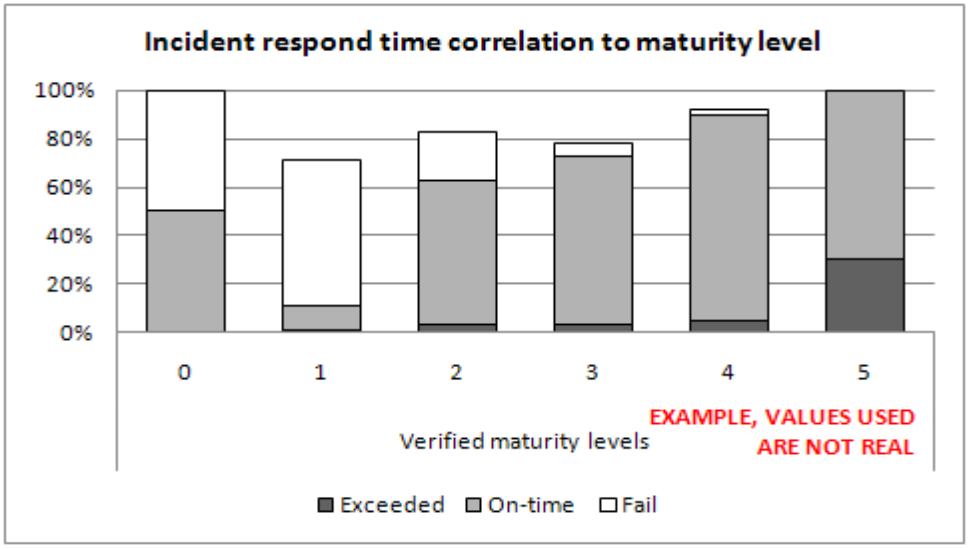


Figure 5 Example of how incident respond time is used for IT continuity management maturity model evaluation (Syrjänen 2009.)

If critical incident occurs despite all the actions, recovery actions are required to be executed timely. Successful recovery can be analyzed by using two units of measurements. Recovery time objective (RTO) is a target time set for resumption of product, service or activity delivery after an incident. If recovery is successful, recovery time should not be more than agreed on continuity plans and service level agreements. The second unit of measurement is recovery point objective (RPO) which is a point in time to which data has to be recovered in order to resume IT services. In practice successful recovery is made if the usable data restored is not older than what is agreed on continuity plans and service level agreements. In order to define what successful recovery is, both RTO and RPO requirements must be fulfilled. In theory percentages of successful recovery actions should correlate with the higher maturity level as figure 6 demonstrates.

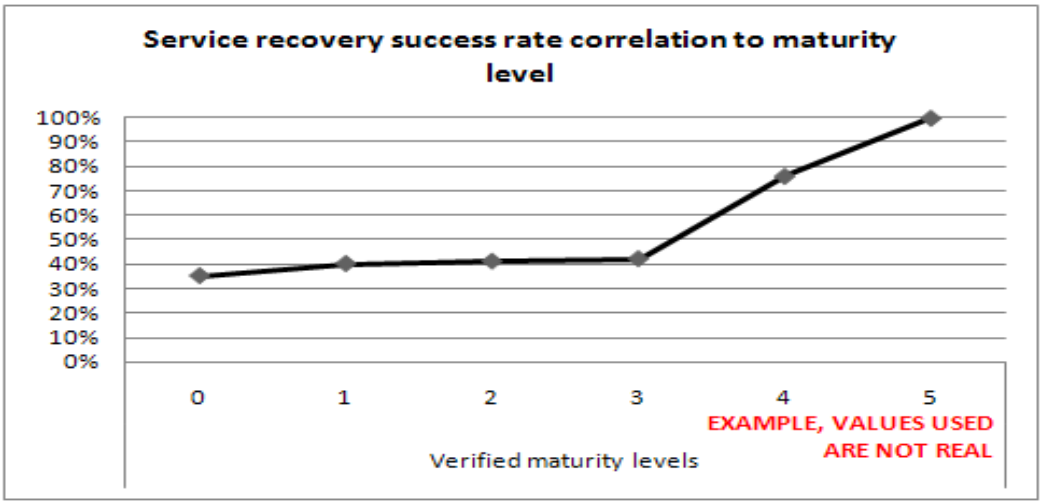


Figure 6 Example of how successful recovery cases are used for IT continuity management maturity model evaluation (Syrjänen 2009.)

The bottom line from the business point of view is that IT continuity management should be able to reduce loss of business and cost of downtime. If the continuity management maturity model creates real value for business, it must be visible in terms of money saved. The basic assumption is that higher maturity level correlates with decreased level of total cost of downtime as demonstrated on figure 7. Total cost of downtime in this case includes the sales value lost, service/ product production costs and the cost of resource (time, money and tools) used during the recovery.

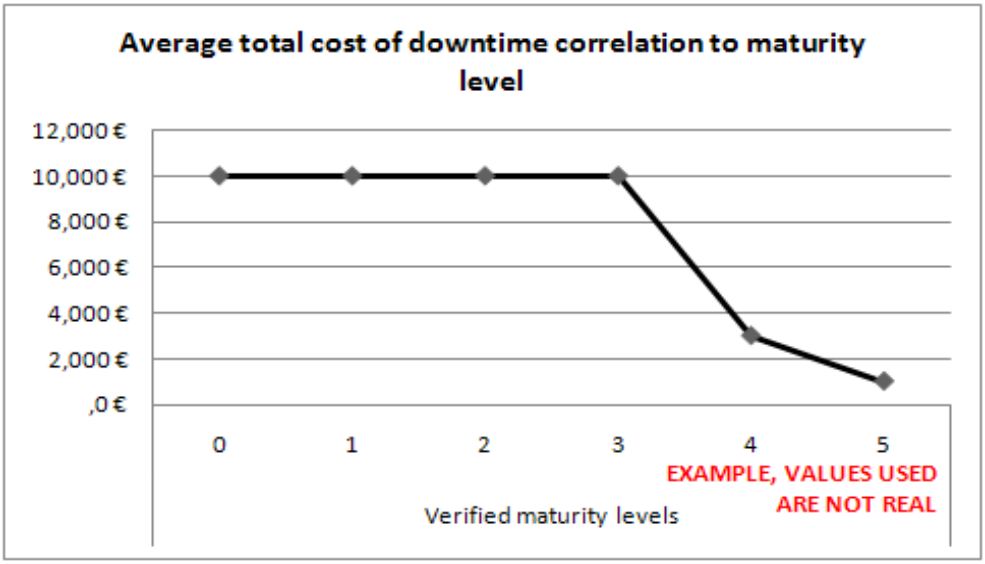


Figure 7 Example of how total cost of downtime should correlate positively in case IT continuity management maturity model should prove its value to business (Syrjänen 2009.)

