LAUREA

Major incident procedure

case: OMX Group

• • • • • • • • • • • • • • • • • • • •

Kupiainen, Petra

2010 Kerava

Laurea Polytechnic
Laurea Kerava

Major Incident procedure
CASE: OMX GROUP/OMX Technology

Petra Kupiainen
Information Technology
Thesis
June, 2010

Laurea Polytechnic
Laurea Kerava
Information Technology
Digital Media

Abstract

Petra Kupiainen

Major Incident Procedure **case: omx group**

Year 2010 Pages 20

OMX is a leading expert in the exchange industry. With more than 60 customers in over 50 countries, OMX provides marketplace solutions for exchanges, clearing organizations and central securities depositories. The head-office is in Stockholm, Sweden.

OMX has its departments located from Helsinki to New York. Most of its services and equipment like servers are concentrated in Stockholm, which makes the communication more challenging between its departments, especially during a major disturbance. There was a larger project in the company and one of the assignments was to create a procedure for a major disturbance using the ITIL principals. ITIL consists of five principal elements, which together creates the Service Management package. These elements include: the business perspective, managing applications, delivery and support of IT services and managing the infrastructure. The focus in this project has been on service support and delivery elements.

Procedure was named a major incident procedure and it consisted of three disturbances, mail problems, virus attacks and network problems. These disturbances were the ones that affected all of the customers and had the most impact on the critical areas of the business. All of the disturbances have defined criteria's, which makes it a major thing: how to act during the disturbance and after it, responsibilities and contact information.

When the procedure was finished and approved it was sent to its personnel by mail, it was stored in the intranet and training for its personnel was arranged. Also the information to the customers was sent out.

The purpose of the major incident procedure was to integrate its department operations, improve communication and teamwork between them. Also communication and information to the customers needed improving.

Key words: ITIL, major incident, procedure

LAUREA AMMATTIKORKEAKOULU TIIVISTELMÄ
Laurea Kerava
Tietojenkäsittelyn koulutusohjelma
Digitaalinen media

Petra Kupiainen

Vakavien häiriötilanteiden prosessikuvaus **tapaus: omx group**

Vuosi 2010 Sivumäärä 20

OMX on pörssitoiminnan johtavia yrityksiä maailmassa. Yrityksen pääkonttori sijaitsee Tukholmassa ja toimistoja löytyy Helsingistä New Yorkiin. OMX kehittää ja tarjoaa teknologiaa ja palveluita yrityksille, jotka toimivat arvopaperikaupan alalla. Asiakkaita heillä on yli 60 useissa eri maissa. Pohjoismaissa ja Baltiassa toimivat pörssit kuuluvat OMX konserniin.

OMX on keskittänyt suuren osan it-palveluista Tukholmaan, mikä asettaa haasteita muissa maissa toimiville it-osastoille, erityisesti häiriötilanteissa, joissa on tärkeää saada tieto perille nopeasti. Yrityksessä oli käynnissä laajamittainen projekti, jonka yhtenä osa-alueena oli kehittää ja tuottaa toimintasuunnitelma vakavia it-häiriötilanteita varten käyttämällä ITIL periaatetta. ITIL koostuu viidestä elementistä, jotka yhdessä muodostavat kokonaisuuden palveluiden hallinnasta tietokannan ylläpitoon. Tässä projektissa käytettiin näistä elementeistä kahta, palveluiden saatavuutta ja tukipalveluita.

Projekti aloitettiin kartoittamalla vakavat häiriötilanteet, joita kertyi kolme, sähköpostiongelmat, virukset ja verkko-ongelmat. Kriteereinä valinnoille olivat ongelman laaja-alaisuus, seuraukset ja vaikutukset kriittisiin liiketoiminta alueisiin. Toimintasuunnitelma nimettiin ”Major Incident Procedure”-prosessikuvaukseksi. Kuvauksessa tarkasteltiin jokainen häiriötilanne erikseen. Jokaiselle häiriölle määriteltiin kriteerit, jolla se luokiteltaisiin vakavaksi, miten tulisi toimia häiriön aikana ja sen jälkeen, vastuu-alueet, tiedotuspohjat ja yhteystiedot.

Prosessikuvauksen kirjoittamisen ja hyväksynnän jälkeen tieto piti saada it-henkilöstölle, joten järjestettiin koulutukset pohjoismaissa, laitettiin toimintasuunnitelma käyttäjille sähköpostilla ja tallennettiin suunnitelma intranet-sivuille, sekä tiedotettiin asiasta myös asiakkaille.

Projektin tarkoituksena oli ensisijaisesti yhtenäistää it-osastojen toimintatapoja, kehittää heidän välistä kommunikointia ja yhteistyötä, sekä lisätä tiedottamista ja kommunikointia asiakkaiden kanssa.

Asiasanat: Vakavat ongelmatilanteet, toimintasuunnitelma prosessi, prosessikuvauksen tekeminen, ITIL

TABLE OF CONTENTS

1 INTRODUCTION

OMX is a leading expert in the exchange industry. With more than 60 customers in over 50 countries, OMX provides marketplace solutions for exchanges, clearing organizations and central securities depositories. The head-office is in Sweden, Stockholm. (OMX Corporation)

I have worked in OMX in the Office IT department for 8 years. I did my practical training in a project that merge Helsinki helpdesk with helpdesk in Stockholm. Nowadays this helpdesk has grown bigger and they have many new customers, activities and responsibilities, so it was renamed to Office IT Service Desk. From this point forward Office IT Service Desk is referred as OIT Service Desk. Since the responsibilities and workflow has grown, there was a need to update and improve service desk working tools and instructions. IT department and also the whole company were going to be re-organized to use ITIL principals. ITIL is a framework that consists of five principal elements, which together creates the Service Management package.

My assignment was to create Major Incident procedure and SMS instructions to the Office IT department using the ITIL principals. Major incident procedure is a mandatory guideline for situations that can cause lots of damage to the company, like virus attack for example.
SMS is a text message to cell-phone and OIT service desk will send those SMS messages to predefined persons during the major incident. SMS instructions are a simple manual describing tool on how to use the SMS program.

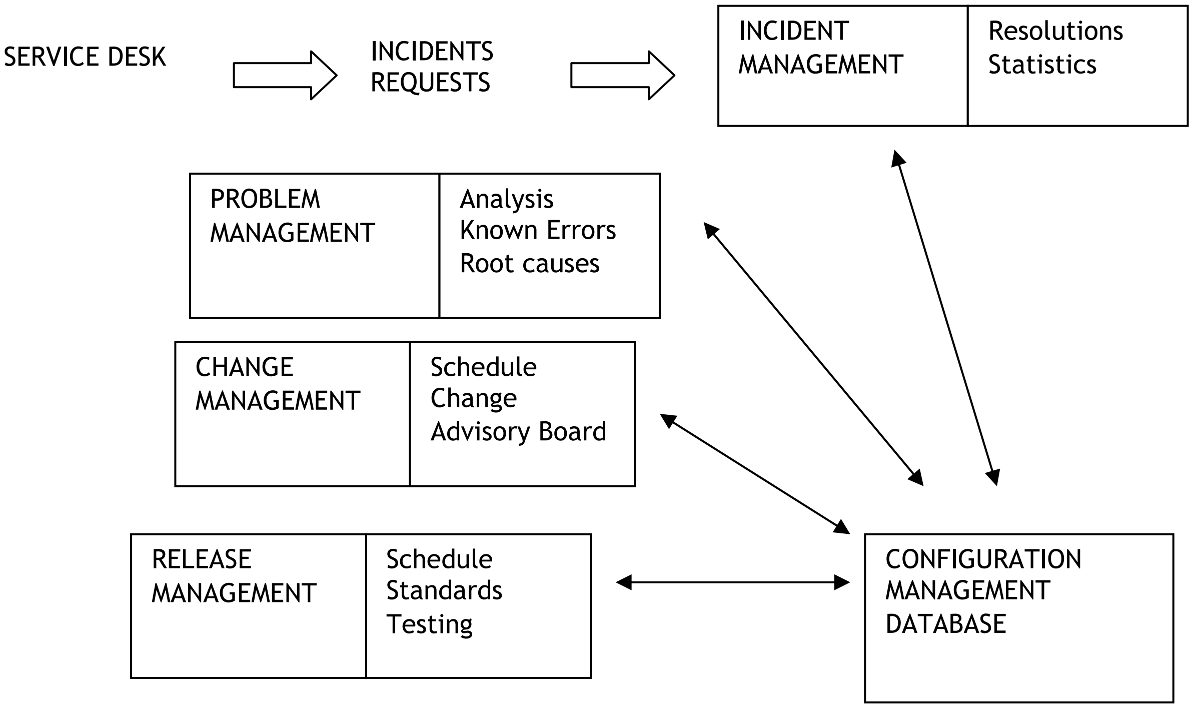
This project was very educational since I had to get to know ITIL principals and how to use them in my own work. Also it was a great opportunity to participate in a project which purpose was to give the customers an even better service.

