LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Developing Contingency Plan In Governmental Organisation From The Perspective of ISO 22301

Wannous, Ali

2014 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Developing Contingency Plan In Governmental Organisation From The Perspective of ISO 22301

Ali Wannous
Degree Programme in Security Management
Bachelor's Thesis
May, 2014

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security Management

Ali Wannous

Developinging Contingency Plan In Governmental Organisation From The Perspective of ISO 22301

Year 2014 Pages 48

Business continuity management system has become the concern and interest of the organization of different sizes. Organizations started to be aware of the importance of the continuity/contingency plan after several incidents happened around the world, where organizations faced a complete breakdown and were forced to shutdown their business operations for good.

The objective of this study is to implement a concrete contingency plan for governmental body by applying business continuity management standard ISO 22301 and risk management standard ISO 31010 published by the International Standard Organization. The standard's requirements been implemented to help organizations secure their business operation continuity after an unforeseen event has happened, Disaster Recovery Plan. The model used in the standard is clear and easy to follow up with to implement an effective and efficient disaster recovery plan.

The project was done for the Governing Body of Suomenlinna. Different materials were provided to understand the business continuity plan implemented before taking over and thoroughly went through the plan to build mind map to follow during the project. The implementation had to be thought through from the perspective of Business Continuity Management System ISO 22301. The process started from the Business Impact Analysis (BIA), where each process's sub-processes analysed to understand the role they have within the organization and upon the results manage to implement the continuity plan according to the standard's requirements. Received answers from different personnel when we needed to more details regarding certain subjects. The work was done according and upon the supervision of Suomenlinna's security specialist. Practically new documents were built and at the same time upgrading older documents to go fulfil the requirements of ISO 22301 standard.

The objectives given and achieved, the tool provided by the ISO 22301 helps the organization to implement continuity management system according to the standard's requirements. Following the requirements will give the organization a better understanding of the continuity management systems principles. The organization must see what's more suitable to its business to implement the right continuity management system.

After the implementation was ready conducting an audit according to the local authority and standard requirements followed testing it. The audit helped to analyse the business continuity management system's efficiency and whether there has been failures to be fixed for a better result.

Keywords: business continuity, risk management, contingency plan, ISO 22301, audit, Suomenlinna, diasater recovery plan

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Programme

Ali Wannous
Develop**ing Contingency Plan In Governmental Organisation From The Perspective of ISO 22301**

Vuosi 2014 Sivumäärä 48

Jatkuvuussuunnitelusta on tullut intressi kaikenkokoisille organisaatioille. Organisaatiot ovat aloittaneet ymmärtämään jatkuvuussuunnittelun tärkeyden, kun maailmassa on tapahtunut erilaisia kriisejä, joiden jälkeen yritykset ovat hajonneet ja joutuneet lopettamaan toimintansa kokonaan.

Tämän työn tarkoituksena on näyttää miten jatkuvuussuunnitelma rakennetaan virastossa, käyttäen International Organization for Standardization (ISO) standardeja jatkuvuussuunnitelusta ISO 22301. Standardien vaatimukset on toteutettu, jotta voidaan auttaa yritystä turvaamaan heidän liiketoimintonsa ennalta-arvaamattoman kriisin tapahtuessa. Standardissa käytetty malli on selvä ja sen muuttaminen toimivaksi järjestelmiin toipumissuunnitelma.

Projekti tehtiin Suomenlinnan hoitokunnalle. Erilaisia taustatutkimuksia tehtiin, jotta pystyttiin ymmärtämään jatkuvuussuunnittelu ennen kuin tehtiin suunnitelma jota voitiin seurata projektin aikana. Projektin suoritus ajateltiin ISO 22301 ja ISO 31000/31010 puitteissa. Projekti alkoi Liiketoiminta-analyysin tekemisestä. Tutkin jokaisen prosessin ala prosessien ymmärtääkseni niiden roolin viraston toiminnassa, tuloksista pystyin rakentamaan jatkuvuussuunnitelman standardien puitteisiin. Sain lisätietoa viraston henkilöstöltä, kun siihen oli tarvetta. Työn etenemistä ja tuloksia valvoi Suomenlinnan hoitokunnan turvallisuusasiantuntija. Käytännössä työssä tehtiin uusia dokumentteja ja päivitettiin vanhoja, jotta ne täyttivät ISO 22301 standardin vaatimuksia jatkuvuussuunnittelun osalta.

ISO 22301 standardi auttaa organisaatiota täyttämään standardissa annetut vaatimukset jatkuvuussuunnittelun osalta. Suunnitelmassa olevia ohjeita ja vaatimuksia noudattamalla, organisaatio pystyy paremmin ymmärtämään jatkuvuussuunnittelun tärkeimpiä kohtia. Jokaisen yrityksen tulee itse nähdä mitkä asiat jatkuvuussuunnittelussa on tärkeitä heidän organisaatiolle, jotta jatkuvuussuunnitelma pystytään toteuttamaan suunnittelua tehokkaasti.

Kun jatkuvuussuunnitelma saatiin toteutettua sitä testattiin ja auditoitiin, jotta se täyttäisi paikallisten viranomaisten ja standardien vaatimukset. Auditointi auttoi arviomaan jatkuvuussuunnittelun tehokkuutta ja sen virheitä, mikäli niitä korjaamalla pystytään saavuttamaan parempi tulos.

Avainsanat: Jatkuvuus, riskien hallinta, jatkuvuussuunnittelu, ISO 22301, auditointi, Suomenlinna, toipumissuunnitelma

Table of contents

1 Introduction

Business Continuity provides assistance to take into account the key business processes, acknowledge the threats to normal operation, and strategies to ensure the effectiveness and efficiency of the organization's business continuity management system response to the difficulties, which will appear during and after crisis. It is seen as a new alternative approach even though the organization has been following in the past certain recovery procedures that make up for the business continuity.

There have been events around the globe recent that have put the organizations in front of challenges to be prepared to manage unforeseen risk circumstances that threatens organization's future. Implementing disaster recovery response plan that predicts disaster or emergency scenarios such as natural, accidental or intentional events are no longer enough. Therefore, in our current day the risks that are surrounding the organizations require non-stop, interactive process continuation plan that will assure organization's important operational activities before, during and before all after a crisis event. In the society the mentality towards the risks thinking has changed. There are more growing risks, which have been floating up to the surface mainly with the developed technologies, that been causing lots of troubles for the organizations and in particular those with information technology systems. Currently organizations are aware of the different risks and are forced to accept the facts of their reality potential threats.

Securing organization's assets is for their benefits. CEOs and stakeholders are demanded to invest more money into recovery plans to secure the necessary assets. Suitable administrative structure is necessary to put together an effective crisis management, which will guarantee those who are involved in dealing with the crisis management knows who are responsible to make decisions, how the decisions are implemented to assign roles and responsibilities to participants. The selected personnel to take part in the crisis management team must be assigned to perform the specific roles as their normal duties and not as volunteering personnel. As a duty towards the stakeholders, every organization's leadership has a responsibility of planning for its survival. In addition, organizations operate similarly to company; they all have staff or resources doing work for customers. Organization's income doesn't always come directly from the customers, but the profits are been made from the income that are coming from different resource than main customers at times, and for the organization not aware of what it is supposed to be doing, then at some point the income will be reduced and it might stop from coming, which means the organization will have to close down its business and everybody will loose their jobs.

The thesis action research is based on the internship I have recently fulfilled at the Governing Body of Suomenlinna. In 2013 the governing body had to follow the demands of the United

Nation Educational, Scientific and Cultural Organization (UNESCO) to have an effective business continuity plan to protect the island of Suomenlinna as it is part of the protected heritage sites in the world. Therefore, developing and implementing a new plan to replace the decades old version of business continuity plan that covers all the demanded specifications appointed in the international standard Societal security – Business continuity management systems - requirements ISO22301.

Before putting the implementation together, had to go through each process and thoroughly understand its sub-processes' main tasks listed in the Business Impact Analysis (BIA) sheet. The studying of the processes was penetrated together with the security management specialist who was approving the work and suggestions as well as providing all the information needed. Also had a chance to discuss with different personnel from different units to help understanding more about their tasks in the unit. The BIA procedure helps to analyse each process and look at the level of the risk is threaten by, then listing down options of solutions for each process to mitigate the risks to the minimum. Besides following the continuity standard requirements, and just like any other management system, had to include requirements from the Risk Management System ISO31000.

The purpose of the implementation is to improve the readiness of the organization to face any kind of unforeseen event. All threats have been taken into consideration fire, flood, information security threats, internal and external threats, etc. Different options of responding to the different events have been considered, and created a list of personnel that would be involved in managing the crisis. To have the ideas organized properly to avoid confusion, created a schedule to discuss each process separately by collecting all needed information and to stick to the organization's own timetable. Each process took nearly a day to be able to create a mind map of what is needed to be done to implement a functional and effective business continuity management system.

In the later stages of this thesis will have the discussed topics *continuity planning, contingency plan, crisis management and communication, disaster recovery, ISO22301, business continuity capability, case of visiting nursing association (VNA), benefits of business continuity management system, cost effectiveness, competitiveness and the supply chain, corporate governance and directors' liabilities, Plan-Do-Check-Act (PDCA) model,* and *the Governing Body of Suomenlinna – case* with further description and details.

2 Continuity planning

Business Continuity Planning is a tool to assist any organization to be ready to respond to crisis caused by unforeseen event. The event could be natural disaster, terrorist attacks, loss of power, and any kind of interruption that would have a negative impact on the business operation (Doughly, 2001).