4 Maturity model evaluation

4.1 Value to IT service management

ISO/IEC 20000 (2005) standard provides a management system for information services. This model integrates a number of IT processes into one management system allowing the IT organisation to avoid overlapping between the processes, to allocate resources, to measure activities against objectives and to improve process performance. The overall goal is to meet end customer quality requirements, managing costs with balanced level of assurance of service continuity. Service management follows the plan, do, check, act methodology while managing process to process alignment, change management and linking to business objectives and requirements. Service continuity is one of the main processes the objective of which is to ensure that agreed service continuity and availability commitments can be met in all circumstances. (ISO/IEC 20000, 2005.)

At the time IT continuity management maturity model was developed, the service management framework was under a planning phase. Due to this reason, continuity management was managed independently until the service management implementation phase was initiated. The purpose of service management was to provide a central management entity and unify all IT service demand and delivery processes. By that time all relevant IT processes were reviewed against ISO/IEC 20000 standard before implementation. In order to have successful integration between the processes it was seen vital that:

- roles and responsibilities were defined in each process
- process terminology and deliverables were equivalent with ISO/ IEC 20000
- the monitoring, measuring and review methods for each process were defined

IT continuity planning process was built on five phases, each with different objectives, outcomes and interest groups. First phase objective was to understand reasoning, requirements and risks regarding continuity management. This phase required strong competence in business case building and impact analysis as well as direct interaction with business stakeholders. The objective of the second phase was to identify and list available solutions with cost/benefit calculation. Approval for the final selection was received from the business owner before starting the implementation. As service managers' role was considered important in requirement management it was natural that responsibility for the first two phases was given to service managers.

The objective of continuity planning phases 3, 4 and 5 was to implement selected solutions, ensure competencies and verify continuity solution functionality by carrying out technical exercises. The implementation of the three phases was assigned to computer managers and technical configuration managers, who were already responsible for service deployment and delivery. Because of the similarity between the tasks in continuity management and the general IT management workloads did not grow. Due to this reason, incorporating the continuity planning responsibilities as part of managers' current roles increased their commitment remarkably.

In order to support the implementation a simple RACI (Responsible, Accountable, Consulted and Informed) table (table 3) was published and communicated widely. Due to the simplicity of this tool, communication concerning the IT continuity management process and each role was easy.

		Service manger	Computer manager	Configuration manger	Continuity team	Process owner
Create	Initiate and co-ordinate IT continuity creation process	A/R	C	C	C	I
	Understand risks and business impacts	A/R	C	C	C	I
	Assess solutions and get business approval	A/R	C	C	C	I
Deploy and maintain	Implement the plan according the strategy	A	R	C	C	I
	Communicate the plan scope and objectives	A	R	C	C	I
	Maintain competence by training	A	R	C	C	I
	Test the plan regularly	A	R	C	C	I
	Up-date the plan on demand	A	R	C	C	I
Continuity management	Process and documents validation	I	I	I	R	A
	Monthly management reporting	C	C	C	C	A/R
	Process development	I	I	I	R	A
	Process communication and awareness	I	I	I	R	A

Table 4 IT continuity management "Responsible, Accountable, Consulted, Informed" -model (RACI) (Syrjänen, 2009.)

According to ISO/ IEC 20000 (2005, 12) IT service continuity strategy should be based on maximum acceptable continuous period of lost service and degraded service levels during a period of service recovery. Continuity plans should be extended to take into account dependencies between service and system components. These documents should be stored and maintained so that these are up-dated and available when needed for recovery purposes. (ISO/IEC 20000, 2005.)

Since overlapping documents could create confusion among users, it was imperative to review all IT planning and operative documents and align these with IT continuity related documents. Due to this reason IT continuity team developed and released document templates for continuity planning purposes. As an example, IT back-up, recovery and restoration instructions were defined as sub-documents for the purpose of combining all the proactive and reactive controls together. In addition to the IT continuity plan template, risk, impact analysis and technical exercise result templates were released.

In order to ensure that relevant IT continuity documents are created and stored appropriately, IT services must pass a validation before they are allowed to move on to the next phase of the maturity model. This validation was carried out by continuity professionals, who reviewed the content and the result. To make sure that IT services understood the reasoning for approval and rejection, validation criteria was published and shared with all services. The

validation criteria contained a checklist that IT services could use for self-assessment before sending documents for validation team. Openness with maturity level evaluation and using a common scale for measuring the progress built confidence between the continuity specialist team and the service managers.

The validation process of the IT continuity documentation verified that outcomes of each phase were consistent and the document quality met the standards. Having validated the service continuity planning deliverables, validation team informed the IT service team about the results. This information was also delivered to the IT continuity management process owner, whose responsibility was to provide an IT level continuity status report to senior management (Figure 8).

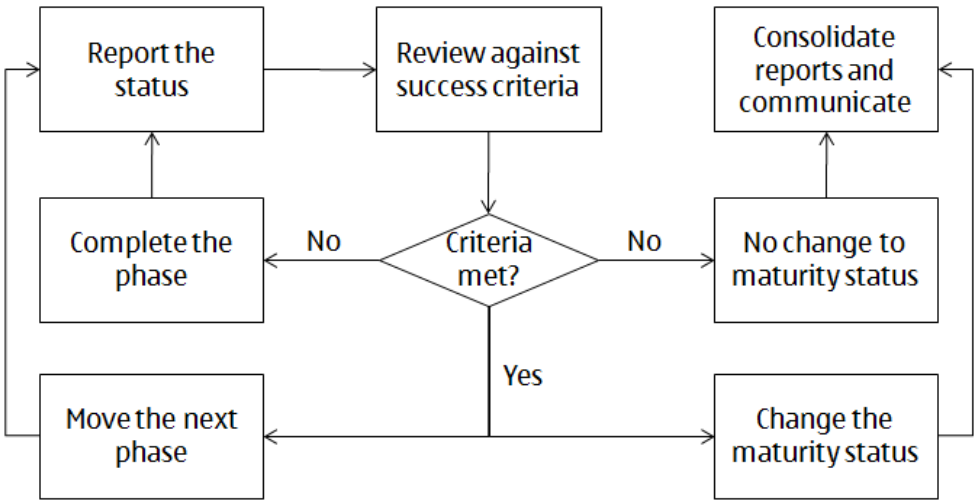


Figure 8 Maturity status validation process (Syrjänen 2009.)