2 CENTRAL CONCEPTS

2.1 IT Infrastructure Library

“Developed in the late 1980’s, the IT Infrastructure Library (ITIL) has become the world-wide *de facto* standard in Service Management. Starting as a guide for UK government, the framework has proved to be useful to organisations in all sectors through its adoption by many companies as the basis for Service Management. Today, ITIL is known and used worldwide.”(OGC 2001,1.)

ITIL consists of five principal elements, which together creates the Service Management package. These elements are: the business perspective, managing applications, delivery and support of IT services and managing the infrastructure. (0GC 2001, 4) As the project was carried out in the IT department, the focus was to use ITIL Service support and delivery elements. These elements are meant for different target groups.
Service delivery includes contracts, agreements and planning for the future and its customers are the budget-holders, which make all the important dissension. Service support includes the daily work, solving problems and supporting users in their day-to-day business.



Picture 1 ITIL SERVICE SUPPORT (Aim Academy course material)

Picture is a draft from the ITIL course material. In the picture is shown, that there is one database and all of the changes are made there. All of the management boxes have their own individual task. Incident Management takes care of the daily issues, Problem Management is concentrating on larger problems, Change Management does the systems and software changes and Release Management carries out the changes, when new software launches.

2.2 Major Incident Procedure

Major incident procedure is a mandatory guideline to situations that might cause a seriously damage to the company, financially or time-loss. There are four types of major Incidents that are covered in the procedure: mail problems, virus attacks, domain problems and network problems.

Major incident procedure is needed because:

Service desk staff is overloaded when there is a serious problem
Communication between IT services and customers needs improvement
Local IT departments are kept in the dark, they also need information as soon as possible
Technical staff is too busy fixing the problem. Common rules a required to work faster and more productive

2.3 Service Desk

The Service Desk is an important function in the different Service Management processes. It is a contact place between service providers and customers/users, on a day-to-day basis. It is also a single-point for reporting incidents and making service requests. Service Desk keeps users informed of any changes that might have impact to their day-to-day activities, like service events, actions and opportunities. (OGC 2001, 14)

2.4 OIT Service Desk

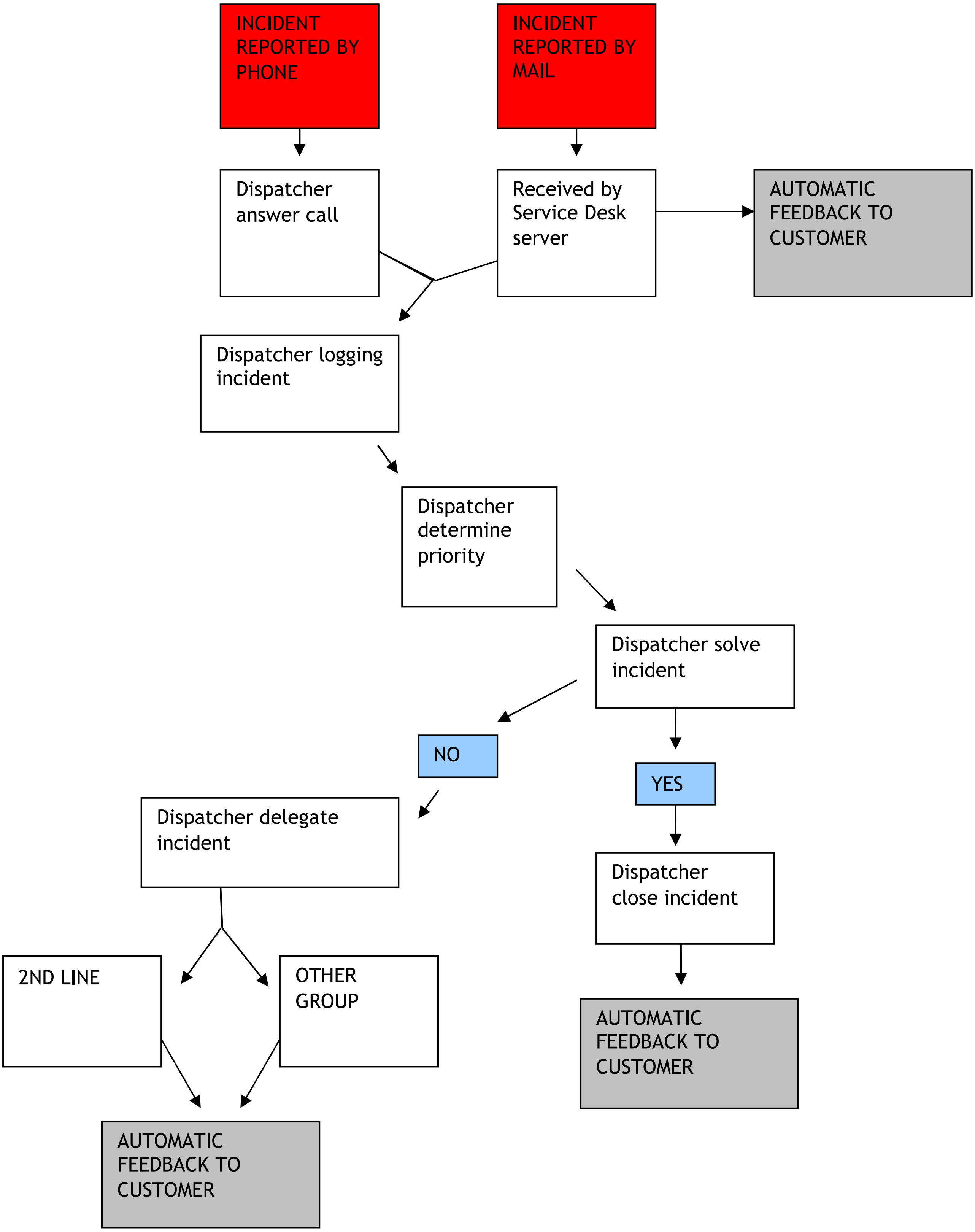
The OIT Service Desk is an internal technical support function within OMX with a round the clock availability. The OIT Service Desk is responsible for Incident Management and it provides a single point of contact for all the customers/users within OMX. Users can contact OIT Service Desk via telephone, email or by the OMX Customer Support Web.
The OIT Service Desk is always responsible for resolving Customer requests. When extra support is needed the OIT Service Desk will take ownership of the customers request and escalate it to 2nd and 3rd line support until resolution.

2.4.1 Service

The OIT Service Desk is always available to respond to phone calls, emails and web requests from the customer. Initially, the request will be recorded in on-line log system.
When the user is identified the OIT Service Desk will request details on what service and systems the request concerns. The specific issue will then be recorded and a priority will be agreed with the user. If possible the Service Desk will immediately resolve and close the request. If it cannot be resolved immediately it will be processed in accordance with the agreed priority.