Figure 1. Business Continuity

The tool planned taking into consideration the business main interests. Every organization has to have a clear picture on how to react on interruptions, and the management is strongly demanded to be involved. The management is responsible to assure that every involved staff with responsibilities is aware of the task supposed to fulfil when a disruptive event has stroked, in other words roles of the "emergency" team are crystal clear. The tool has to contain plans to save the organization from total business collapse and minimize the loss in profits, assets, data, etc. Therefore, plans such as Disaster Recovery, Business Resumption, and Crisis Management are important to be discussed within the Business Continuity Plan, also known as Business Contingency Plan. The most important element to build an effective and sufficient plan is for organizations to follow the standard provided by the International Standard Organization, ISO 22301. The standard is provided for all organizations concerned about the protection of their business operations and want to assure the continuation/resume of their business after unforeseen events. There are organizations that couldn't resume operations after 9/11 attacks because of weak BCP and in worst cases not having a plan imple-

mented at all. Companies that were badly affected by the Fukushima earthquake, which caused major loss of businesses that probably until now cannot resume business operations (Doughly, 2001).

A survey has been conducted to look for answers whether the private organisations have embraced the federal government implemented Continuity of Operations Planning (COOP). The COOP planning contains elements that seen important in continuity plan that described in the federal documents, and the same survey was conducted in public departments. The results indicated that regardless of the organisation's efforts in adopting a well structured planning, they seem to still be at risk for breakdown in crisis situations. They must be very sure that all services in crisis situations are good to operate (Somers, 2007).

The financial crisis or recession has been discussed by the authors, which led many companies losing billions, stakeholders and customers. The outcome of the result reached was that many companies were not bothered in investing money to have a plan assisting them to come over the crisis without losing the benefits of having stakeholders and customers, which means will not be losing billions. Therefore, the article discussed the importance of the Business Continuity Plan (BCP)/Emergency Management (EM) and the importance of the communications. Also mentioned the standards that organizations should be following. Basically as they didn't have a CP or anything that would save them from losing everything, the businesses fell apart and lost everything (Adkins, Thornton, and Blake, March 2009).

Referring to the article there are three different stages followed in terms of timing and adaptation. There are two stages occurred during the transition Deliberate Planning, which specifies action plan whereas Contingency Planning specifies backup plan. The last plan that occurs is recognized as Reactive adjustment that appears during adaptation plans upon task conditions (DeChurch and Haas, June 2008).

Business Continuity Guideline is an assistance to guide organizations to take different factors and the procedures into consideration to ensure the viability of its operations after a disaster (ASIS International 2014, 6).

The most comprehensive alternative method to protect the organization from losing interest of customers and owners is implementing an effective and sufficient Business Continuity to secure the continuity of the business operations after unforeseen disruptive event. (Drewitt 2012, 5)

Business Continuity Management (BCM) Plan details different kind of plans needed to respond to disruptive event. During the implementation stage of the BCM Plan risk assessment is con-

ducted to assign the needed instructions on how to react during the incidents, therefore, the Incident Management Plan (IMP) is a clear detailed guideline for all teams taking part in the emergency circumstances (Blyth 2009, 1).

Figure 2. Business continuity management

2.1 Contingency plan

Contingency plan is not developed to have a response for different disasters, or preparing different types of scenarios or having a list of different response items based on already expected disruptive events. Basically the main purpose of the plan is developed to backup the business continuity strategies and understanding the conditions that seen as a least serious threats are important to be considered within the framework to be handled (Myers 1999, xvii).

Senior management adopted the idea of Contingency planning for disaster as first priority. They need to figure out who can implement the plan? Who is responsible to ensure that the plan is efficient and works well? The problem that some of the managers do is just having a plan in black and white that is not embraced by the line managers and are not understanding the importance of that embracement, will most likely cause troubles and confusion when it is the time to be penetrating the plan when a disaster happens to stabilize it. There are mistakes that have been done before that has coasted the organization great losses such as worrying about to keep the computer running instead of concentrating and focusing on keeping the business operation running. Another mistakes that has occurred before like having a plan

concentrating only on technological disasters, computers, and totally ignores the most important issue that are the potential physical threats, which can cause bigger problems such as inaccessible buildings or inoperable operations (Myers 1999, 1).

The implementation of contingency plan to protect the organization form the threats that will have a magnificent effects on the business operations in terms of loosing vital buildings, production or distribution operations caused by natural disruptions, sabotage, or environmental conditions. The past years contingency plan's focus was only concentrating on the short-term loss of data processing because was a target by externals. As a result auditors have been putting huge pressure on the management to extend contingency plans to reach out for the temporary loss of accessing buildings from computers. The mind-set, policy and strategy, and the approach were seen as a success in data processing, but as the contingency plan is not suitable for facilities then it is a problem (Myers 1999, 2).

For the long-range *facility contingency planning* is a strategic planning exercise conducted by independent facilitator and not by someone who is from the organization or information system staff. The detailed required specifications and procedures to back up computer data are not penetrated to ensure departments' operation business continuity. The most important thing is to make sure that the information system personnel are not involved in planning facility contingency plan because they are thinking more of the plan as a computer system. Therefore, an outsider contractor or staff planner is the right option to be responsible for developing contingency plans for facilities (Myers 1999, 2-3).

During the plans implementation for protecting computer processing and loss of facilities, and because there are two different things the mindset is very different, as an example, IT equipment has been destroyed and to restore the operation, it is important to be precise, systematic and detailed procedures as required. But looking at the facility (administrative departments) or manufacture operation or distribution activities the procedures are different. To ensure business continuity in administrative departments or production operations there are different options used, all up to the nature of the physical disaster, the level of damage and the condition of the building to regain access entering it. There are specific actions that will need to be left for the department managers to consider it in the implementation when a disaster has occurred. Furthermore, the senior managers will have to understand that developing a multiple combinations types of disaster recovering plan will not work (Myers 1999, 3).

Specialization is required to develop contingency planning. To determine the right one to develop the plan, it is realistic to hand over the assignment to professionals from consulting firm that provides such services. Even when turning the assignment to firms, it doesn't mean

that problems do not exist, the most known problem is that firms shuffle staff between assignments and many times it lands to someone who does not have much experience in facility contingency planning, that will cause the firm another problems like confusion, false starts, time delays, and excessive costs. The firms that provide such services are trained to solve process problems that concentrates on as much details as possible, which is opposite to what some of considered ”professionals” uses in their plans ”what if” strategies that are cost-effective contingency planning (Myers 1999, 3).

2.2 Crisis management and communication

Security and safety threats towards both, public and private organization, will have to be aware of to mitigate the sudden risks. Crisis Management contains the following areas 1) Analysis (Innovative risk assessment) 2) Prevention (Risk regulation and mitigation) 3) Preparedness (Planning and networking) 4) Sense-making (managing radical uncertainty) 5) Steering and synthesizing (scaling and coordinating response operations) 6) Meaning-making (Crisis communication in the (social) media age) 7) Managing adaptation (enacting accountability and protecting learning) 8) Training for enhanced skills. The areas discussed from the EU-based disaster studies’ perspectives for security and safety (Hart and Sundelius, 2013).

The owners are always looking for resilience in their organisations, and to reach the stage of resilience there are crisis management and strategic planning guidelines. In the article, the study is providing results for a better future that is covering not only disaster but any risk that could damage the organisation’s business operations (John and Seville 2011, 5620).

After implementing the crisis management plans, the organization must conduct organizational performance (OP) evaluation during crisis. The purpose is to follow up with the learning process to provide accurate decisions during crisis. The whole process is named a multi-dimensional framework for evaluation OP during crisis (Wang, 2012).

Crisis management is not implemented for what after the disruptive event, but also to be able to prevent a crisis from happening. Vulnerability detection, controlling and controlling the crisis and that’s why a strong leadership is important in every organization that care about its reputation in front of the stakeholders and customers (Kahn, Barton and Fellows 2013, 393).

Crisis communication is essential in a middle of chaos, important part in the crisis management. A quality communication tools are needed to keep all teams informed about the procedures. The plan has to include clear guidelines (Who, What, Where and When) the organization must follow. Building the network is important, and by keeping all alternatives available to be used media, organization’s internal information sources and outside agencies. It is im-

portant that the organization can responds to the crisis before even knowing all of the details. Then forming partnerships is also important to be taken into consideration during the crisis. Keep the media up to date on what's happening and can have one spokesman responsible for that task, listening to the public concerns is important, and being open and honest plays a role of remaining a good reputation in the future (Veil and Husted 2010, 132-134).

Internal communication is essential and important to take place between managers and employees. According to the study and survey conducted within several Italian companies, can realize that communication between the two groups sometimes is not efficient to the point where it should be. Some employees have not taken the guidelines seriously that they didn't understand the importance of their participating during crisis. It is important to use a clear and simple language to pass on the information that managers want the employees to know. Basically the communication between managers and employees should be fully straightforward without missing important links (Mazzei and Ravazzani 2011, 246-248).

There is theory called The Situational Crisis Communication Theory (SCCT), which requires from the managers to implement utilized response strategies that accepting responsibilities concerning crisis is very important. According to the case study developer, Coombs, the managers must evaluate crisis situations then they can develop an appropriate crisis response strategy following the SCCT model factors (Sisco 2012, 2-3).

Crisis management is in need for a communication plan for effective cooperation, detailed rescue activities and to be able to instruct the public during emergency. As public interests is seen priority, public organizations assure the efficiency of managing crisis to provide full service to the public interest and to secure the safety of the citizens. Hereby we understand that the contribution of crisis communication is very helpful starting from the understanding level of risk to the cooperation whilst responding to the activity. Crisis communication is essential for a successful crisis management (Palttala and Vos, 2011).