After reviewing the process used in IT continuity management, the IT service management developers supported the idea that the process could be integrated directly into the IT service management model without additional changes. This impartial expert review also proved that the model was consistent with industry standards and could therefore be easily used either as an independent management system or as a subsystem of another management system. One of the findings was that the true driver was not the process itself but the simple tools and clear responsibilities between teams and managers.

4.2 Value to IT line organisation

Company IT is a matrix organisation. On the vertical axis operations were process driven and on the horizontal axis dedicated units were responsible for managing resources and assets. Time allocation of resources was based on semi-annual planning process. In practice, business objectives were converted into unit, team and individual level objectives for the upcoming 6

months. After the closure of each planning cycle, managers reviewed how well objectives were reached by using criteria for minimum, target and maximum level performance. Successful performance result would lead to high payout to teams and individuals, while a poor performance would lead to a smaller reward, if any.

As IT continuity management was one of the key areas having a strong business support, the ability to link planning phases into the objective setting and performance evaluation was seen important by the management. In order to support the units' planning process and service team members' objective settings, the continuity team developed an IT continuity objectives scorecard. The scorecard provided the baseline objectives and performance criteria for each maturity level. The IT teams could reflect the current continuity maturity status the one defined in the scorecard and set new objectives. Important part of scorecard implementation was to generalize it in such a manner that the scorecard could be adapted across the IT organisation. This allowed a wider group of IT professionals to be part of continuity maturity model objective settings.

Team objectives on the scorecard (Attachment 2) were initially designed so that IT service teams' achievements were expected to progress level by level until the highest level of maturity was reached. After the highest maturity level was obtained, teams' objective was to focus on different types of continuity exercises. Later, the objective scorecard contained two measurement parts focusing objectives to continuity exercises only.

The target group for the first part were all the IT service teams whose applications' continuity maturity status was on phase 5, meaning that all phases were completed and validated by the continuity team. For this target group the objective was to maintain phase 5 status providing sufficient evidence on how well technical exercises were conducted and what action plans for improvements were available. The target group for the second part were the teams whose applications' continuity maturity status was under the phase 5. For these teams the objective was to complete the planning and implementation phases including the technical exercises.

In order to achieve the maximum performance level IT teams had to complete the continuity exercise. Integrating the reward system with the maturity model increased the number of technical exercises and, by that, assurance of working recovery solutions. One of the key challenges was the fact that due to several reasons technical exercises may need to be postponed. This might decrease motivation and affect the teams' commitment. The challenge was solved by designing the risk acceptance criteria that would be signed by the business owner, thus freezing the IT continuity progress until it could be continued. This approach

ensured that even if the IT continuity planning progress was on hold, it would not have a negative impact on the reward system of individual employees.

Overall perception was that IT continuity management maturity model provided a solid foundation to line management purposes as planning phases were linked to people's roles. One of the success factors in getting teams and individuals to commit to the continuity objectives were the transparent and equal performance metrics used.

4.3 Value to IT governance

IT governance integrates and institutionalizes good practices to ensure that the enterprise's IT supports the business objectives. It enables the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities, and gaining competitive advantage. IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives. (COBIT 2007, 5.)

To put it short, a well established IT governance model should ensure that:

- IT enables the business to maximize benefits and opportunities
- IT resources are used responsibly
- IT risks are managed appropriately

According to COBIT (2007), strategic alignment focuses on ensuring the linkage between the business and the IT plans defining, maintaining and validating the IT value proposition, and aligning IT operations with enterprise operations. Due to the nature of the business and the end customer expectations and regulations, business continuity management has an important role in the Company's strategic initiatives and operations. As an example, business continuity related policies require each business and support unit to implement continuity management practices throughout the whole organisation. With the help of the IT continuity maturity model, the IT directors were able to demonstrate that continuity management was aligned with the strategic and operational objectives of the Company. Capability to demonstrate the managed approach has strengthened the business directors' trust in IT's capability to ensure continuity of IT services.

Value delivery is about executing the value proposition throughout the delivery cycle. In practice this means that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT. IT continuity maturity model was de-

signed so that process steps which would normally be extensively documented were summarized into few pages and support documents. In addition the work routines were embedded in the normal management processes avoiding overlaps with the similar process. All above reduced the complexity of the process and, by that, optimized the planning and implementation work.

One of the key objectives for the business critical processes was to decrease unplanned downtimes. After comparison of the monthly availability reports and the IT continuity maturity levels, the correlation between decreased down times and higher maturity levels was undisputed. As an example, one of the business owners reported about an incident related to failure in IT: "We faced a serious incident and invoked the continuity plan. Thanks for the recurring exercises we managed to recover and restore the system so fast that there was neither downtime nor slow down" (Major incident report 2009). Due to the continuity management maturity model the Company has gained remarkable savings and increased customer satisfaction. Whether this could have been achieved without the maturity model is not known but the results displaying the correlation should not be ignored.

Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure (COBIT 2007). In order to ensure optimal implementation of the IT continuity management maturity model it was enforced only for the IT systems and services related to critical business processes. For the non-critical IT services the use of maturity model was optional. As a result, this increased teams' commitment as now there was a rationale why the IT service team should use time and resources for continuity planning.

The concrete benefit of using the maturity model reporting function was that it provided a transparent information hub between the critical IT services. In practice, IT services could collaborate and plan objectives that would support the resolving of mutual challenges like reusing a common recovery solutions. As a result IT service teams avoided double work and increased the efficiency of the organisation.

The primary target of the IT continuity maturity model was to steer planning teams into step-by-step to continuity planning and implementation. Even though the focus was more on overall process management, the deliverables from each process phase provided information also for other management purposes. As the business impact analysis included loss value calculations and information about cross dependencies, the results could be used for information systems classification. Communicating the findings of the continuity tests and exercises improved end-to-end continuity planning between the business and IT units.

According to COBIT (2007), risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding risk management responsibilities into the organisation. From the risk management viewpoint, maturity model and its deliverables provided valuable information for several purposes. First phase performance criteria required that each critical IT service must complete a risk analysis in order to progress to the next maturity level. Continuity risk analysis provided insight into risks related to technology, people, processes and infrastructure. All these may interrupt the services for prolonged time or, even worse, cause a total loss of data. By comparing the results of risk analysis across the IT services and IT units, risks managers were able to identify signs that may indicate changes on risk level and which would therefore require more attention from the management.

Risk, by its very definition, always includes uncertainty about the severity of impact and probability of occurrence. The phase 5 performance criteria of the continuity maturity model required that application and service should have undergone technical exercises. The technical exercises provided the risk management with information about the capabilities to respond to interruption and disruption risks revealing the residual risks. Capability to measure and provide validated technical exercise reports was valuable for corporation risk management, as this information could be used for group level risk reporting. One of the most concrete benefits was that maturity level information could be used for insurance negotiations. Ability to demonstrate tested and validated continuity plans did have a positive impact to the insurance premiums.