When needed, the OIT Service Desk will escalate the request to 2nd and 3rd line support and request feedback after certain intervals. The feedback will be recorded in the log system and will be made available to the user. The OIT Service Desk will also call or email the feedback to the user. Incidents requiring hhgher att%ntion will immediately be escalated by the OIT Service Desk, using the Major Incide.t procedure, The3e incidents owner will always "e the Incident Manager. Incident Manager is a role within tHe OIT Service Desk and it is available in a Major Incident situations.

The OIT Service Desk is also responsible for informing the customer about any reduction in the services used by the customer. The OIT Service Desk will be made aware of such issues from system operators or from other customers experiencing problems.


INCIDENT REPORTED BY PHONE
INCIDENT REPORTED BY MAIL
Dispatcher answer call
Received by Service Desk server
AUTOMATIC FEEDBACK TO CUSTOMER
Dispatcher logging incident
Dispatcher determine priority
Dispatcher solve incident
NO
YES
Dispatcher delegate incident
Dispatcher close incident
2ND LINE
OTHER GROUP
AUTOMATIC FEEDBACK TO CUSTOMER
AUTOMATIC FEEDBACK TO CUSTOMER

Picture 2 OIT Service desk flowchart

2.4.2 Availability

The OIT Service Desk Function is available around the clock.
The support can be handled in two different languages around the clock: English and Swedish.
The support can be handled in two supplementary languages: Finnish and Danish, within the office hours.

On hand support resources are distributed in **the** following locations:

Sweden	US
Finland	Canada
Denmark	Australia
Norway	Hong Kong
Iceland	Singapore
Baltic	India

UK get on hand support from Sweden every second month.
OIT Service Desk can deliver a higher quality service by having support resources in the same time zone and geographical region as the Customer.

2.4.3 Priority

The OIT Service Desk works with fixed priority levels. The defined priority levels and the maximum resolution times for incidents are:

Priority	Explanation
Critical	Major Incident Very High Internal to be resolved immediately. Work until resolved all hours.
High	Immediately attention. Work during Office hours.
Medium	Start to work with **it** within 1-2 working days. Work during Office hours.
Low	Start to work with **it** within 7 working days. Work during Office hours.

2.5 Remedy Action Request System

Remedy Action Request System (also known as Remedy, AR System and ARS) is a Client-server software application with development environment from BMC Software. Action Request System uses a third party database, like SQL Server or Oracle for storing data in tables. Action Request System has an open API, a feature which allows users to create custom client tools and scripts that talk directly to the Action Request System. (Wikipedia)

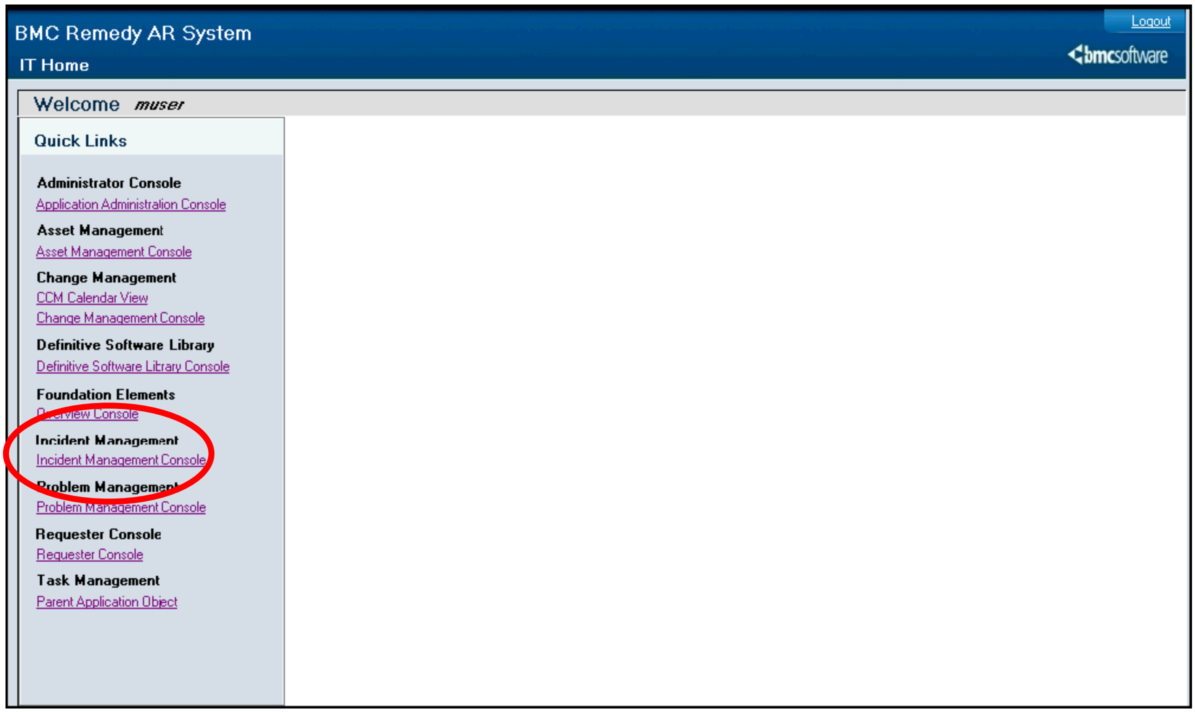
To use Action Request System a client tool is required to interact with the main component, AR Server. There are different client tools, like BMC Remedy User or BMC Remedy Administrator. The clients communicate with the AR Server via the open API. (Wikipedia)

Action Request System has different applications. Here is a list of some of them:

BMC Remedy Help Desk
BMC Remedy Service Desk: Incident Management
BMC Remedy Service Desk: Problem Management
BMC Remedy Change Management
BMC Remedy Customer Support
BMC Remedy Service Level Management
BMC Remedy Asset Management
Knowledge Base

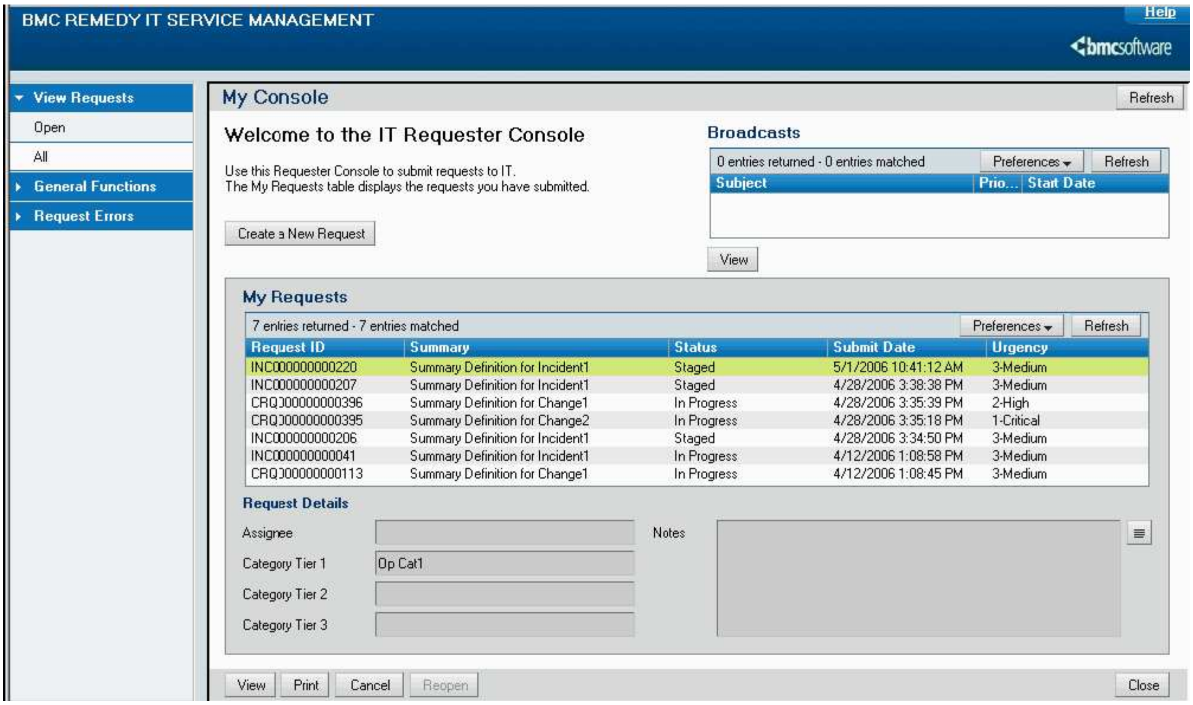
2.6 Action Request System in OMX

Action Request System used in OMX is specially tailored, every unnecessary features and applications has been removed. OIT Service Desk will login into system and the main console view will open. Service Desk uses the Incident Management console.