2.3 Disaster recovery

The Disaster Recovery (DR) actions are not active only after the event have stroked, it is active all the time, but after the event has passed the organization is then in the process of re-establishing its operational strength. There are different impacts caused by disasters, and depending on the type of the disaster, there has to be suitable emergency response. Within the DR plan there has to be different opportunities for organizations to be able to follow during the recovery process (Lindell 2013, 798-810).

The Disaster Recovery Plan has to be tested when the implementation is ready to identify any errors that might occur during the process to be fixed. The whole purpose of the plan is to

protect the organization's operation and the computer services. The key-element is that the organization is ready to react with very minimum loss, be stable and to be able to recover the lost data (Wold, 2006).

Business data is irreplaceable, there are steps to be considered to develop successful data recovery plan after unforeseen event. The required steps 1) Planning 2) Identify critical data 3) Create appropriate policies and procedures 4) Determine type of backups 5) Develop recovery processes 6) Plan testing and maintenance (Wallace and Webber, 2011, 319-320).

The Disaster Recovery Plan is part of the contingency plan, understanding the different phases of a disaster will help the team decide about the plan needed to implement. The facility contingency plan must include three deliverables time periods 1) Risk management program 2) Emergency response plan 3) Business continuity strategies. The time periods are part of the disaster life cycle that contains four time periods 1) Prevention/Preparedness training 2) Organized response/Damage containment 3) Protect cash flow/Use alternate procedures 4) Restore facilities/Resume normal operations (Myers 1999, 7-8).

During the Data Recovery Plan implementation and analysing through all possible threats that might strike the organization, and the geographical location has to also be considered. The understanding of the geographical location is that different states face different type of disasters (hurricane, tornedo, fire, flood, etc) that may also cause loss of data. Therefore, proper plan where all risks assessed will help to avoid losses (Dolewski 2008, 11).

The occurred disasters are more than just server crashing, router going down, virus or a worm damaging the organization data, they are as well terrorist attacks, natural disasters, collapse of a facility, fire, etc. The important issue is that organizations must be prepared for all possible unforeseen events, and having backups to all of their data is essential to be able to bounce back after an event has taken place. Backups could be something like having replacement drive, or to be able to divert loads of works to another machine. Therefore, for organization to be able to resume business operation as fast as possible, Disaster Recovery Plan must be implemented to have an effective reaction to the incident (W. Freeman, 2002).

The Disaster Recovery Plan has several stages the organization needs to follow, and to climb the ladder to be back into operations with minimum amount of time. The stages recommended to follow up with are:

- Understanding an organization's activities and how all resources are interconnected
- Assessing an organization's activities in all areas, including operating procedures, physical space and equipment, data integrity and contingency planning

- Understanding how all levels of the organization would be affected in the event disaster
- Developing a short-term recovery plan
- Developing a long-term recovery plan, including how to return to normal business operations and prioritizing the order of functions that are resumed

It is very important that the DRP is tested after implementation in case there are unseen gaps that might be crucial. And if changes within the business plan do happen, the DRP has to be updated upon the changes to keep it up to date (W. Freeman, 2002).

The disaster recovery plan will be foremost covering the technical issues (failed hard drives, processors, motherboards, data loss, data damage, viruses, external or internal attacks, etc), however, natural disaster is way much more to plan for and that's why Business Resumption Plan is thoroughly implemented to give a better instructions about how, where, when and who responsible for the task assigned to the personnel involved. Later on in the chapter will have better explanation regarding BRP. A successful DRP has to include the following procedures (W. Freeman, 2002):

- Critical data must be backed up and fully documented. The server where the backup has been made must be defined, type of backup device.
- Backups must be distributed to different secured offsite storages (recommended to have more than one backup). The set saved in secured offsite storage must be rotated at minimum once a week. Also it is important to maintain a full month end backup. In addition, it is recommended to have an emergency repair disk in secured offsite storage.
- Software media including serial numbers, account information, contact information, and any other data should be securely stored offsite.
- For the safety of the backup on the servers is important to connect uninterruptible Power Supplies to the servers.
- LAN/WAN documentation should be maintained offsite.
- Staffs', suppliers' and clients' documents containing their full information must be stored in secured offsite.

Site services

Implementing the disaster recovery plan, the team will have to put all possible ideas in one box to have different options available to help the organization get back on its feet after an event. Looking into the different services provided by companies offering disaster recovery services. The organization must plan for analysis and classification of data. The firm has to think about the valuable files containing important information that backing up the data is on the top of their agenda. Before spending part of their budge protecting the data, the team

should make sure that the cost is proportional to the value of the data (Wallace and Webber, 2011).

In case the organization loses not only the data but also the hardware on which the data is stored, that means the organization must think of backup location to be able to set up replacement hardware. One of the options is to have a contract with companies offering services such as Hot Site, Warm Site, Cold Site, Mobile Site and Mirrored site as an off-site facility as a replacement. These sites help organizations to resume operations for certain amount of time. The difference between the services:

1. Hot Site is providing computer and network operations when a computer or equipment disaster takes place, which gives a chance for businesses to continue operating. Hot site is fully equipped for the organization to continue operation, including office space and furniture, telephone jacks and computer equipment.
2. Warm Site has a ready to go systems and communications, but data will have to be restored on them before can resume operations and use them.
3. Cold Site is a similar service to hot site that provides office space, but it is customer's responsibility to provides and installs all the equipment needed to be able to continue operations. Although cold site costs less but preparing the place to become a space to resume the business operations, it will take little longer for the organization to start operating again.
4. Mobile Site is transportable office containing fitted IT and communications equipment. Transported by a truck and can set it up at any desired suitable location. it is recommended for the site to be configured before usage to be considered a viable recovery solution. Service-level agreement is necessary in case the organization is buying services to make sure the vendor is committed to meet its needs in an emergency.
5. Mirrored Site is as site that looks exactly the same as production site and where data has been stored in real time. This most expensive option seen as the fastest alternative to resume business operations (Wallace and Webber, 2011).

Recovery time objective

After a disaster organizations wish to resume operation as soon as possible, therefore, recovery time objective is important element within the disaster recovery plan. The recovery time objective is target time set to resume operation of products such as computers, systems, network or applications after an event has occurred. The recovery time objective is measured in seconds, minutes, hours or days (Rouse, 2011).

The RTO is a sensitive element while implementing Business Continuity Plan in the organization, because whilst planning the RTO the team will have to do calculations on the time needed to recover and then they will be able to determine the necessary needed prepara-

tions. Let's say if the organization needs a 2 hours of recovery time objective, and because the organization wants to achieve the recovery in 2 hours then it will have to invest good amount of money in a disaster recovery centre, telecommunications, and necessary technology systems. If the organization's recovery time objective is 2 weeks the money invested will be much less, because after the occurred incident the organization will have time to search and find resources (Rouse, 2011).

Recovery point objective

When the organization faces a technological failure (hardware, programme, etc) which will lead to a breakdown in computers, systems and network, then recovery point objective is used to be able to recover files from backup storage to resume a normal operations. It also helps to specify the failure occurred in seconds, minutes, hours or days by scanning the system going backward to reach the point when the failure occurred (Rouse, 2011).

After the RPO has been conducted on the computer, system or network given and defined the failure, then the team will have to determine most suitable backup needed to be made. Together with the recovery time objective assists the team to pick a technology and procedure specified in the disaster recovery. If the demanded RPO is an hour then the backup must be conducted once an hour (conducting backup every hour will most likely be very expensive), and here when the team needs to look at the best disaster recovery solution that will be external and redundant hard drives. For higher amount of RPO hours, let's say 100 hours then backup must be conducted in breaks of 100 hours or less, and the most suitable solution will be compact disk. The last solution is most probably cheaper in a time the organization is trying to resume business operations and get at least part of the lost revenue caused by the disaster (Rouse, 2011).

2.4 ISO 22301

The international standard, management systems standard, has been developed to be the guideline for implementing Business Continuity Management System for all different sizes and types of organizations colleges, businesses, government departments or any business operation. The officials, who are responsible to track companies business operations, authorize the standard certification. These organizations are implementing their BCMS under the conditions and concerns of the legislators and regulators, which will give the customers a positive impression about the organizations holding a good practice in BCMS. The ISO 22301 will provide a positive performance by the business continuity manager to prove the execution of highest management level by achieving the recognized standard. The standard has actually became as a backup help for governments and regulators who started recognizing that business continuity will help to minimize the disruptive incidents on society, therefore, governments and regulators started to assure from organizations that they have implemented appropriate busi-

ness continuity. Because businesses are depending on one another it is important to assure that suppliers are able to continue providing products and services when incidents have occurred (Tangen and Austin, 2012).

The standard is mainly used for certification but it includes requirements where it describes the central elements of business continuity management. There is another standard developed which has extended guidance to give a broader detail on every requirement found in ISO 22301, the standard known as ISO 22313. The organization can use the ISO 22301 to conduct interior audits to measure itself against good practice. The results that auditors have raised in their reports will then be reported to the management. The requirements provided by the standard have a great positive influence on organizations than those whom choose to be certified against the standard (Tangen and Austin, 2012).

Organizations need a well-defined response structure for unforeseen incidents, and ISO 22301 provides that structure for the sake of organizations' future. It emphasizes that when the incident has taken place, the responses are escalated in time and manpower are ready to take necessary actions upon incidents. After an incident has occurred, the organization is responsible to communicate with possibly affected external parties, for instance if the organization produces a life risk product (eg. fireworks) and an explosive happened, then it is important that the organization communicate with the pubic areas surrounding the facility where the incident occurred (Tangen and Austin, 2012).

The interesting thing is to know how well are the governments following the ISO22301, although they are proud providers of own standards, they demands from local organizations to follow their regulations. The United Kingdom is always demanding from job seekers and business owners to concentrate on following the regulations implemented in the British Standard (Tangen and Austin, 2012).