According to COBIT (2007), the purpose of performance measurement is to track and monitor strategy implementation, project completion, resource usage, process performance and service delivery. As an example, this can be done by using balanced scorecards that translate strategy into action to achieve goals. The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After critical IT processes and controls have been identified, maturity modelling enables gaps in capability to be identified and demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target level. (COBIT 2007, 5.)

With the help of IT continuity maturity model it was possible to create a scalable scorecard that transformed planning phases into measurable actions. The standard unit for measurement was a single IT system and its maturity level. Table 5 demonstrates how to measure the number of critical IT systems that have met the continuity maturity performance criteria on each of the four IT units (A, B, C and D).

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
IT Unit A (16 IT systems)	3	5	4	2	4
IT Unit B (13 IT systems)	1	4	2	4	2
IT Unit C (16 IT systems)	0	2	4	5	5
IT Unit D (21 IT systems)	5	6	7	1	2
TOTAL:	**9**	**17**	**17**	**12**	**13**

Table 5: The Simplified scorecard for maturity measurement. Given values are only examples, not real figures (Syrjänen 2009)

The simplified scorecard provided a snapshot about the current situation of target units and IT systems, but as such did not provide enough information for continuous follow-up and reporting. The gap was solved by combining each system's maturity level with the time dimension. This simple approach made it possible to create an IT continuity maturity scorecard that could be used for reporting the continuity management status of the whole IT. For the purpose of this thesis the author has designed an illustration of the IT continuity maturity scorecard (Attachment 3) with pseudo data.

Status bars on the IT maturity scorecard (Attachment 3) show how the imaginary IT teams are progressing with the given continuity planning objectives. As this example demonstrates, the first part of the year shows that most of the measured IT systems were on initial phase, making business impact analysis and collecting requirements. Based on this information the conclusion is that there is 0% assurance that systems are recoverable in case of a major incident. Status information from June shows that 25 systems out of 40 have completed the technical exercise required in phase 5 by successfully demonstrating verified capability in recovery and restorations. The remaining 15 cases have progressed well but continuity capability is not yet proven. When reviewing the end of the year results, we can make a few observations. There have been changes between the initial number of the measured units and the end year numbers. Common reason for this is the natural lifecycle of the IT systems e.g. ramp downs and integrations. 95% of the systems managed complete technical exercises, which can be translated as an increased level of assurance in recovery capability. Even though this is merely an example of how to use the IT scorecard, it underlines the importance of consistent and comparable metrics. A useful side benefit is the power of visualization when communicating the results to the senior management.

The office of CIO (CIOO) was responsible of collecting and consolidating all information about the quality of operations and the progress of strategic initiatives. Along with other priority IT processes IT continuity was one of the key processes that needed to be reported to the senior

management. A challenge for a small unit was how to be able to keep reporting process light but still be able to provide reliable information for IT scorecards. This problem was solved by using the IT continuity maturity model reports.

Due to the simple model, continuity status information was collected directly from the IT service teams and analyzed in a relatively easy manner. The status of continuity management was easily adopted by the senior management, as the link between the continuity objectives and performance was consistent and traceable. For the first time senior management could set measurable objectives to the whole IT in continuity planning and be able to follow the progress. Possible issues on the progress were easy to spot and, if necessary, management could initiate corrective actions and allocate extra resources for continuity management.

4.4 Value to corporate governance

According to the Finnish Central Chamber of Commerce (2003), corporate governance can be defined as a system that helps managing and controlling the enterprise. In order to succeed in this objective, enterprises are expected to comply with several regulations and external drivers. The term compliance is either a state of being in accordance with established guidelines, specifications or legislation or the process of becoming so. In the legal system, compliance usually refers to behaviour in accordance with legislation. Compliance in a regulatory context is a prevalent business concern; in the Company compliance can be split into two areas 1) compliance against external regulators and 2) compliance against internal regulators.

The information security and crisis management policies of the Company state that information services must provide documented business continuity and disaster recovery plans. This requires rigorous actions in order to ensure that business continuity arrangements will work within critical timescales as planned. Corporate IT has responsibility for developing a framework that includes plans and procedures for building resilience on such a level that it will support business in a balanced manner. Given policies underline the importance of validation of the agreed actions, therefore plans should be reviewed and tested on a regular basis and in case risk levels have increased.

Sarbanes-Oxley Act (SOX), issued for U.S. legislation by the Securities and Exchange Commission (SEC), requires enterprises to document audit and use controls to ensure correctness of the financial reporting. Common assumption is that continuity management is part of the SOX control frame, however the standard clearly states that a company's business continuity or contingency plans have no effect on its current ability to report financial status. Though continuity management is not a mandatory control, daily backup procedures should be addressed in management's assessment of internal control over financial reporting. Appropriate backup

and recovery procedures allow for proper control over the restoration process, ensuring the integrity of the information; therefore it provides an important financial reporting control. (Price Waterhouse Coopers 2004, 67.)

New York Stock Exchange (NYSE) Rule 446 (2004) requires that members and member organisations must develop and maintain a written business continuity and contingency plan establishing procedures relating to an emergency or a significant business disruption. In addition, each member or member organisation must disclose to its customers how its business continuity and contingency plan addresses the possibility of a significant business disruption and how the member or member organisation plans to respond to events of varying scope.

Security, internal control and risk management functions' role is to ensure the implementation of the control framework according to relevant regulations and operating principles. As the Company policies and external regulations require, the organisation should be able to demonstrate its continuity capability, which also covers information systems. Beside the need to comply with the regulations and policies, external groups are requesting information about the current continuity status while securing their own delivery channel and business. As an example, insurance companies regularly assess risk level as a part of insurance practice and information system related risks are under this assessment.

Regulations, policies and best practices emphasize that IT continuity management and recovery planning are two of the key controls in minimizing the loss of critical data and ensuring continuous business processes. An important success factor for an external audit or assessment is the organisation's capability to provide fact-based information about effectiveness of the controls and coverage over the company's critical functions and its assets. Due to a consistent and verified maturity model, the Company IT has the ability to deliver up-to-date fact-based information about the capability of the IT services and systems to respond and recover in case an incident occurs. In addition, demonstration about rigorous continuity management system builds trust between the Company and its partners, not to forget co-operation with the local emergency authorities.