Picture 3 OMX ACTION REQUEST MAIN CONSOLE

The Requester console serves as the front end to the Incident Management applications. The console is the entry point for users to create, view, update, or cancel their own service requests.



BMC REMEDY IT SERVICE MANAGEMENT

My Console

Welcome to the IT Requester Console

Use this Requester Console to submit requests to IT.
The My Requests table displays the requests you have submitted.

Broadcasts

0 entries returned - 0 entries matched

Subject	Prio...	Start Date

My Requests

7 entries returned - 7 entries matched

Request ID	Summary	Status	Submit Date	Urgency
INC000000000220	Summary Definition for Incident1	Staged	5/1/2006 10:41:12 AM	3-Medium
INC000000000207	Summary Definition for Incident1	Staged	4/28/2006 3:38:38 PM	3-Medium
CRQ000000000396	Summary Definition for Change1	In Progress	4/28/2006 3:35:39 PM	2-High
CRQ000000000395	Summary Definition for Change2	In Progress	4/28/2006 3:35:18 PM	1-Critical
INC000000000206	Summary Definition for Incident1	Staged	4/28/2006 3:34:50 PM	3-Medium
INC000000000041	Summary Definition for Incident1	In Progress	4/12/2006 1:08:58 PM	3-Medium
CRQ000000000113	Summary Definition for Change1	In Progress	4/12/2006 1:08:45 PM	3-Medium

Request Details

Assignee	
Category Tier 1	Op Cat1
Category Tier 2	
Category Tier 3	
Notes	

Picture 4 OMX ACTION REQUEST REQUESTER CONSOLE

2.7 Short Message Service (SMS)

Short Message Service (SMS) is a communications protocol allowing the interchange of short text messages between mobile telephony devices. The SMS technology has facilitated the development and growth of text messaging. The connection between the phenomenon of text messaging and the underlying technology is so great that the term "SMS" is used as a synonym for a text message from another person or the act of sending a text message. (Wikipedia)
In OMX there is a program where is possible to define contact lists and messages to users. SMS is only used to send critical messages during an incident.

3 PROJECT DESCRIPTION

3.1 Customer

OMX is a leading expert in the exchange industry and it owns exchanges in the Nordic and the Baltic region. OMX develops and provides technology and services to companies in the securities industry around the globe. OMX has operations in Australia, Canada, China, Denmark, Estonia, Finland, Hong Kong, Iceland, Italy, Latvia, Lithuania, Norway, Singapore, Sweden, UK, US. (OMX Corporation). OMX has three cornerstones: operating OMX-owned marketplaces, developing cutting-edge technology and global customer base. These cornerstones together give OMX an ability to provide solutions for more efficient securities transactions. Vision is to be known as the world leading partner in securities transactions. (OMX Corporation).

“HISTORY

1985 OMX starts derivatives exchange

1987 World’s first publicly listed exchange

1991 World’s first integrated derivatives trading and clearing system

1994 First exchange in Europe to accept remote members

1997 Creation of derivatives link network

1998 Merger of OMX and Stockholm Stock Exchange

1998 Joint trading platform, initiative started on all the Nordic exchanges

2001 Common member and trading rules instituted in Nordic region

2002 Formation of EDX derivatives exchange – OMX and London Stock Exchange

2003 Merger of OMX and HEX, including Tallinn and Riga exchanges

2004 Acquisition of Vilnius Stock Exchange

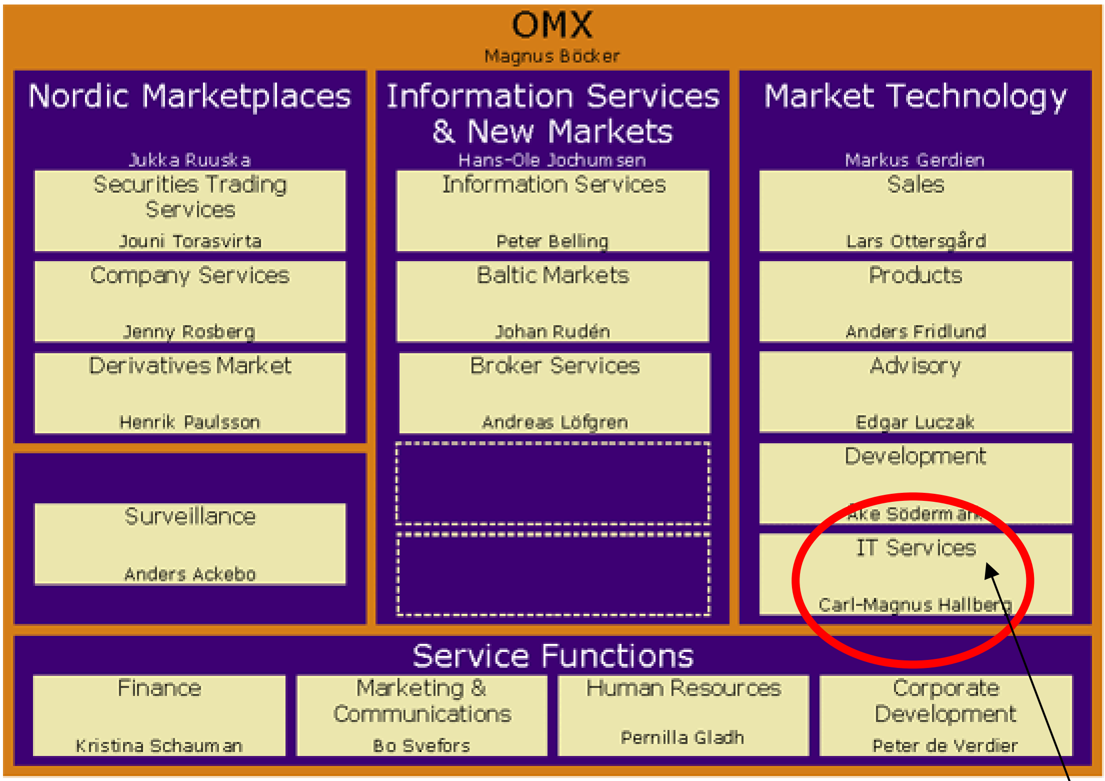
2004 Implementation of joint trading platform on all Nordic exchange

2005 Merger of OMX and Copenhagen Stock Exchange

2006 Launch of OMX Nordic Exchange

2006 Merger of OMX and Iceland Stock Exchange”

(OMX Corporation)



Picture 5 ORGANIZATIONAL CHART (OMX Corporation)

Project department

3.2 Project assignment

Project assignment was to get to know ITIL principals and create Major Incident procedure for Office IT department using those principals. The Major Incident procedure was ordered by OMX Technology and the project was mainly carried out in Stockholm, Sweden.
In OMX we already had basic process plan to major incidents, so I was required to use this process plan in my own work. That's why my work is called procedure instead of process, since the main plan is called process.