2.5 Business Continuity Capability

Business continuity is an expression that every company aim to include in its regulatory capabilities. The policy document is considered as part of the strategic plan mechanism. The lifecycle of business continuity management system is ready to be used after the basic documents are produced, approved and communicated (Hotchkiss 2010, 7).

The figure below (Figure 1) expresses business continuity capability basic requirements. The lifecycle does not stop after the last stage, the Audit. Major steps are constantly reviewed for further development on practical business continuity capability (Hotchkiss 2010, 7).

Figure 3. Lifecycle of business continuity capability

Business Impact Analysis

The organization's key products and services are considered to construct continuity plan to support the business operations, therefore, business impact analysis gives the opportunity to identify the sensitive processes to reduce the potential risks towards the products and services to the most minimum acceptable level (Hotchkiss 2010, 7; St-Germain, Alu, Lachapelle and Dewez 2012).

Threat Analysis

The business leaders will give their opinions about the reviewed threats during the BIA interviews, and depending on the views provided by the team. To continue with the lifecycle, the risks that don't have high impact will be analysed in the following stages risk assessment and scenario development (Hotchkiss 2010, 7).

Risk Assessment

After identifying the risks is important to conduct a further analysis of the possible disruption they represent (Hotchkiss 2010, 7). In addition, ISO 22301 suggests the implementation of the process as a referral to the ISO 31000. The purpose of the proposal is to establish, implement, and maintain a systematically documented assessment process concerning the disruptive events the organization might have to deal with (St-Germain, Alu, Lachapelle and Dewez 2012). The figure below gives better explanation on attributes of risks (Wallace and Webber 2011, 37).

Figure 4. Attributes of risk

Risk management principles are the same in all organizations, although they measure their risks in different ways, at the end the supply or availability of resources and money will help the organization to meet the requirements of the corporate governance. The important thing that matters is health, other people and money. Money will help us buy and gain everything else apart from health and other people. There are organizations in the public and voluntary sectors that money is the thing that makes the best, bigger or brand leader, or to provide service within their community, and anything else that they wish to do (Drewitt 2005, 2).

Organizations should be aware of the priorities they set regarding their major partners, customers, and major contracts as business continuity scenario. In case the major customer decides that now will stop buying the products or services supplied by the organization. How much would it matter when buying services stop and if so, why? If the customer stops buying because the supplier lost the facility, is it then the main reason or is it because they have found another supplier? The risks are categorized into three different types (Drewitt 2005, 3):

1. Organisation ceases to be viable due to adverse levels of business, profitability, cost fluctuations and compliance with relevant legislation, contracts and codes
2. Organization's sustainability is in danger as it might engage in an activity that customers haven't requested
3. The organization is sustained but its ability to operate has been effected by unexpected situation, incident or materialised threat.

Out of the mentioned risks, organizations base their *business continuity plan* upon the third category, because it is recognized as operational risk (Drewitt 2005, 3).

Design risk scenarios

The management proposes reaction strategy on certain risks identified by the first group, which is the BIA (Hotchkiss 2010, 7).

Design business continuity management procedures

After designing the risk scenario, it is important to develop functional, testable, and documented procedures on occurred scenarios. The stages penetrated to ensure activities continuity and unforeseen event management (Hotchkiss 2010, 8). Successful procedures shall include the following protocols (St-Germain, Alu, Lachapelle and Dewez 2012):

- Appropriate internal and external communications establishment
- To be aware of the immediate steps necessary to take during disruption
- Flexibility is important to be able to respond to unexpected threats and to make needed internal and external adjustments
- Pay full attention on the events that would have potential disruptive impact on operations
- Developing stated assumptions and an analysis of interdependencies
- Effectively implementing appropriate mitigation strategies to minimize consequences.

Exercising and testing

To ensure the efficiency of the business continuity management system procedures, and that they are meeting the objectives of the business continuity, the organization has to test them regularly. Testing the procedures is to guarantee selected strategies will provide recovery and response within the time limit the management set as a goal (Hotchkiss 2010, 8; St-Germain, Alu, Lachapelle and Dewez 2012).

The organization that is keen on ensuring the safety of its future is required by the ISO 22301 (2012) to conduct exercises and tests that:

- Business continuity management system's objectives and scope are meeting
- Based on well planned reality scenario with clear aims and objectives
- Different relevant parties involvement taking part in the exercise is preferable
- Minimize the risk of operations disruption
- Documenting results of the exercise containing outcomes, recommendations, and actions to improve the implementation
- Revision of the reports to promote continual improvement

- Conducting the exercise whenever there is a significant change within the organization or the environment in which it operates (ISO22301 2012, 19).

Update capabilities

The procedures results may not be as expected but will have to be recorded, and it is favourable to reanalyse the procedures to be tested again (Hotchkiss 2010, 8). ISO 22301 requires a regular monitoring after the Business Continuity Management System (BCMS) has been implemented as well as periodic reviews to improve operation. The following penetrations are important to be conducted to ensure efficiency:

- Monitoring procedure keeps on running until the organization's continuity policy, objectives and targets are met
- Measuring the processes, procedures and functions performance that protect its prioritized activities
- Monitoring the standard and the business continuity objectives to ensure compliment
- Monitoring old failures in the BCMS's performance by conducting internal audits
- The management review the evaluation of all the monitors and measurements conducted throughout the penetration stage (St-Germain, Alu, Lachapelle and Dewez 2012)

Audit

Regularly conducting audits on the capabilities that will lead to corrective action and a new Business Impact Analysis (Hotchkiss 2010, 8). According to the ISO 22301 every organization must conduct internal audits to test whether the business continuity management system is responding to own requirements, international standard requirements and that is effectively implemented and maintained. In addition, the organization is required to (ISO22301 2012, 20-21):

- Plan, establish, implement and maintain audit programmes including the frequency, methods, responsibilities, planning requirements and reporting. It is important to consider within the programmes the results of previous audits and the processes concerned
- Define the audit criteria and scope of each audit
- To ensure the objective and impartial of the audit process auditors must be selected to conduct the audits
- The results of the audits must be reported to the relevant management
- To keep possession of the documented information as a proof of the audit programme implementation and audit results.

Any schedule included in the audit programme must be based on the risk assessments results of the organization's activities, and based on the results of the previous audits. Audit proce-

dures must cover the scope, frequency, methodologies and competencies, also the responsibilities and requirements for conducting audits and reporting results (ISO22301 2012, 21).

After the audit has been conducted, the management is responsible for the audited area that important corrections are corrected without any delay to eliminate nonconformities and their causes. The verified actions taken and verified reporting results must be included in the follow-up activities (ISO22301 2012, 21).

The module in the centre of figure 1 represents the governance of the continuity capability. The module is always used in every stage of the lifecycle that does have a continuance affect on people during the lifecycle. Well-structured governance will provide an assistance to ensure that all involved individuals will achieve a goal to support the business continuity (Hotchkiss, 2010).

2.6 Example of disruptive event

The fire event that happened in Visiting Nursing Association (VNA) and the aftermath has proved the importance of a solid Continuity Plan. The reaction of the management and the reaction of the responsible continuity plan team have helped the organization to resume operation in a very short time until headquarter has been reconstructed (Blake and McGrady, Decmber 2011).

The fire event at the visiting nursing association has been a lesson that taught several other organizations about the importance of Business Continuity and Disaster Recovery Plan (BCDRP). In the case Blake and McGrady (2011) have pointed out the important procedures taken to help manage the crisis professionally. The first lesson learned is that disruptive events do happen at anytime and when you don't expect them. But the VNA did not sit back and relaxed because they did believe that disruptive even would strike at any time and they were prepared by putting together a plan. The first step they took is creating business continuity and disaster recovery plan, and key elements in the plan were implemented. Creating a successful plan would not have been possible if the senior management did not give their full support and planning a budget to construct the plan. As the association concentrated on creating the plan and seen as a priority, other organizations where not thinking about following the VNA steps and were seen as unprepared and off guard. One of the advantages in the plan is assisting the organization to anticipate emergencies, reducing shock, and proving that will help minimizing the impact when having an immediate response planned. After the implementation was ready, the key players in advance understood own roles, and the planned phone call trees initiated the communication with stakeholders (Blake and McGrady, Decmber 2011).

The second lesson learnt is the effectiveness of the communication. The excellent leadership skills performance by the top management was at the necessary level because of disaster scenarios was thought through before the fire event happened. After the scenario drill, the senior management started cooperating with the business continuity and disaster recovery (BCDR) team and began implementing the plans disaster response and recovery. The other individuals were included in the plan are the department managers, CEO, public relations, executive staff, and other key individual (Blake and McGrady, Decmber 2011).

As planned in the implementation, the public relations department took the necessary actions and began to collect number of communications for employees, patients, clients, the Board of Directors, donors, vendors, the media and the community regarding the fire. According to the plan they had a central message that has been repeatedly stated "All services will continue uninterrupted." The department of public relations and the CEO regularly held progress update meetings, press conferences, and communication with donors. Upon the effectiveness and constant communications, donations and assistance from other non-profit organizations, vendors, and community started immediately donating to the organization and providing necessary helps. The efficiency of the communication put out an important message to the competitors that thought would take advantage of the event happened to the organization, which is the Visiting Nursing Association is still operational and serving clients (Blake and McGrady, Decmber 2011).

The third lesson that was learnt is having a network that would be able to help during disasters, called Social Capital. The VNA CEO and management understood the importance of finding a new location for their Disaster Recovery (DR) command, and a long term location where they could have placed their employees until the headquarters site has been reconstructed for the staff to move back. Building the social capital network has enabled a fast collaboration with private, public, and other nonprofit organizations in the same area location. The Social Capital network helps the organization to be able to find assistance to continue serving their clients (Blake and McGrady, Decmber 2011).