From internal control, security, and risk management point of view, the maturity model has provided an excellent tool whenever there has been a need to review and report IT continuity capability to stakeholders. In addition, the continuity maturity model has been so effective that it has been benchmarked also by other process areas and adjusted for their own use. This may provide an excellent answer to the question "did the model bring any value to business"?

4.5 Value to individuals

What does the model provide for a single member of an IT community i.e. “What’s in it for me”? This is a question we all would probably want to ask when we start working with new tasks like IT continuity management. For the past three years the Author position has allowed him to have constant communication with the IT service team members. This communication has contained two main topics: 1) explaining to the new service managers what IT continuity management is all about and why they need to do it 2) discussing and agreeing on a given team member’s individual objectives and incentive planning.

The research revealed that the topic continuity management is a difficult subject for many. Change resistance seemed to high at the start of communication but disappeared soon after. Based on the feedback from the IT managers the workflow was easy to follow as the steps were practical and target-oriented. The success criterion of each phase emphasizes the end result and allows the person responsible to decide how to accomplish this result. According to discussion with the IT managers in most of the cases the feedback about the model could summarized in a words of “I understand what is expected from me and I can choose how to do that”. This implies how important it is for the doers to control their own work in order get a high level of commitment to the objectives.

Individual incentive planning is one of the most important reward systems in the Company. From an individual’s point of view it is important that objectives can be set and measured explicitly in order to avoid any interpretations about the level of achievements. Another important feature was that the objectives are fixed, not changed randomly. For both viewpoints the maturity model provided a structured solution as IT continuity management objectives are based on static and measurable success criteria. This transparent approach allowed IT managers and their team members to include continuity management related tasks as a part of the individual reward system.

5 Conclusions

The overall goal of this thesis was to review what kind of value the IT continuity maturity model has brought to the target organisation and its business objectives. Based on the research findings the **model has worked as a catalyst for increasing awareness about continuity management**.

At the time of writing this, the maturity model has been used for three years and is a widely adopted method of setting objectives and measuring success in continuity planning. The way **people communicate about the continuity capability** demonstrates how well the model has

been accepted among various interest groups in the IT organisation. It is notable that stakeholders from business and IT management **understand in a consistent manner** the reported maturity levels. **When communication reaches a level where a single value and its implications are understood widely in the same way, it indicates a successful implementation of a common model and terminology**. It is safe to assume that one of the success factors for the implementation was **a simplified process model using terminology that is familiar for most of the process-oriented teams instead of using business and IT continuity terminology.** This, in turn, made the simplified senior management reporting possible, as senior management understood the content of the report. Results indicate that this was the key for **increased management commitmen**t and support for IT continuity management.

The maturity model was tightly linked to individual objective setting and the reward system so it is natural to assume that using the maturity model the teams' commitment to plan and implement continuity solutions timely was increased. Recent observations among the IT service units revealed that the **IT service teams are interested in using the maturity model as a part of their incentive planning**. This kind of feedback increases confidence that the model measures the right things also in people management level. Linking the model to the reward system has also **increased curiosity among other than the critical IT service teams.**

Observations revealed that **IT services that had reached maturity level 5 managed critical incidents and recovery actions successfully in all reported cases**. Even though the number of incidents did not reduce remarkably, **the number of critical incidents decreased** as incidents were handled in a timely manner before they could escalate to a serious level. In terms of money, the correlation between the cost of downtime and maturity level was obvious: **the higher the maturity level, the lower the total cost of downtime**. Thus, the IT continuity management maturity model **business benefits were realized on a very concrete level**.

The success factor for the maturity model implementation was the way it **connected IT service teams' incentive planning to completion of successful technical exercise and gained the senior management's attention.** As an indirect consequence of this method the increased management support enabled IT service teams to build solutions that prevent and limit the critical incidents in practice. The inevitable conclusion is that **the maturity model (soft approach) had a positive effect on the designing of resilient information systems (hard approach) and increased assurance of effective IT continuity management**. Summa summarum, maturity model did make a difference as it pulled the IT organisation into an IT continuity management practice in which no other method had so far succeeded.

6 Discussion on results

6.1 Achieved results

As the scope of this thesis was a large and relatively homogenous organisation, the observations may not apply to other organisations in a similar way. In order to validate the results from this study, one should conduct a similar type of research in another organisation. By extending this research to cover more than one organisation a researcher should be able to do benchmarking between the organisations in scope. This may be somewhat challenging as, based on my personal perception and experience on the field of business and IT continuity management, maturity models are rarely used. Another challenge for doing this type of research is that continuity management related information usually contains facts about the company vulnerabilities and failures. This type of information is often treated as sensitive and therefore cannot be published on a level that scientific publications require. This was also the reason why I did not use statistics from the IT service reports. Although exact facts and figures had to be excluded from this thesis, I hope it will still provide insight about what benefits maturity model implementation may provide for a company.

Although the research results were surprisingly positive, one question remains: could this achievement have been reached without the IT continuity maturity model? In order to be able to answer this question, the unique element of the maturity model that underlines its success must be identified. In my opinion the key was the means to convert standard process into pragmatic and measurable steps so that the whole concept was understood by the senior management. To put it short, the model succeeded in drawing the management's attention. Regardless of the method, standard or language I strongly believe that any method will succeed if it has management support from the very start of implementation. Thus, this research also reveals the necessary success factors for implementing any type of process. My conclusion is that this achievement could have been reached by other means too as long as management support was secured. I believe that in order to design a working maturity model, understanding of organisations' management practices and the dynamic that motivates people such as individual incentives is required.

6.2 Measured results

When discussing the results, it is sensible to take a few steps back and reflect on the results using an objective measurement. This can be done by using a commonly accepted maturity model originally created by P. Crosby in 1979 and later developed and maintained by Carnegie Mellon University and Software Engineering Institute. The Capability Maturity Model integration (CMMI for Services 2009) also known as CMMI is a collection of best practices from government and industry. Over time, the model has evolved and the latest version is targeted

to evaluate information and IT related process maturity levels reflecting the following industry standards:

- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 20000: Information Technology—Service Management
- Control Objects for Information and related Technology (CobiT)
- Information Technology Services Capability Maturity Model (ITSCMM)

CMMI highlights that the quality of a system or product is highly influenced by the quality of the process used to develop and maintain it. In practise this means that the maturity level of an organisation provides a way to predict its performance in a given discipline or set of disciplines, for example BS 25999 BS 25777 continuity standards. According to the standard, experience has shown that organisations do their best when they focus their process improvement efforts on a manageable number of process areas at a time. The standard provides five maturity levels, which are used to characterize organisational improvement relative to a set of process areas, and capability levels to characterize organisational improvement. (CMMI for Services 2009.)