3.3 Future projects

The Procedure for OIT was part of the ITIL implementation that OMX is implementing (One process at a time), the internal project for that was called the CSIP.
In the near future there are going to be other implementations in other departments as well as other procedures in OIT, such as computer management procedure, which will contain a list of all computers and accessories in use. These new procedures will help us to organize computers and software, and they will create a base for more effective organization.

3.4 My goals

This was a great opportunity to be a part of international project and increase my communication and writing skills in English. Working environment in Sweden is different from Finland so I got a good work experience from this project which will benefit me in the upcoming assignments. My goals in this project were to understand ITIL principals and how to use them to create the procedure. Also getting to know Service Desk routines and tools was one goal that I wanted to accomplish. Last, but not least, my personal goal was to open communication channel between myself and my co-workers in Stockholm and in Copenhagen.

4 PROJECT EXECUTION

The project started in September 2006. The Project team and management were located in Stockholm, so all the meetings around the project were there. My contact persons were Marie Carlsson (Manager) and Carina Fridell (Service Desk leader).

4.1 My assignment

My involvement started in October 2006. My assignment was to create Office IT procedure, which included all the possible system failures that will affect many users and were consider major. My assignment started with participating in many meetings in Stockholm. I received a lot of material and got so much information that it took few days to process it all. I also participated on ITIL course. The procedure was supposed to be using the ITIL principals, since the future projects will use the same principals. By doing that, the company hopes to achieve similar procedure structures.

4.2 My schedule

During the fall I made three trips to Stockholm, but most of the writing work I did at home. My time in Stockholm went mostly in meetings, in gathering information and in communication with my co-workers. The procedure was supposed to launch in March 2008. I had enough time to write the procedure and in the end I even had some extra time.

4.3 Writing the procedure

The begging was difficult, of course, but when I organized all the information I had and wrote one chapter at time, the whole picture started to be formed. Since I was full-time mom I did most of the writing at night, when it was nice and quiet. Although the writing was challenging and very rewarding since I needed to think almost every word I write.

4.4 Training

When the Major Incident procedure was finished it was time to held training to IT personnel in Stockholm, Finland and Copenhagen. The purpose of the training was to give the personnel more information about the procedure and let them ask questions. The most important reason that we decided to hold training was to show everyone how important it is to follow this procedure during the major incident and how it will hopefully improve communication between IT personnel and customers/users.

4.4.1 Training in Stockholm

The first training was in Stockholm and it was scheduled on January, 15-16.1.2007.
I flew to Stockholm on 15th of January in the morning. I had reserved a meeting room and sent the invitations to personnel before. Most of the IT personnel are located in Stockholm, so I needed to keep several training sessions. I had scheduled four training sessions per day, two in the forenoon and two in the afternoon. One training session lasted approximately one hour.

All trainings went well and hopefully we sent the message to the IT personnel how important it is to work altogether during the major incident and in all times as well.

4.4.2 Training in Copenhagen

Training in Copenhagen was scheduled on January, 24.1.2007. I flew to Copenhagen on 24th of January in the morning. All the meeting room reservations were made for me by a colleague in Copenhagen. Training went fine, although some of the information was unnecessary for them.

4.4.3 Training in Helsinki

Training in Helsinki was scheduled on February, 12.2.2007. The training was a different from the other trainings since it was held in Finnish language and it was easier to talk to people that I have worked with in several years. Actually it wasn't even a real training, we just discussed about the Major incident procedure and I also showed how the Action request console is going to look and how it is going to work. Discussion was very productive and I hope that the co-work will work smoothly between these countries in the future and especially if we have some major incident.

4.4.4 OIT Global meeting

The project ended with a big global meeting in Stockholm. The meeting lasted for three days and during that time we had more ITIL information and on-going ITIL projects in the company. We got the information about the offices in New York, Sydney, and Reykjavik. I also held my last training in this meeting and all thought that the personnel in New York and Reykjavik had received the procedure by mail and that they understood the big picture better in this training. The global meeting was a success and ended with good Swedish food and wine with a pleasant company.

5 PROJECT ESTIMATION

5.1 Project success

Altogether the project was a success. We were able to create the new procedure and get it in use. Also we got new software to handle incidents. The procedure was done using the ITIL principals which will be more advanced in the near future when we will decide to reform other processes in the IT department. The Major Incident Procedure is just one part of the IT department document and work flow that needs to be reformed. Functional work tools are crucial to large IT department in order to work smoothly and give customers the best service as possible.

5.2 Project manager estimate

Project Manager was satisfied with my work effort and especially she was very pleased with the major incident training that went well and hopefully gave employees more information.

5.3 My learning

In the beginning of the project I had couple of goals for my learning. First, I wanted to learn the ITIL principals and how to use them in practise. Second was to improve my writing skills in English and third was to get to know my co-workers better. I took the ITIL course and I think I got the information I needed, so my goal was fulfilled and I was able to write the procedure. Since I have been writing this thesis, I have discovered that my writing skill in English has been improved enormously and I have increased my vocabulary. My co-workers in Stockholm, Copenhagen and Helsinki have become more familiar. Now I have more information about their job description and agendas, especially in Stockholm. So, I can say that the project was a success as well as my own learning.

List of sources

Aim Academy’s course material

OGC Best Practice for Service Deliver ITIL The key to Managing IT Services

Project material/Meeting material

http://en.wikipedia.org/wiki/Action_Request_System
(seek and read 21.1.2008)
http://www.omxgroup.com/omxcorp/?languageId=1
(seek and read 15.1.2008)
http://en.wikipedia.org/wiki/Short_message_service

(seek and read 21.1.2008)

List of captions

LIST OF APPENDIX

APPENDIX 1

Major Incident Procedure

IT Services, Office IT

This document describes the procedures for managing Major Incidents affecting the office environment.

Document Id:	MIP01012007
Document Version:	2, Approved
Document Owner:	OIT Helpdesk
Last updated:	Tuesday, June 22, 2010 by Petra Kupiainen

Contents

Document Control

Document location

Document location
OMX Insite

Revision History

Version	Date	Changed by	Summary of Changes
1	3.1.2007	MaCa	First approved version
2	28.2.2007	PeKu	Changing the SMS message text

Approvals

This document requires the following approvals:

Name	Title
Mika Rytkönen	Process Manager, Incident Management
Marie Carlsson	Office IT Manager

1 Types of incidents

The following types of Major Incidents is covered in this procedure

- Mail
- Virus
- Domain
- Network (contacts)

1.1 Major Incidents

Below is a list which will tell if the incident is considered major.

If the following criteria will be realized, then the incident is considered to be Major and the Major Incident routine is required to take in use (Activities are described in chapter 2).

1.1.1 Criteria for opening a Major Incident

Mail

- Necessary to stop or delay incoming/outgoing mail due to incidents or virus.
  Weekdays - more than 30 minutes
  Week-ends - more than 4 hours
- Mail service not available. Not estimated to be able to restore service:
  Weekdays - within 30 minutes
  Week-ends - within 4 hours

Virus

It is very complex to list criteria for virus as they often are based on several components and how they relate to each other such as spread and the harm the virus causes. Therefore the decision must be based on skill/knowledge and decided from case to case.

The following issues should however be considered:

- The virus is spreading out of control (for example: mail attachment)
- Virus is threatening business operations
- Virus is classified as very harmful by anti virus companies

Domain/Network

This major incident is probably something that will happen rarely. Although it is important to cover this since the problem may occur in the business critical departments.