Social capital is defined as "resources embedded in a social structure which are accessed and/or mobilized in purposive actions." Organizations and their leaders foster social capital to recruit and develop board members, raise philanthropic support, develop strategic partnerships, and for many other purposes.
Upon the solid social capital network, the CEO of the VNA utilized the network and he was able to find a temporary location within 24h where operation could be resumed. Also, the organization was receiving loans from different organization such as 100 spare desktop computers and some printers. These offered elements were in another organization's storage as part of own disaster recovery plan. There were board members, donors and other agencies as

important stakeholders that supported the VNA during their recovery by contributing time, cash, equipment, and facilities (Blake and McGrady, Decmber 2011).

Visiting Nurses Association fulfil the requirements demanded by the US Government. The Health Insurance Portability and Accountability Act (HIPAA) Regulatory Compliance demands the associations in the health field to have an off-site data centre to assist the agency to operate uninterrupted during and after disaster. The VNA adopted the electronic medical records (EMRs) and following the HIPAA Security Rule demands its network essence had been relocated that 45 servers were moved out of the association's headquarters to fully redundant secure data centre. The security rule mandates assist the organization to cover all entities during implementation administrative, physical, and technical measures to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI). In Addition, Health information that includes health plans, health care clearinghouses, and health care providers, which transmitted electronically are as well covered entities (Blake and McGrady, Decmber 2011).

Visiting Nurses Association's quick recovery from the fatal disaster would not have been possible without an effective off-site data centre implementation for both Electronic Medical Record and business software. The possibility of accessing the internet from the temporary location, the association managed to access the off-site data centre to process patrol for employees and contractors, access electronic medical records, make payments to vendors, and complete statutory reporting. This stage was lesson four (Blake and McGrady, Decmber 2011).

The fact is that during the disaster there will be loads of different obstacles and telecommunication is a major one. During the VNA disaster event damaged Telephone Equipment and Voice Network was a challenge, lesson five. In the burnt headquarters building the telecommunication switch is installed and severely suffered from smoke damage, and because the switch was out of order the telecommunication between headquarters, branch offices, and off-site data centre was not possible. The challenge put the emergency management team to quickly implement a plan to resolve the problem during the disaster recovery phase. The members of the emergency management team immediately begun communications using cellular phones belong to them. Additionally, cellular phone provider loaned the organization 40 cellular phones and were activated for key individual and departments. At same time the main phone numbers the organization uses were forwarded to an answering service from the central office of the phone company. Through the activated answering service the incoming calls were transferred to the appropriate department based on calling tree. The telecommunication switch was sent off for maintenance and it was out of order for 3 weeks after the fire (Blake and McGrady, Decmber 2011).

In the start of writing this paper I have mentioned about backing up all paper version information into digitalized documents. As a lesson 6, a mistake was made by the agency's secretary, who was maintaining paper Rolodex that contained information of contacts for vendors, board members, donors, employees, suppliers and other key contacts that was destroyed by the fire, and none of the information was saved digitally in the database or anywhere else. In addition to the loss of the contact information that were on the secretary's desk, there were another set of limited number of documents on staffs' desk and they weren't digitalized and were destroyed in the fire. After the problem was occurred, the employees together with the emergency management team started to recreate contact information and any other lost work that was on staffs' desks and was not in the database. Although recreating the contact list was a great effort by employees and emergency management team there was still key contacts information were missing from the newly constructed list. After recreating the list all information were fed into the database and daily were backed up to an off-site location, they still had to think through to try and figure out the information that still missing form the electronic form (Blake and McGrady, Decmber 2011).

Every organization has to think about the necessary insurance policies that are important to follow at start-up for any emergency that might face in the future. Regardless of the full collaboration with the insurance company, it will not always recovery all assets lost back for the organization that means that insurance policies have fallen short.
For every organization protecting the staff is first priority, followed by protecting financial data, copies of signed contracts, databases, custom software, human resource files, insurance files, and proof of ownership and loss. While the reconstruction was taking place and nearly ready, the organization's insurance coverage was reaching the maximum value of the building based on the assessed tax value and created issues regarding the insurance coverage. The example, the insurance did not recover full replacement costs for desks and filing cabinets. The other problem the agency faced is that the upgraded computers and other equipment were not covered because they were not added on the policy. But because collaboration between organization and insurance is important, the agency sent off a letter notifying them of the upgraded equipment that were purchased. The insurance did accept the letter and did issue a full recovery costs (Blake and McGrady, Decmber 2011).

Sometimes there are costs that comes the insurance's way and are the ones that were never considered. In this case the significant costs, unconsidered, were cleaning the damaged equipment, documents, and other needed services as a result of the fire. In the existing insurance policy there wasn't any agreement that the insurance will cover employees' personal items left in the facility during evacuation. Organization signing a deal as a coinsurance policy may have covered the employees' personal lost items. As the facility was constructed the in-

surance doesn't cover the additional costa, therefore, donors and a credit from financial institution covered VNA's shortfalls costs (Blake and McGrady, Decmber 2011).

In this lesson 7, the organization realised that probably hiring an expert with insurance knowledge is worth the cost to be able to advice the assets to the insurance coverage. Another possible alternative is to select a member with good knowledge to assist reviewing with the insurance rating and the policy schedule of contents for necessary changes. (Blake and McGrady, Decmber 2011)

During a crisis all employees' feelings are right at the edge and for some employees the crisis brings the best in them, therefore, remaining resilient is important. Human Capital Resiliency (HCR) is Business Continuity and Disaster Recovery Plan (BCDRP) important part. HCR gives the organization the ability to react and respond to its workforce posed threats. The VNA CEO and management felt relief when all employees were safely out of the building. After the evacuation the BCDR team started to prepare for communication with the employees to address them on updates regarding the fire, options regarding Monday's work timetable, and arrangements for the upcoming days. Immediately communicating with the employees is an important step of an existing BCDRP. Employees that have been working remotely in the home health area would continue normally working because they didn't regularly go to the headquarters location. Home health group needed supplies from headquarters; they were advised to call their supervisor as the reordered supplies and arrived at the temporary location on daily basis. For employees that have been able to telecommute from home were asked to stay at home. They were kept up to date on all notifications regarding the payroll and other systems at the interim location immediately after the loaned computers are installed. In addition, the company kept the website up to date and asked employees to keep checking the website on a daily basis for updates (Blake and McGrady, Decmber 2011).

After the list of the lessons learned from the event, it has proved that having an effective business continuity management system does save the organisation from a total catastrophe. The system has assisted the organisation to resume operations in a very short time from the day of the disruptive event. As it has mentioned that the continuity plan does not save the organisation from unforeseen events but does assist the organisation to avoid a full collapse that will be forced to get out of business that will effect many staff, suppliers, consumers, etc.

3 Benefits of business continuity management system

Every organization needs to look for best alternative options in how to protect their business operations from falling apart and leading to a complete collapse (Drewitt 2005, 17). To structure solid business continuity the organization must implement *business continuity manage-*

ment system. For an effective *business continuity management system,* it is recommended that organizations fulfil the requirements given by the International Standard Organization and the local authorities. The International Standard has pointed out specific requirements to implement structural and solid *Business Continuity Management System* (BCMS) (ISO 22301 2012, V).

It is in the organization's benefits to have implemented a structural business continuity management system that is suitable with its business operation. The BCMS will assure the importance of the following elements (ISO 22301 2012, V):

- understanding the organization's needs and the needs and the necessity for establishing business continuity management policy and objectives
- implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents
- monitoring and reviewing the performance and effectiveness of the BCMS
- continual improvement based on objective measurement.

The business continuity management system has key components, just like any other management system, are important to follow. The key components are *policy, people with defined responsibilities, management processes*[1]*, documentation providing auditable evidence, and any business continuity management processes relevant to the organization* (ISO 22301 2012, V).

Business continuity management system is not developed for no reason. The purpose of the system is to assist organizations for developing and implementing an efficient BCM programme. The keys things that organizations need to look into *cost effectiveness, competitiveness and the supply chain, and corporate governance and directors' liabilities* (Drewitt 2012, 19).

3.1 Cost effectiveness

According to the Pareto Principle plenty of organizations achieve only 20% of their efficient business continuity arrangements for 80% of the effort expended. The organizations that invest in the remained 20% of the effort in an excellent business continuity approach are those who will achieve 80% of the benefits (Drewitt 2012, 20).

Business continuity management (BCM) gives the greatest opportunities to put organization think of the things that could possibly go wrong and alternatives of preventing and mitigating

[1] Management processes relating to policy, planning, implementation and operation, performance assessment, management review and improvement.

them. By following the opportunities will help the management to avoid saying "*we didn't think of that"*. Once the implementation is done well, the result will have a positive impact on the regular maintenance of plans, contingencies and other arrangements that are up to date and suitable to fit the purpose of the implementation. As organizations keep investing in resilience arrangements in one way or another, it will make much sense that the investment been done to become part of the BCM. The BCM programme becomes effective when both resilience and preparedness arrangements are combined together as a cohesive whole. The benefit from the cohesive whole is that the inappropriate existing risk control measures and resilience arrangements will be reviewed and adjusted to become appropriate and cost effective (Drewitt 2012, 20).

3.2 Competitiveness and the supply chain

In someone's minds there is a thought that without *business continuity plan* or *business continuity management system* a business can be lost. According to the author there are situations that a supplier lost to another because the other had BC plan or BCMS. However, it is regularly growing the number of organizations are interested to learn more about their suppliers' resilience to things that might go wrong. Organizations do that as part of their supplier assurance because they want to know how their suppliers will be able to ensure continuity of supply or service when unforeseen event happens. Recently, although it is progressing slowly, more and more larger organizations are asking to learn about the suppliers' business continuity resilience arrangements. Presenting a good set of arrangements will give a positive understanding concerning the competitive ability the supplier has (Drewitt 2012, 20).