On maturity Level 1 processes are usually ad hoc and chaotic. The organisation usually does not provide a stable environment to support processes (CMMI for Services, 26). Reflecting this definition, the Company IT continuity management model is far more sophisticated as it is fully managed and organized.

On maturity level 2, projects, processes, work products, and services are managed. Process adherence is periodically evaluated and process performance is shared with senior management (CMMI for Services, 26). Reflecting the maturity level 2 definitions, the IT continuity management evaluation proved that the process is managed as there are nominated people whose responsibility it is to develop and implement the model. As demonstrated earlier, the maturity model is used for management reporting providing information to senior management on how the IT continuity management implementation is progressing.

On maturity level 3, rules are integrated into the current process portfolio. Processes are well characterized and understood and are described in standards, procedures, tools, and methods. On maturity level 3, processes are described more rigorously than on maturity level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. (CMMI for Services, 27.)

IT continuity maturity model is defined, documented and it provides tools for each process phase. Roles and responsibilities are defined and, furthermore, there are clear verification

steps in order to keep the quality of the process outputs on a desired level. In this case the desired level is capability to respond to incidents and continue operations without interruptions. Evaluation has proven that all the CMMI maturity level 3 requirements are carried out; in some cases on a rigorous level, e.g. when it comes to technical exercise requirements.

On maturity level 4, the service providers establish quantitative objectives for quality and process performance and use them as criteria in the managing processes. Quantitative objectives are based on the needs of the customers, end users, organisations, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of the processes. Performance models are used to set performance objectives for service provider performance and to help achieve business objectives. A critical distinction between maturity levels 3 and 4 is the predictability of process performance. On maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques and is quantitatively predictable. On maturity level 3, processes are typically only qualitatively predictable. (CMMI for Services, 28.)

A fundamental part of the IT continuity maturity model is the ability to incorporate process steps to the performance evaluation of people and teams. Based on the known performance one can predict remaining assurance regarding the continuity capability. This information can be used for setting new objectives with delivery time requirements. As demonstrated earlier, the capability of the IT continuity maturity model was linked to the metrics that are used for statistical analysis about the process effectiveness and realized benefits.

On maturity level 5, an organisation continually improves its processes based on a quantitative understanding of the common causes of variation inherent in processes. A critical distinction between maturity levels 4 and 5 is the type of process variation addressed and accepted by the organisation. In practice processes tend to evolve as other processes and renewed requirements affect the model. (CMMI for Services, 28.)

IT continuity maturity model evaluation did not reveal how the continuity management process variation is controlled. However, the study showed that the maturity model itself has had an effect on other IT service processes. While writing this thesis, ITIL 3 implementation had progressed to a stage where all IT service processes are integrated into one manageable entity. That also includes the IT continuity management process. This raises a question and concern whether ITIL 3 implementation will affect the maturity model. Initially the maturity model was designed so that ITIL 3 was noticed among other standards. Due to consistency between the ITIL 3 and the maturity model it is likely that the change will have a minimum impact to the integrity of the maturity model and its capability to enhance continuity management execution. I am confident that the maturity model will remain intact when it en-

counters pressure from process development. I believe that the biggest risks are the individual contributors who will promote the change based on their own preferences even if this conflicts with recognized benefits. It is hard to predict the future, but I feel that as long as the maturity model provides fact-based status information, guides the activities, and has a link to individual level rewarding, the integrity of the model will be secured.

Based on comparison between CMMI maturity levels and the results of maturity model evaluation results, a few conclusions can be drawn. First of all, CMMI level evaluation would not succeed unless the relevant information was available. Positive reflection with the recognized industry standard strengthens my opinion that this thesis managed to focus on the most relevant topics and produce information that can be used for overall maturity evaluation. Second and perhaps a more important observation was the fact that the current IT continuity management status has almost reached CMMI maturity level 5. Maturity evaluation provides accurate and adequate amount of information to conclude that IT continuity management maturity CMMI level is at least 4. Evaluation does not provide enough information to answer the question if IT continuity management maturity model complies with the CMMI maturity level 5. The reason for this might be the fact that there has not yet been any major transformation activity, the result of which could be used for the CMMI level 5 reasoning. However, as mentioned earlier, ITIL 3 change will provide the missing piece of information. After this we will have an answer to the question whether IT continuity maturity model complies with the highest process maturity level.

My conclusion based on the results of this maturity model evaluation indicates strongly that the model has reached a high maturity level. Considering this I do not see any reason to continue the action research and recommend closing the cycle and entering to new area of research.

6.3 Limitations

As far as limitations regarding the research are concerned, it is the author's perception that the only substantial limitation was the Company confidentiality policy of information that could not be shared. Due to this, statistics such as number of incidents, monetary figures, exact numbers and value correlations cannot be shared in this thesis. Basically this means that regardless of the research method, quantifiable data that reveal the actual capability of the target organization is not available. This limits information sharing between the research subject and the academic community. This does not however limit the publishing of the model itself.

Due to scoping of this research there is no indication that the use of the maturity model is limited only for IT continuity management process or the type of organization. My initial opinion is that the model could be relatively easily adjusted to fit other target orientated processes e.g. innovation process. The reason for this is the fact that the core of the model follows the basics of quality processes and common object orientated management principles. However it is imperative that regardless of the processes the performance criteria should be simple and connected to measurable actions so that doers know what they must accomplish. Another question is would this approach increase quality and productivity in other process areas like it does with the IT continuity management. I believe that the key is connection between the maturity model and rewarding systems. If no such systems exist yet, the maturity model may provide the foundation for creating one.

7 Further research

The scope of maturity model is the IT service level continuity management where the standard unit of measurement is resiliency or recovery capability of an information system in scope. Today's information systems are integrated and more dependable on each other. This will increase the need for end-to-end information flow continuity. As a result, single service and system level continuity management may become obsolete. However, this raises another question: will the IT continuity maturity model be flexible enough to be adopted into the revised scope?

I believe that when the system integration has reached this level, the maturity model must take a new scope and measure continuity of the end-to-end information flow. Extended approach may reveal the weakest link in the chain and thus steer senior management's attention about where to focus resources. The fact is that information systems are already heavily integrated. The complexity of IT system interdependencies and shared responsibilities over the organisation boundaries prevent us to from creating the extended maturity model for IT continuity management. In order to adjust maturity model to support end-to-end IT service continuity management, in-depth knowledge about the systems' interdependencies is the next success factor for the maturity model evolution.