Network: On-call is 24*7 and is activated from the **OSC/first line**

The following issues should be considered:

- Several users can't log in the computer in different sites
- Domain controllers are down
- Several computers are down in business critical areas
- The connection to other location fails
- Firewall authentication to Office environment fails

1.1.2 Criteria for closing the Major Incident

Mail

- Service is restored and is not effecting daily business operation.
- If the service is restored, but long queues exist in the system, the Incident Manager might reduce the staff working with the incident and close the phone conference. The incident will however be regarded as open until normal operation is restored.

Virus

- The virus is identified and it is known how it is spreading
- It is known how to clean computers and the information is disseminated to affected offices/sites.
- All currently connected computers have been cleaned
- There are personnel available at other affected offices/sites with information, competence and tools to handle laptops the following working day. Information to users is set up in all entrances to affected OMX offices.

Domain/Network

- Log-in is possible again
- Broken equipments are repaired/replaced
- Network connections are working again

2 Activities

2.1 Incident detection

Incident can be detected by user or IT personnel. If detection is made by user, they will likely call to Service Desk, which will inform System Management. If detection is made by System Management, it is important that they inform Service Desk, so that they have information to users. Also co-operation between IT departments is very important, especially in Major Incident situation.

Activity	Responsible
Alert Responsible On-Call (ROC) person for System	Service Desk, System Management
Perform incident assessment and decide if Major Incident or not	
Inform the Service Desk and the other on-call line	
Inform the Incident Manager	

2.2 During incident

Incident Manager will be the information channel throw the whole procedure. Service Desk will keep the users happy (giving the information that they need, nothing more nothing less)

Activity	Responsible
Open telephone conference	Incident Manager
Send SMS information about the Major Incident, **Use pre-defined template SMS list: *"OFFICE Incident"***	Service Desk
Call in on phone conference to get information on extent of and if additional resources are needed.	System Management (all available staff)
Update the Service Desk answering machine with short information about the disturbance (instant phone message)	
Inform other parts of ITS, if it's necessary (SMS) DCS on-call makes the assessment if there is a potential threat to the production environment and if other teams should be involved as well	Incident Manager
Inform users using appropriate information channels	Service Desk
Virus incidents: Assure the different offices have the appropriate information and tools to clean-up the virus	System Management
Inform all parties involved when incident is closed using appropriate channels	Service Desk

2.3 Incident follow-up and reporting

Create Major Incident report and conduct follow-up meeting using designated template	Incident Manager
Follow-up on identified actions until solved.	Office IT Manager
Register the incident in the ARS Remedy system	Service Desk

2.4 Post incident activities

Some of the major incidents might need activities although the incident itself is solved. These actions are called post incident activities and here is instructions how to handle them.

2.4.1 Mail

- Give users instructions how to handle if they received virus in mail (attachment). System Management needs to give details to Service Desk (virus name etc.), so they can inform users by mail or by phone.
- Advise users to clean up mail regular bases to avoid server overload (After incident is good to remind users to clean their mailbox once in a while)

2.4.2 Virus (Cleaning and Pre-scan)

1. Pre-scan

The VirusScan Enterprise software contains a feature that enables technical staff to remotely force a re-boot of the computer and then immediately perform a thorough pre-scan of the computer before it accesses the network.
This feature can be activated during a virus related incident.

2. Cleaning

- Assure the different offices have the appropriate information and tools to clean-up the virus. Depending on type of virus the information should be distributed to offices using these channels.
  - Send by mail
  - Published on Intranet
  - Verbally on the phone conference
- Assure there is information displayed in all entrances to OMX buildings informing the users that they are not allowed to connect portable computers to network without having them controlled by the local Office IT department first.
- The Incident Manager is responsible for assuring resources are available at each affected site and escalate to ITS Management if needed.

3 Decisions

During the incident there might be important decision to make and here is the list of them and who is authorized to make the decision.

If several roles are listed under "Authorized to take decision" this means that the decision can be taken by **anyone** of the listed roles. This procedure is necessary to avoid situation that no-one can't make the decision on a critical moment.

3.1 Mail

Decision needed	Authorized to take decision
Stop or delay incoming/outgoing mail (Back-Office for Hire must be informed! See 5.3)	• Incident Manager • Responsible On-Call, System Management • OIT Manager
Close mail servers (Back-Office for Hire must be informed! See 5.3)	• Incident Manager • Responsible On-Call, System Management • OIT Manager
Restart mail system	• Incident Manager • Responsible On-Call, System Management • OIT Manager
Restore (when/if and to what extent)	• Incident Manager • Responsible On-Call, System Management • OIT Manager

3.2 Virus

Decision needed	Authorized to take decision
Close down the Fire Wall between Office and Production environment	• IT Security Manager • Manager IT Services • (Head of group security)
Close down all connections to the Internet	• IT Security Manager • Manager IT Services • (Head of group security)
Terminate connection to other offices	• IT Security Manager • Manager IT Services • (Head of group security)
Close user accounts	• Incident Manager • Responsible On-Call, System Management
Close VPN connection	• Incident Manager • Responsible On-Call, System Management

3.3 Domain

Decision needed	Authorized to take decision
Close down the Fire Wall between Office and Production environment	• IT Security Manager • Manager IT Services • (Head of group security)
Replace broken equipments	• Incident Manager • Responsible On-Call, System Management
Close down domain controller server	• Incident Manager • Responsible On-Call, System Management

4 Roles and responsibilities

4.1 Responsible On-call (System Management)

- The ROC is responsible for informing the IM of what resources are needed. Also the ROC is responsible for delegating tasks to resources and sees to it that they are executed. The ROC will keep a close contact with the IM and make sure the IM is updated on the progress of dealing with the incident.
- Log all actions with corresponding timestamps during the Incident.
- If On-call personnel is in need of help from other resources this should be reported to Incident Manager who has the authority to use any resources within IT Services
- Inform Incident Managers of possible problems during the Incident and directly inform about all actions taken.

4.2 Incident Manager

- Inform customers about the status, severity and impact from both technical and business perspective
- Log all actions with corresponding timestamps during the Incident
- Write the Incident report
- Contact Problem Management for follow-up meeting (if necessary)
- The Incident Manager has the authority to call in and use any needed resources within IT Services during a Major Incident

4.3 Service Desk

- Give users information over the phone
- Assist Incident Manager if needed

5 Information channels

5.1 Incident Managers and on-call personnel

- Incident Managers (Weekday 09-17 CET)
  Incident Managers (all other times)
- Responsible On-call (ROC) Mail
- Responsible On-call (ROC) System Management
- Responsible On-call (ROC) Network

If Incident Managers are occupied, ROC will act as Incident Manager

- OIT Service Desk

5.2 Phone conference numbers

Host	Dial:	**6700**
	Enter code:	
Guests	Dial:	**6700**
	Enter code:	

Useful features

*0	Get in touch with operator	*6	Self-mute/un-mute
60#	Mute all guests	61#	Un-mute all guests
*7	Lock/un-lock the meeting		

5.3 Information via phone call (Back-office for hire)

In case of mail problems where there is need to either **Stop or delay incoming/outgoing mail** or **Close mail servers**, Back-Office for Hire must be informed! This is applied 08:00 – 18:00 CET.