Suppliers that fail and disappoint their customers during a disruptive incident are hardly getting away with "*it wasn't our fault"* and the business that took a year to win might be lost for perhaps five years or even longer than that. Suppliers that let their customers down to a certain degree but are able to present, and before all communicate, that BC arrangements are in place, which will lead for a greater support and loyalty from the customer that will also help the supplier to win the customer again when it comes to renewing contracts in the future. For the organizations that are willing to be securing part of their business through the tendering process will find out that qualification criteria will start including business continuity or resilience arrangements, and it is not far from happening that organizations will start demanding from suppliers certification under the ISO22301 or BS25999 as criterion (Drewitt 2012, 21).

Organizations that haven't yet developed an effective business continuity management system would not be able to secure certification fast enough to meet the criterion, the plan is strategic for organizations involved in this type of supply mechanism (Drewitt 2012, 22).

3.3 Corporate governance and directors' liabilities

Corporate governance has been in organizations lives for many years and it has been argued that in old times of responsibilities and by doing things the right way have saved the directors or the organizations from being involved in major fraud or other wrongdoing. According to the author Drewitt (2012), in the United Kingdom the directors' responsibilities were practiced upon expectations that all their act is in the best interest of the company, and proving that their work been done for the sake of their company lawyers and judges were the ones to give an opinion (Drewitt 2012, 22-23).

In the United Kingdom there is an Act called Companies Act 2006, which demands from directors to be cooperating with higher level of expertise. In the Act there is not a clear mentioning about business continuity but it is recognized as a criminal offence the directors will be facing if they do not practice a reasonable care, skill and diligence towards the company as a whole and not as a department or division (Drewitt 2012, 23-24).

By the time business continuity and its management are benefiting from specific skill, knowledge and experience, the risks to be mitigated and expected to be there are not specialised and in most organizations the director is expected to be aware of the hidden risks. This explains to us that just assuming someone else is taking care of the incident that has occurred or thinking that nothing will ever happen, as things never went wrong before, is characterised as neglect. Basically neglecting and failure to act in appropriate way will be with by common law, the directors might face personal liability and their protection by their company will not be in place. If something does go wrong the board will be called for a meeting to question if the procedures to mitigate the risks were planned. The directors that can demonstrate that they have had plans and arrangements to face a risk that has occurred will be in a significant place against any claim. (Drewitt 2012, 24-25).

3.4 Plan-Do-Check-Act (PDCA) model

The International Standard created the "Plan-Do-Check-Act" (PDCA) model to be applied to planning, establishing, implementing, operating, operating, monitoring, reviewing, maintaining and continually assuring the effectiveness of organization's business continuity management system (ISO22301 2012, V).

The model also ensures on a certain degree of firmness with other management systems standards to support, integrate and to operate with related management systems. The standards are like *ISO 9001 quality management systems, ISO 14001 Environmental management systems, ISO/IEC 27001 Information security management systems, ISO/IEC 20000-1 information technology – Service management, and ISO 28000 Specification for security management systems for the supply chain* (ISO22301 2012, V).

Plan (Establish)	Establish business continuity policy, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organizatiuon's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and Improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Table 1. Explanation of PDCA model

The figure below give a better explanation how does the business continuity management system takes the act of interested parties, via needed actions and processes that produces continuity outcomes to meet the requirements (ISO22301 2012, V).

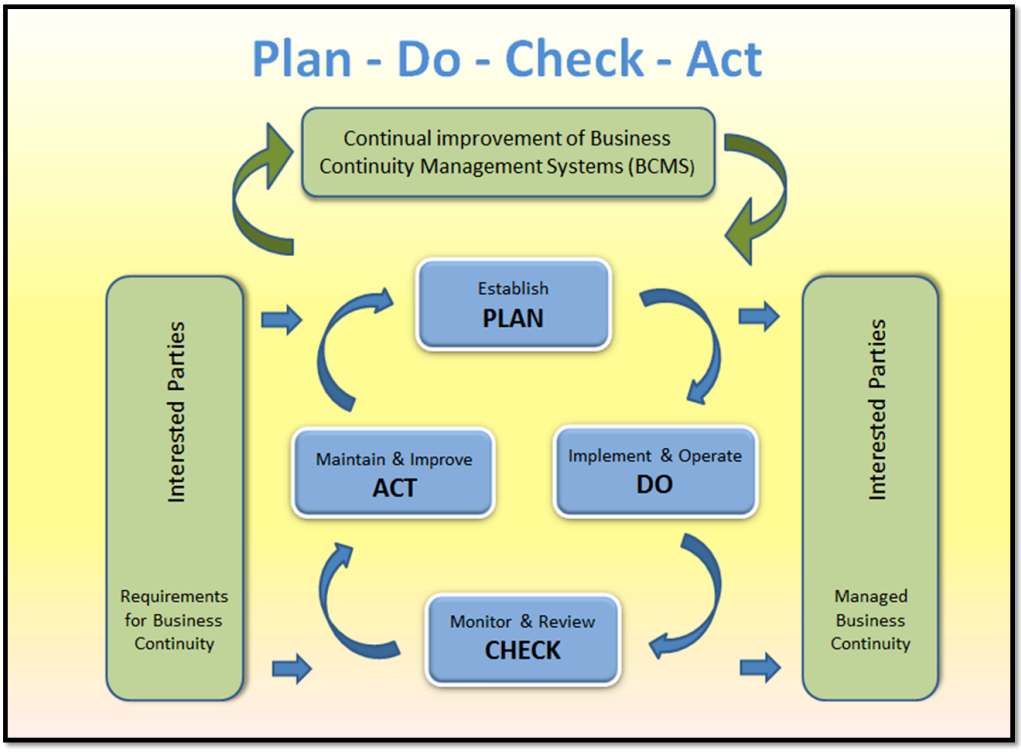

Figure 5. PDCA model applied to BMCS processes

4 Action reasearch

Action research is an educational or occupational studies conducted for a better methods to assist involved participants for better results approach and to improve actions (Richard Sagor 2000).

The group of members taking part in the action research find it a great experience opportunity as well as it has positive impacts in many relevant different ways. All participants are determined and focused on the research they are conducting and that will guarantee them a relevant result, and at the same time they will be the ones gaining the result to use them in their future projects. The tool has given me the opportunity to develop my knowledge about business continuity management system to be able to establish the system in relevant context and easy to understand (Richard Sagor 2000).

For a relevant results and self development there is a cycle that is important to be followed that will assist the participants to create constructive action research. There are seven steps to focus on for a constructive action research (Richard Sagor 2000):

1. Selecting a focus
2. Clarifying theories
3. Identifying research questions
4. Collecting data
5. Analyzing data
6. Reporting results
7. Taking informed action

Step 1: Selecting a focus

To start the action research process is important to have a core subject that need to do the research about. For every research has a certain focus point which means there has to be a question (Richard Sagor 2000):

What are we aiming at to investigate for a relevant results?

Step 2: Clarifying theories

Action research is based on the values, beliefs and perspectives of the theoretical methods the participants are using related to the topic (Richard Sagor 2000).

Step 3: Identifying research questions

Every group that is starting to do a research about certain topic they will have to come up with meaningful questions to assist the researches to achieve the goal (Richard Sagor 2000).

Step 4: Collecting data

The research needs to be based on best data for a perfect action research. For that to be accomplished the contributors to support their actions by having reliable sources and valid information, there should not be a single resource as backup. A constructive action research the contributors will have to use several independent sources to collect the needed data for their final result, it is known as *triangulation*. The term is defined as looking at the same subject but from many different angles (Richard Sagor 2000).

Step 5: Analysing data

After gathering the data needed, the researchers can identify the patterns and trends data used in the answers found to construct their paper. There is a couple of generic questions important to be asked to ensure the liability and the value of the resources:

What is the story told by these data?

Why did the story play itself out this way?

After the questions have been answered, the contributors will have a better understanding on how to improve the knowledge they already have on certain subject (Richard Sagor 2000).

Step 6: Reporting results

As in every procedure different type of work, reporting is an element that assists contributors to receive second pinion. The problem is when a single researcher is working on a subject alone then having a second opinion might pull the progress of the research slightly back. The reporting will help to improve the research for the best as a result of a second opinion and a revision (Richard Sagor 2000).

Step 7: Taking informed actions

The contributors participating in the action researched to develop implementation plan are involved in the planning process action. It a stage that will help the researches from not falling in the same mistakes they did in their earlier experience. This final step will raise the researchers to a different level of knowledge gaining valid and reliable data in developing themselves (Richard Sagor 2000).

4.1 The Governing Body of Suomenlinna

The thesis is based on the internship I have recently fulfilled at the Governing Body of Suomenlinna, which was in need for an updated *business continuity plan*. It is important that the new management system is simple and effective. To construct an effective implementation found it ideal to base the plan upon the ISO22301-standard that guided through the process to build the system. The *Governing Body of Suomenlinna* operates under the mentor of the Ministry of Education and Culture. The island Suomenlinna is an important part of the city of Helsinki economically and historically and a tourist attraction site. Suomenlinna is a herit-

age-protected site and the task of the governing body is responsible for maintaining the historical buildings, maintenance and presentation. The employees working in the governing body is about 65, and during the high season, like summer, the amount of employees can reach 95. Additionally to the governing body of Suomenlinna, there are on the island the Border Guard, Armed Forces Naval Academy and the prison (Suomenlinna Management Plan 2014, 5-7).