Next step after the end-to-end maturity model implementation could be towards the core business processes. Example of a possible scope could be the commonly used Order-To-Cash (OTC) process, which covers activities from customer ordering the product, fulfilment of the order, product delivery, invoicing and payment collection. I believe that the core of the maturity model phases would remain the same as in IT continuity management, but the performance criteria would need to be adjusted to fit with the scope. As an example, for OTC the new unit of the measurement could be the sub-processes of the OTC process. The maturity

model would probably meet similar organisational challenges as IT because each OTC sub-process is managed in a different business unit. Distributed approach may increase “silo-thinking” resulting in creation of business continuity plans with narrow scope. Such a plan would surely serve the continuity objectives of each business unit but nothing more. If the maturity model is not comprehensive, we may fail to ensure continuity of an end-to-end process. My opinion is that in order to avoid risk of end-to-end process continuity failure, maturity model should be managed by a process owner on the core process level i.e. OTC level. This will not remove the responsibility of the business unit to implement business continuity management by using the maturity model, but it will ensure a holistic view over the whole supply chain.

Comparing the continuity management maturity levels of two or more companies will raise the challenge on a new level. The prerequisite for starting this kind of research is that all units of analysis should be at the highest level of maturity; otherwise comparisons are practically impossible to make. Due to differences in size, industry, and company culture the maturity models differ between various companies. This would probably be the major obstacle to overcome in order to get consistent and comparable results. Another challenge is how to get access to confidential information like incident reports that are needed for research purposes, especially if the companies in scope are competitors. And even if access were granted, would confidentiality constrain what could be published? Despite the challenges I believe that this kind of research will confirm whether my theory about the maturity model as a catalyst for improving continuity management is true or not. I am also confident that this type of research may be useful not only for continuity management practitioners but also for the development of other management practices and processes. Perhaps the most interesting case could be based on testing continuity maturity model in a company that operates in a multi-industry sector and has centralized corporate governance. This would be the most optimal situation because the maturity model could be tested in different contexts. A centralized management system may help to sell the research to all industry sectors and, in return, senior management may get comparable results about the corporate business continuity management maturity level.

The final and perhaps the most demanding area of research is to integrate the maturity model into other processes e.g. innovation process, financial management or project management. It would be interesting to find out if the maturity model would work as a catalyst for both cyclic and linear processes. The first step could be to benchmark this maturity model to other similar models and find out whether it is something unique that would provide a new standard for management.

8 References

8.1 Books and publications

Baskerville R., Meyers M. 2004. Special issue on action research in information systems: making is research relevant to practice – foreword. MIS Quartely Volume. 28 Issue.3, 329-335.

British Standard Institute 2006. BS 25999-1 Business Continuity Management: Code of practice.

British Standard Institute 2008. ISO/IEC 21827 Information technology — Security techniques — Systems Security Engineering: Capability Maturity Model.

British Standard Institute 2005. ISO/IEC 20000-1 Information technology — Service management — Part 1: Specification.

British Standard Institute 2007. BS 25999-2 Business Continuity Management: Specification.

British Standard Institute 2008. BS 31100 Risk management: Code of practice.

British Standard Institute 2008. BS 25777 communications technology continuity management: Code of practice.

British Standard Institute 2003. PAS56 Guide to Business Continuity: Publicly Available Specification.

Brue G. 2002. Six Sigma for Managers. New York: McGraw-Hill.

Davison R., Martinsons M., Kock N. 2004. Principles of Canonical Action Research. Information Systems Journal. Volume 14. Issue 1, 65-86.

Graham J., Kaye D. 2006. A Risk Management Approach to Business Continuity. Connecticut: Rothstein Associates.

Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; and Ram, Sudha. 2004. Design Science in Information Systems Research. MIS Quarterly. Volume. 28 Issue.1.

IT Governance Institute 2007. Control Objectives for Information and Related Technology. Rolling Meadows: The IT Governance Institute.

Järvinen P., Järvinen A. 2004. Tutkimustyön Metodeista. Tampere: Opinpajan Kirja.

Suominen A. 2003. Riskien Hallinta. Helsinki: WSOP.

Mahdy G. 2001. Disaster Management in Telecommunication, Broadcasting and Computer Systems. Chichester: John Wileys & Sons.

Pirinen R. 2009. Research Framework of Integrative Action. Americas Conference on Information Systems (AMCIS 2009). August 6-9, San Francisco, California, USA.

Westerman G., Hunter R. 2007. IT Risk, Turning business threats into competitive advantage. Boston Massachusetts. Harvard Business School Press.

8.2 Electronic references

Carnegie Mellon University and Software Engineering Institute. 2009. CMMI for Services, Version 1.2. Printed 11.11.2009. http://www.sei.cmu.edu/library/abstracts/reports

The Central Chamber of Commerce of Finland. 2003. Corporate Governance Recommendation for Listed Companies. Printed 9.10.2009.
http://www.keskuskauppakamari.fi/kkk/julkaisuja/publications/en_GB/corporate_governance/

Finnish Financial Supervisory Authority. 2004. Standard 4.4b Management of operational risk issued 25.5.2004. Referred 7.11.2009.
http://www.finanssivalvonta.fi/en/Regulation/Standards/Financial_sector/4_Capital_adequacy_and_risk_management/Documents/4.4b.std1.pdf

Jackson O. 2008. The Impact of the 9/11 Terrorist Attacks on the US Economy. Referred 7.11.2009. http://www.journalof911studies.com/volume/2008/OliviaJackson911andUS-Economy.pdf

Puolustustaloudellinen suunnittelukunta Helsinki. 2002. New Yorkin WTC–terrori-isku ja toiminnan jatkuvuus, opit suomalaisille yrityksille ja julkishallinnolle. Referred 7.11.2009.
http://www.huoltovarmuus.fi/documents/3/WTC-julkaisu_5_2002.pdf

Moen R., Norman C. 2009. Evolution of the PDCA Cycle. The Asian Network for Quality Congress (ANQ 2009). September 15-19, Tokyo, Japan. Printed
28.11.2009.http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

National Institute of Standards and Technology Administration U.S Department of Commerce. 2002. NIST Special Publication 800-34: Contingency Planning Guide for Information Technology Systems. Referred 7.11.2009. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

National Bureau of Standards. 1981. Federal Information Processing Standards Publication 87 1981; Guidelines for ADP Contingency Planning. Referred 7.11.2009. http://www.niatec.info/pdf

National Fire Protection Association. 2007. NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs. Referred 7.11.2009. http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf

Price Waterhouse Coopers. 2004. Sarbanes-Oxley Act: Section 404 Practical Guidance for Management. Printed 6.7.2009. http://globalbestpractices.pwc.com

New York Stock Exchange. 2004. Rule 446 – Business continuity and contingency plans. Printed 11.11.2009. http://www.nyse.com

8.3 Non- published references

Company IT. 2007. IT Continuity management process: instructions, scorecards, communication kits and standard operation model.