Markets Helpdesk	+46 8 405 **7400**

5.4 SMS to predefined recipients

SMS is sent out by OIT Service Desk (available 24x7).
Complete list is available in:

\\Seomadm1\OMT\OMT Operations\IT Services\Processes

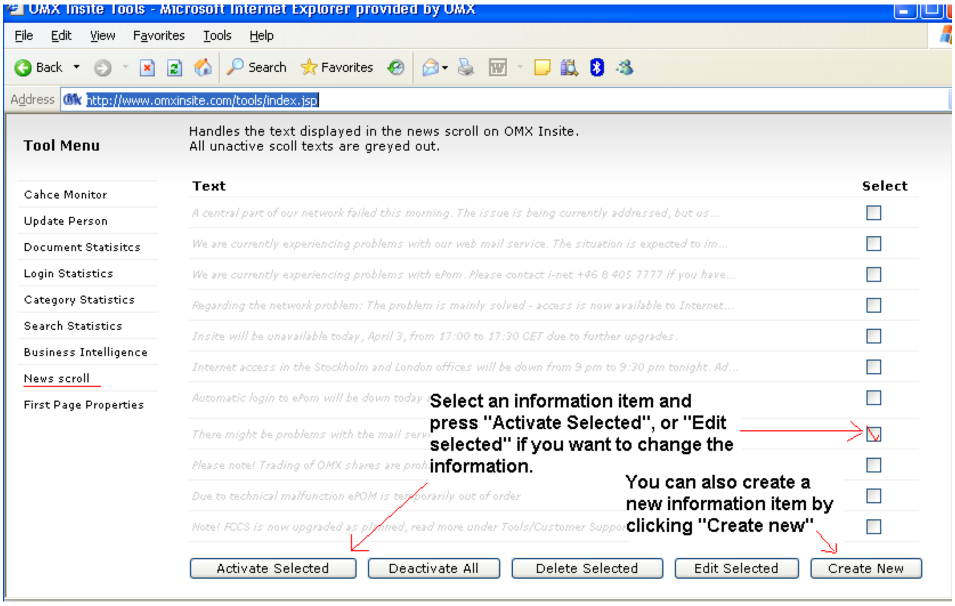
5.5 OMX Insite – News scroll

The news scroll is to be used primarily to inform about system errors concerning the whole company. Please note that the whole company all over the world will see the message. It is not possible to direct the news scroll to certain groups only.

How to create a news scroll?

Go to http://www.omxinsite.com/tools/index.jsp and choose News scroll.

Contact:
OIT Service Desk


OMX Insite Tools - Microsoft Internet Explorer provided by OMX
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.omxinsite.com/tools/index.jsp
Activate Selected
Deactivate All
Delete Selected
Edit Selected
Create New

Tool Menu

- Cahce Monitor
- Update Person
- Document Statisitcs
- Login Statistics
- Category Statistics
- Search Statistics
- Business Intelligence
- News scroll
- First Page Properties

Handles the text displayed in the news scroll on OMX Insite.
All unactive scoll texts are greyed out.

Text	Select
A central part of our network failed this morning. The issue is being currently addressed, but us…	□
We are currently experiencing problems with our web mail service. The situation is expected to im…	□
We are currently experiencing problems with ePom. Please contact i-net +46 8 405 7777 if you have…	□
Regarding the network problem: The problem is mainly solved - access is now available to Internet…	□
Insite will be unavailable today, April 3, from 17:00 to 17:30 CET due to further upgrades.	□
Internet access in the Stockholm and London offices will be down from 9 pm to 9:30 pm tonight. Ad…	□
Automatic login to ePom will be down today	□
There might be problems with the mail serv	□
Please note! Trading of OMX shares are proh	□
Due to technical malfunction ePOM is temporarily out of order	□
Note! FCCS is now upgraded as planned, read more under Tools/Customer Suppor	□

Select an information item and press "Activate Selected", or "Edit selected" if you want to change the information.

You can also create a new information item by clicking "Create new"

5.6 Mail to all employees

Must be authorized by: Incident Manager or Office IT Manager

Send out a mail to affected/selected user groups using one of the following mail lists:

@All-Sweden
@All-Finland
@All-Denmark
@All-Iceland
@All-Norway
@All-Latvia
@All-Lithuania
@AllEstonia
@All-UK
@All-Italy
@All-US
@All-Canada
@All-Australia
@All-HongKong
@All-India
@All-Singapore

Or if problem consist whole company use group **@All-OMX**
Group containing all employees at OMX (contains the groups listed above).

5.7 Information displayed on screen in the reception area at Tullvaktsvägen

Currently no specific authorization is needed.

The info to be displayed (usually a PowerPoint slideshow) shall be sent to OIT Service Desk. They will logon to the computers with the administrator account, store the presentations locally and then start the presentations on the computers connected to the projectors.

The computers are (from left to right) SE10PROJ01, SE10PROJTV01, SE10PROJ02.

Note! This information will be visible for external visitors and customers and should be carefully used!!

5.8 Changing "instant phone messages" for the Service Desk during an incident (Ext. 7777)

To activate and deactivate ”instant phone message”, the initial queue message for each queue is switched.

- Call extension 1047 and follow the instructions.
  Press either "1" to activate a message or "0" to deactivate.
- There are currently three different instant phone messages to chose between:

No.	Message text
1	We are having problems with the email right now, if you are having problems with something other than email stay on the line and you will be re-directed to Office IT Service Desk.
2	We are having problems with the network right now, if you are having problems with something other than the network stay on the line and you will be re-directed to Office IT Service Desk.
3	We are having problems with OMX Insite right now, if you are having problems with something other than OMX Insite stay on the line and you will be re-directed to Office IT Service Desk.

The standard message is as follows:

No.	Message text
4	There is lot of calls right now, you will be placed in a queue and we will serve you as soon as possible. You can also send an email to OIT Service Desk.

5.9 SMS to all employees

Must be authorized! Information must be approved by Press Office & Internal Communication Manager.

This will only be used under very special circumstances. Currently this is possible only at 08:00 – 18:00 working days. Information is sent out by OIT Service Desk.

5.10 Sample texts

Here are some samples of information texts:

Mail	
SMS	**SMS #1** MAJOR INCIDENT VERY HIGH INTERNAL: **Mail system down**, please join conference. Phone: + 46 8 405 6700, Code : 122110# //OIT Service Desk **SMS #2** Status Information: **Mail is working.** //OIT Service Desk
Insite News scroll	• We are experiencing mail problems at the moment. Information will be published as soon as we have any news or estimates when it will be solved. • Mail problem solved, queued mails will be delivered ASAP.
Mail to users	• At the moment there are problems with (*incoming* or *outgoing* mails), we are working with the problem and will inform you when we have more information and when it is solved. • Mail problem is solved! Mails sent to/from OMX are queued and will be delivered ASAP.

Virus	
SMS	**SMS #1** MAJOR INCIDENT VERY HIGH INTERNAL: **VIRUS** is spreading in office environment, please join conference. Phone: + 46 8 405 6700, Code : 122110# //OIT Service Desk **SMS #2** Status Information: **Virus** is under control, information will follow. //OIT Service Desk
Insite News scroll	Virus infection in OMX! OMX was hit a virus and it is spreading by mail, don’t open attachments until you are sure that those are safe.
Mail to users	Should be decided from case to case, depending on type of virus! • OMX was hit by a virus. If you suspect your PC is infected, call OIT Service Desk +46 8 405 7777. • Virus infection stopped! Do not click on attached files unless you are expecting files and are sure of the origin and that they are free of virus.

Domain	
SMS	**SMS #1** MAJOR INCIDENT VERY HIGH INTERNAL: **Network problem**, please join conference. //OIT Service Desk **SMS #2** Status Information: **Network problem** found, information will follow. //OIT Service Desk

Appendix A Checklists

5.11 Mail

The following activities/checks should be performed during a major incident related to mail.

Activity	Ok
Check if virus.	
Check if hardware malfunctions.	
Check for network problems.	
Determine the extent of the problem, does it concern outgoing, incoming or both.	
Is it internal or external?	

5.12 Virus

The following activities/checks should be performed during a Major Incident related to a virus attack.