The form of the Governing Body is based on four processes *maintenance process, restoration process, the world heritage services process and administration and legal services process*. The maintenance process is responsible for maintaining the internal facilities and the external surroundings, as well as the neatness of the environment. The restoration process is responsible for the annual constructions, supplementary constructions and cultural environment development. The world heritage services process is responsible for presenting Suomenlinna and tourist information. Additionally, handle the meeting and ceremony facilities marketing and the site's quality control. The administration and legal services process supports functions such as human resources, communication and legal services. Also security operational unit belongs to the administration services, which security specialist is responsible for developing security related issues (Suomenlinna Management Plan 2014, 5-7).

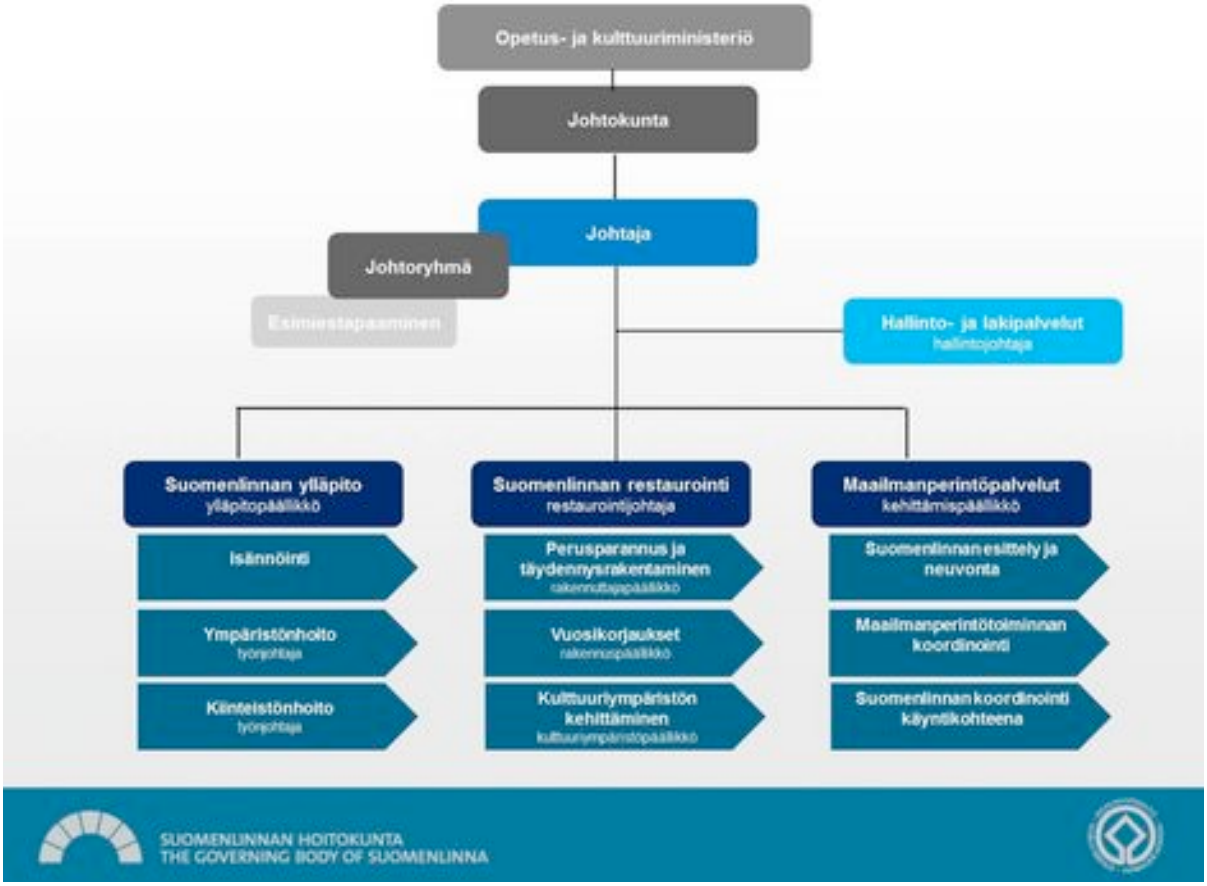

Figure 6 The Governing Body of Suomenlinna

The governing body employees tasks differs from one to another, and the job description depends on the unit he/she belongs to. The security service process main focus is to keep on following up on the health and safety regulations in different work tasks. As an example, the construction individuals must have the helmets and safety shoes along with other safety equipment depending on what they are doing. The task differs from the individuals working in the administration unit who are more focusing on the workplace well-being, as an example (Suomenlinna Management Plan 2014, 5-7).

The focus was concentrated right from the beginning on implementing an easy management system without any complications or unnecessary documentation. The important thing was to have the system functionally easy that when is needed to update or maintain can be done without any extra effort. Implementing the continuity plan was upon the suitability and interest of the organisation.

4.2 Management Plan project

In 2010 the process of implementing the Management Plan started after the first workshop meeting of the representatives of the World Heritage Sites of Finland, and the main purpose of the meeting was to create a new management plans. The goal to achieve from the set of meetings, at the end of 2011 they have met seven times, to support the idea of creating the management plans process, and to guarantee the making of the comparable structure and quality of the Finnish plans (Suomenlinna Management Plan 2014, 5-7).

Since the decision was made, the Governing Body of Suomelinna produced the plan to move forward and started to put all the details together. The organization has used materials as background including the analysis conducted regarding the present situation with a support of the UNESCO providing the Enhancing our Heritage Toolkit and materials provided by the Suomenlinna Tomorrow Project. The implementation planned by the contributors of the organisations and residents of the fortress through the representatives on the Board of the Governing Body, the Suomenlinna Tomorrow Project and Management Plan Workshops (Suomenlinna Management Plan 2014, 5-7).

The plan contributors have structured together a consisted few layers to assist the long-term goals to be in practice. The highest level of the consisted layers is a vision of crystallising the informal interchange of thoughts about the World Heritage Site. There are seven different strategic developments that have been defined including furthermore detailed objectives and actions. During the duration of the plan there are implemented actions defined in the separate Action Plan included in the Management Plan. All the actions under the strategic development areas have been gathered and grouped, and a schedule has been assigned for the implementation and indicators to be fulfilled. Furthermore, the Enhancing Our Heritage Toolkit

is used for the UNESCO Periodic Reporting, and at the same time the plan is updated. The toolkit is consistent alternative to improve the work of the governing bodies (Suomenlinna Management Plan 2014, 5-7).

The Governing Body of Suomenlinna have decided to reconstruct all the their different ISO standards as part of the new management plan strategy to maintain the value of the heritage site of Suomenlinna. The whole idea behind the new plan is to protect universal values to ensure the significance of the site whilst providing an outline policy for stakeholders (Suomenlinna Management Plan 2014, 5-7).

The project started by meeting the security manager at the organisation to understand the needs they are looking for to be implemented. The standard was assigned to me was ISO 22301, Societal Security – Business Continuity Management Systems – Requirements. The stage started by reading through the information provided regarding the processes that need to be included in the continuity plan using the *Business Impact Analysis* procedure. The four processes are *maintenance process, restoration process, the world heritage services process and administration and legal services process*. To establish the *business continuity management system* the following key requirements has to be considered (ISO 22301 2012, 5):

a) Policy
b) Defined responsibilities – staff
c) Management processes
    - Policy
    - Planning
    - Implementation and operation
    - Performance assessment
    - Management review
    - Improvement
d) Documented auditable evidence
e) Process of BCMS important to be relevant to the organization

Each process has detailed tasks sub-processes that were listed down on the *business impact analysis* (BIA) sheet where I had list of questions to be able to follow the lifecycle of business continuity capability (Figure 3). The processes that were analysed using the business impact analysis method are *administration and legal services process maintenance process, restoration process, and the world heritage services process*. The standard ISO 22301 was all the time followed and the *risk management standard* ISO 31000 whilst assessing the risks every process can possibly face.

The business impact analysis sheet assisted us to be able to create a mind map of the already existed of business continuity management system elements and to identify the needed updates and add missing components. During the risk assessment process came across different components that were not considered in the old version of the continuity plan. All risks were taken into consideration from external to epidemic threats.

The project's timetable has fulfilled the ISO 22301-standard requirements. As mentioned earlier in the paper (Figure 5) follows the standard's PDCA-model, which is Plan-Do-Check-Act. The first stage is the *plan*, which understands the business continuity policy, targets, controls, processes and procedures that are necessary to improve business continuity in order to deliver results that are suitable with the organisation's overall policies and objectives. The main focus was to follow the specified requirements provided in the standards. After receiving the needed details about the organisation's business operation, the documentation structured from the provided details was the template to identify the deficiencies. Once the *plan* stage was ready moved on to the next step *do*. The Do-stage is where I had to conduct risk analysis and risk management that assisted me to move forward to the following Check-stage. The *check* procedure is monitoring and reviewing performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement. The identified deficiencies were fixed and the *business continuity management system* reached the required level of operation. After the final stage, as required in the ISO 22301-standard, conducted internal audit for the BCMS then it was ready to provide it to the management for a preview and to give feedback. Throughout the process the security manager has actively been involved and giving immediate comments when needed.

Year	2013		2013 - 2014			
Month	11	12	1	2	3	4
Project's review						
Naming the project						
Identifying the necessary BCMS requirements						
Business Impact Analysis (BIA)						
Risk analysis						
Risk management						
Plan-Do-Check-Act						
Audit						
Management review						

Figure 7 BCMS project schedule

The *risk analysis* and *risk management* process were precede along with the colleague who is implementing the *risk management system*. Together we have identified tenths of risks and learned about the disruptions that will cause the organisation in case any of them take place.

The following examples explain the some of the threats that we have analysed during the Business Impact Analysis (BIA) process. As mentioned earlier we have analysed tenths of different threats and here are few to have better understanding.