Company. 2007. Business and IT Continuity Management Requirements Comparison.

Company IT. 2007. Major incident reports.

Company IT. 2008. Major incident reports.

Company IT. 2009. Major incident reports.

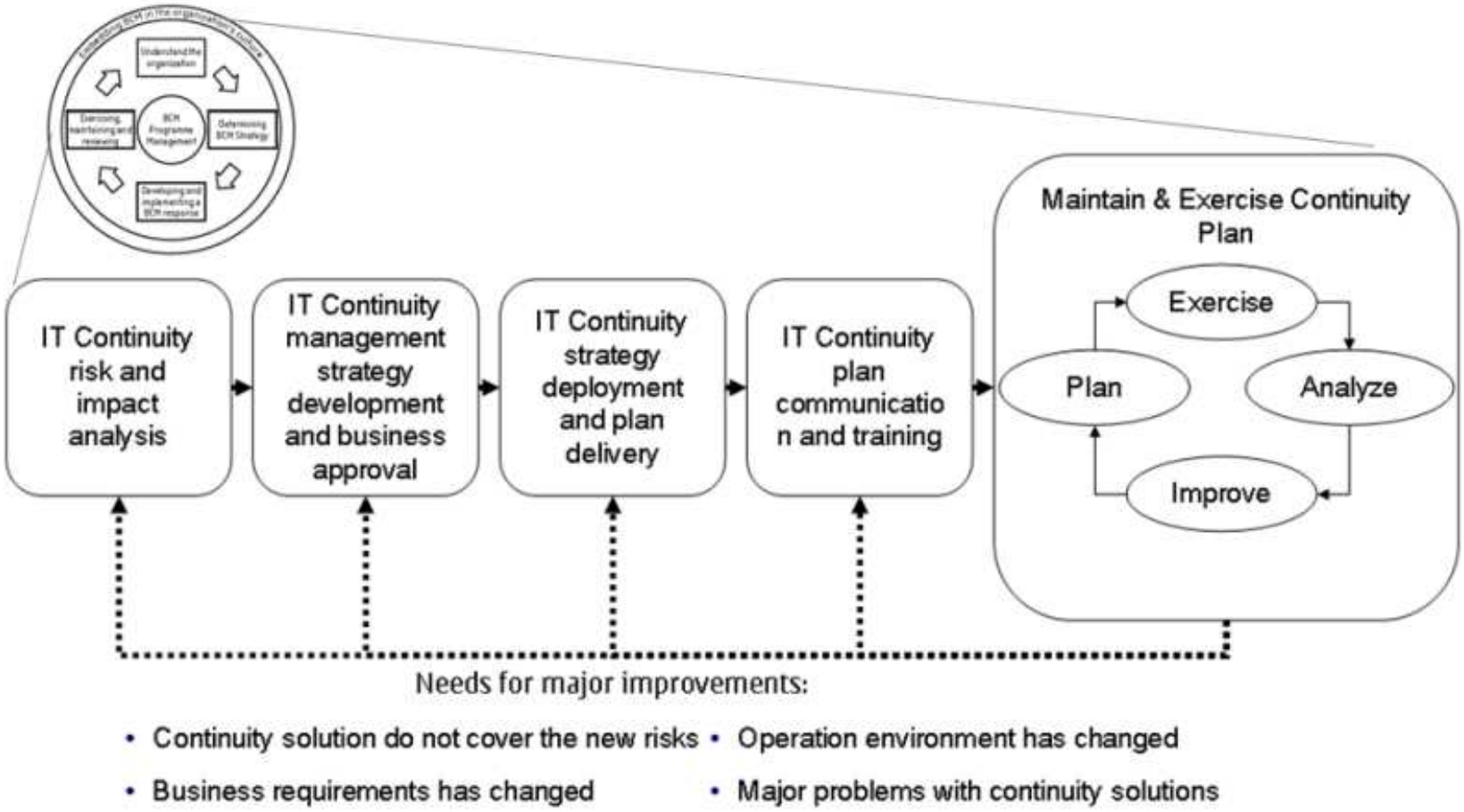
9 Figures

10 Attachments

Attachment: 1 List of industry standards used on this thesis (Syrjänen 2009.)

Standard name	Standardization body	Issued
Management of operational risk	Finnish Financial Supervisory Authority	May 2004
31100 Code of practice for risk management	British Standard Institute	October 2008
BS 25999-1 Business Continuity Management Code of practice	British Standard Institute	November 2006
ISO/IEC 21827 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model	ISO (the International Organisation for Standardization) and IEC (the International Electrotechnical Commission)	February 2009
ISO/IEC 20000-Information technology — Service management — Part 1: Specification	ISO (the International Organisation for Standardization) and IEC (the International Electrotechnical Commission)	December 2005
BS 25999-2 Business Continuity Management Code of practice	British Standard Institute	November 2006
Federal Information Processing Standards Publication 87- Guidelines for ADP Contingency Planning	U.S. Department of Commerce, National Bureau of Standards	March 1981
Information and BS 25777 communications technology continuity management — Code of practice	British Standard Institute	November 2008
PAS 56 Guide to Business Continuity Management	Business Continuity Institute, British Standard Institute	March 2003
CMMI for Services	Carnegie Mellon University and Software Engineering Institute	February 2009

Attachment: 2 Continuity planning process, linked to BCM life cycle model (Syrjänen 2009.)



Attachment: 3 Objectives scorecard comparing initial performance metrics to mature level organisation. RTO= Recovery time objectives, RPO=Recovery point objectives (Syrjänen 2009.)

Reflect current status bellow:	Initial performance criteria			Performance criteria after several observation rounds		
	Min	Target	Max	Min	Target	Max
Phase 0 (new in planning process)	Advance 1 level	Advance 2 levels	Advance 3 levels	Table-top simulation of critical incident invocation and service restoration including a call test of crisis management process, crisis team invocation and communication with business associates		
Phase 1						
Phase 2						
Phase 3			Minimum + demonstrated participation to joint exercise			
Phase 4	Demonstrated table top exercise	Minimum + demonstrated participation to joint exercise	Target + demonstrated technical recovery exercise			
Phase 5				Documented exercise results showing evidence of recovery capability within RTO and RPO	Minimum + follow-up activities to any findings on improvement needs	Exercising of continuity plans including testing of system and data recovery within RTO and RPO, including 1 generation of dependencies OR Verified successful plan invocation and recovery on real incident within RTO

Attachment: 4 IT continuity maturity scorecard example. All numbers and values are pseudo information only for this case (Syrjänen 2009.)