Project risks

When there many projects undergoing at the same time, it is possible that one or two of the projects be delayed due to lack of organising. The important thing in this situation that projects should not be scheduled all at the same time and that project managers are responsible for scheduling the projects to avoid delays. Additionally, not having enough equipment plays its role that will to a weak work quality, which means the staff's training and instructions are important to be clear. The organisation might face a negative reputation when the staffs are not provided with the needed training, for example team leader responsibilities.

The individuals assigned at the manager position should have the needed training and knowledge about the responsibilities has to fulfil them professionally. The manager is also responsible for any equipment installed in the department are not damaged, which means regular documentation of equipment's' maintenance, conducted tests and check-ups.

Facility risks

Not everybody should be granted access to the facility. The outsiders' access to the facility must be very limited, and staff's access within the facility is monitored as well depending on their position in the organisation. If granting access to everybody then the risk of loosing important and sensitive business operation details is high and the competitors will be able to have full usage of the stolen documents. The other possible threat if one of the staff been bribed to release sensitive information to outsiders that can damage the organisation's business operations.

When the information security system is not well protected by certain security procedures that means there is a dark hole that will put organisation's documents under high risks. To avoid disturbing situations the staff will have to be given clear instructions regarding own responsibilities and the access granted within the facility. The procedures to minimize the risks of giving the staff a chance to get hold of sensitive documents that do not belong to their work responsibilities.

Access control is the most important element to help protect the organisation from loosing important documentation and property damaging. In addition installing security systems such as security cameras, motion identifier, sirens, etc.

From my own work perspective, the focus point was to implement BCMS that is simple and easy to use, which fulfil the demands and requirements of the standard. The documentation has been written without any extra unnecessary information to keep the organisation's security issues crystal clear. The ISO 22301-standard specified requirements assist the organisation to add own requirements suitably fit with the BCMS that does follow the requirements of the standard. As it was one of the main goals to achieve, the continuity plan was successfully implemented satisfying the organisation's wishes.

Creating the plan needs enough time to be reserved and it is important to keep up with the schedule. Managing to keep up with the schedule to achieve the goal aiming to reach was a success regardless of the difficulties has faced throughout the process. As it was planned right from the start of the project, the implementation was ready by the time was scheduled and it will be fed in the organisation's own system by the beginning of June 2014 after the final version is reviewed by the security manager of Suomenlinna.

Throughout the process the Governing Body of Suomenlinna's staff have been actively involved by providing the necessary information needed to be considered in the continuity plan. Basically the implementation was not focusing on security unit but on the whole organization, and it was very important to have professionals from different units involved. As in every project unforeseen delays might take place, therefore, reserving enough time was an important element.

The other important element was to be accurate with the planning and to have a clear background review on the topics will be included in the plan, and understanding the standard was very important to be able to create the business continuity management system. As there was researches done in the past, they were useful to consider them and move forward with the plan partly based on them, which in certain way assisted the to begin with the implementation. The work that was done at the start of the process is the main core o move forward in the project that will help avoid any complications if the work was not done right.

As required in the ISO 23301-standard, management's commitment to the project is very important to motivate the staff to get involved and provide the assistance when needed. Opinions regarding the project were considered to be included in the planning. In different stages the staff were actively involved during the documentation, which was a great contribution

effort by them. The easier the implementation is, the easier the staff will receive the information during orientation.

5 Conclusion

Business Continuity Planning is to help assist organizations to face disaster events. The disaster causes disruptions in organizations business operations such as a continuous in providing services. Disruption in business operations means that the organizations will be facing loss of revenues and at worst scenarios the organization will no longer exist because it can't get back on track. Implementing business continuity plan helps the organizations be on the safe side by backing up their valuable information elsewhere than in their own business operation facility, have temporary facilities equipped with all necessary technology to be able to continue with their business with minimum loss possible.

The emergency plan that is implemented has important elements to consider for a better performance. In the business continuity management there is a lifecycle capability, which has several stages to follow to be prepared for unforeseen events. The stages are the key elements for the organizations to see if their implementation is actually working as supposed to. Therefore, after implementing the plan there has to be audits conducted to analyse the execution of the plan. If it fails the team is demanded to start from the beginning to analyse the errors document it and use it again to test the improvements made. They are as well responsible to keep the plan regularly maintained and up to date with every change happens to avoid any harmful error that may cause the organizations a lot of time wasting, customers and financial loss. Following the local standards requirements as well as the ISO 22301 will lead the organizations to the right path and to be able resume business operations whilst dealing with the incident is still on going. The teams involved and are responsible for different plans must keep a clear communication and the cooperation level at the maximum level as possible for a better outcome. Business Impact Analysis procedure is the most important stage whilst implementing the continuity plan.

Communication plays an important role in several ways the importance in keeping the customers and stakeholders updated, contact with media should only be through the communication team, which means staffs or students should not be saying a word to the media that might interpreted their sayings into worse scenario than the reality of the incident. Looking at College perspective, an individual has taken one of the college staff as a hostage and the person is known, no one should mention the name of the individual unless it is coming from the communication team.

Even though the implementation might go through many lots of difficulties because managers always try to save loads of money and when things come to security, they might say that will

never happen and why to waste our money on plans like this. But they will be very grateful at the end when they realize that the team has saved the organizations from greater revenues, customers and stakeholders' loss.
The project at the Governing Body of Suomenlinna was based on the requirements specified in ISO 22301-standard to create an effective and sufficient business continuity management system. As Suomenlinna is protected heritage site there demands from the UNESCO to keep the island safe from high risks that may destroy historical areas.

The procedures followed to implement the plan for Suomenlinna were based on an earlier done research along with the involvement of the staff and managers, which assisted to cover all the important areas that belongs to the governing body. Business Impact Analysis assisted to identify the risks may appear and disrupt the organisation from being able to continue operations. During the stage studied each risks and planned a solution on how to face the problem if it strikes. After assessing the risk conducting an audit is important element to ensure the safety and the success of the recovery plan.

For effective business continuity management system the requirements specified in the ISO 22301 standard must be followed so the organization can meet its objectives and policies it has set to achieve. It is preferable to include other standards and to be more specific Risk Management 31000 standard is the main mentor to be able to analyse and manage the risks.

References

S. J. Blanke and E. McGrady 2011, From Hot Ashes to a Cool Recovery: Reducing Risk by Acting on Business Continuity and Disaster Recovery Lessons Learned

S. Somers 2007, Survey and Assessment of Planning for Operational Continuity in Public Works

Gabriel L. Adkins, Tyler J. Thornton and Kevin Blake 2009, A Content Analysis Investigating Relationships Between Communication and Business Continuity Planning

L. A. DeChurch and C. D. Haas 2008, Examining Team Planning Through an Episodic Lens: Effects of Deliberate, Contingency, and Reactive Planning on Team Effectiveness

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International 2005

Everything you want to know about Business Continuity, Drewitt 2012

Business Continuity Management: Building An Effective Incident Management Plan, Blyth 2009, p. 1

Michael Lindell 2013, Disaster studies

Geoffrey H. Wold 2006, Disaster Recovery Journals, Disaster Recovery Planning Process

M. Wallace and L. Webber 2011, The Disaster Recovery Handbook: Step-by-Step plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, Second Edition

K. N. Myers 1999, Manager's Guide to Contingency Planning for Disasters, Second Edition

R. Dolewski 2008, Disaster Recovery Planning

Cooperation and Conflict - Crisis Management Revisited: A new agenda for research, training and capacity building within Europe, Paul 't Hart and Bengt Sundelius, 2013

J. Vargo and E. Seville 2011, International Journal of Production Research – Crisis strategic planning for SME: finding the silver lining

W. T. Wand, 2012, Evaluating organisational performance during crisis: A multi-dimensional framework

Academy of Management Review, Organizational Crises and the Disturbance of Relational Systems, William A. Kahn, Michelle A. Barton and Steve Fellows, 2013

S. R. Veil and R. A. Husted 2010, Best practices as an assessment for crisis communication

A. Mazzei and S. Ravazzani 2011, Manager-employee communication during a crisis: the missing link

H. F. Sisco 2012, Nonprofit in Crisis: An Examination of the Applicability of Situational Crisis Communication Theory

P. Palttala and M. Vos 2011, Testing a methodology to improve organizational learning about crisis communication by public organizations

S. Hotchkiss 2010, Business Continuity Management – A Practical Guide

K. Doughty 2001, Business Continuity Planning – Protecting Your Organization

International Standard 2012, ISO 22301: Societal Security – Business Continuity Management Systems - Requirements

Internet References

www.iso.org S. Tangen and D. Austin 2012: Business continuity - ISO 22301 when things go seriously wrong. Last Accessed 21 January 2014

www.pecb.org/iso22301 R. St-Germain, F. Alu, E. Lachapelle and P. Dewez 2012: Whitepaper – Societal Security Business Continuity Management Systems. Last Accessed 21 January 2014

www.sans.org W. Freeman 2002: Business Resumption Planning: A Progressive Approach. Last Accessed 27 January 2014

www.whatis.techtarget.com M. Rouse 2011: Recovery Point Objective. Last Accessed 22 January 2014

www.backupworks.com/business-continuity-overland-storage.aspx Last Accessed 5 May 2014

http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453495.html Last Accessed 12 May 2014

http://www.touchstonerenard.com/our-solution-portfolio/management-standards-roadmap/business%C2%A0continuity-iso-22301/ Last Accessed 12 May 2014

http://www.ascd.org/publications/books/100047/chapters/What-Is-Action-Research¢.aspx Last Accessed 16 May 2014

Figures

Tables

Appendixes

Appendixes 1. The Governing Body of Suomenlinna – Project Table of Contents

9 Continuity plan update and audit

10 Reporting