Activity	Ok
Check with Anti-Virus vendors (Nai, Symantec etc) if it is a known virus.	
Determine what the virus does.	
Check patch-levels on contaminated computers.	
Check if the virus spreads.	
Identify the source of the virus.	
Inform affected offices/sites how to clean up the virus	
Assure there is a procedure and resources at all affected offices/sites for managing laptops the following business day	

5.13 Domain

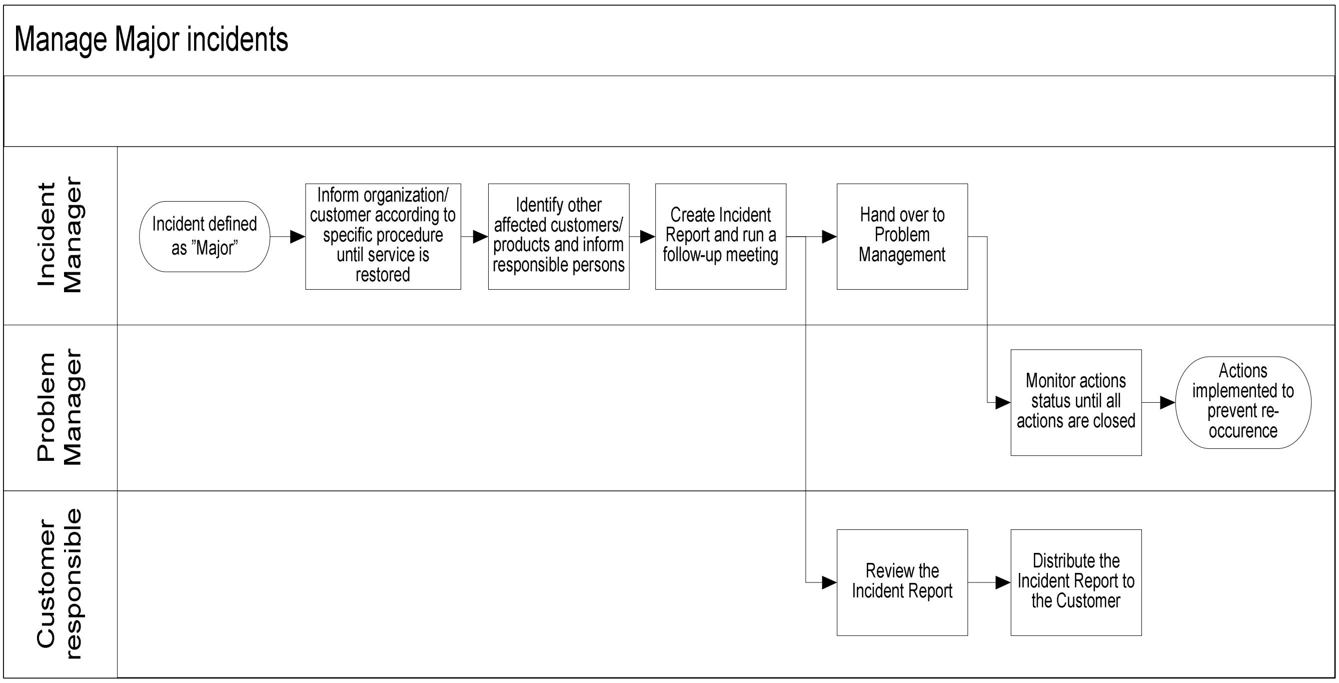
The following activities/checks should be performed during a Major Incident related to a network problem.

Activity	Ok
Check if hardware malfunctions or environmental (power, electricity) problems	
Check how many persons are affected by the incident	
Check that users can log-in	
Inform local offices/sites if it’s necessary	
If network issue contact OSC (Network On-call channel)	

5.14 Service Desk

Activity	Ok
Send SMS to pre-defined list	
Change “instant phone messages” for Service Desk (look chapter 5.8)	
Create News scroll in OMX Insite	
Mail to all users, if necessary (must be authorized by IM or Office IT Manager)	
Give users information by phone when/if needed	

Appendix B Workflow (picture)


Manage Major incidents
Incident Manager
Problem Manager
Customer responsible
Incident defined as "Major"
Inform organization/ customer according to specific procedure until service is restored
Identify other affected customers/ products and inform responsible persons
Create Incident Report and run a follow-up meeting
Hand over to Problem Management
Monitor actions status until all actions are closed
Actions implemented to prevent re-occurence
Review the Incident Report
Distribute the Incident Report to the Customer

Major Incident routine

Office IT

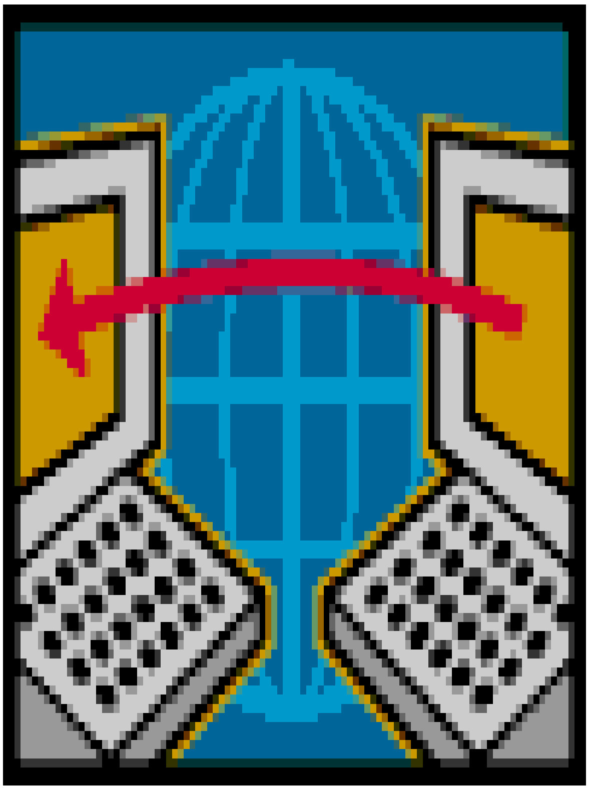
Efficient Securities Transactions

Background

Efficient Securities Transactions

We need to have Office IT organization, that support the global OMX Company.

Incident process and Major Incident routine are one part of that implementation.



APPENDIX 2

Routine

Efficient Securities Transactions

- Incidents (types and definitions)
- Activities (during and after a Major Incident)
- Decisions (who can authorize what)
- Roles and Responsibilities
- Information channels
- Checklists

APPENDIX 2

Major Incident - open

Efficient Securities Transactions

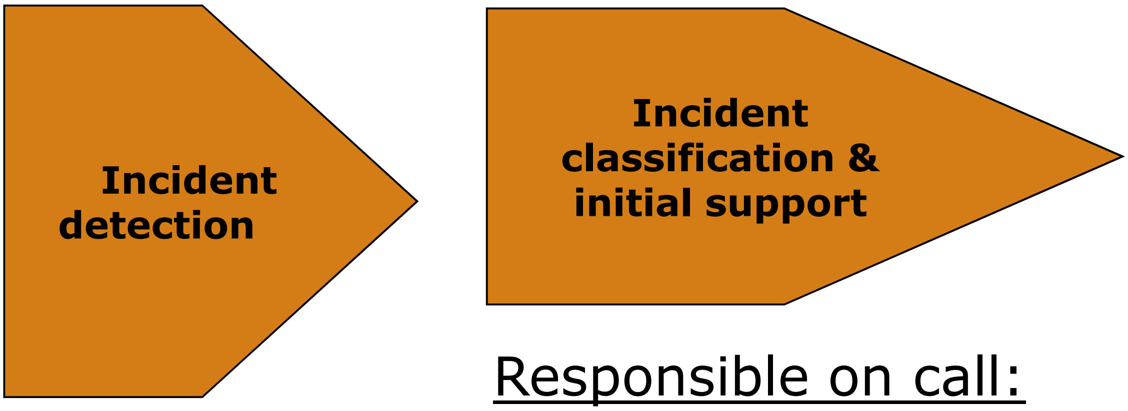
If the following criteria will be realized, then the incident is considered to be Major and the Major Incident routine is required to take in use

- Mail service not available
- Necessary to stop or delay incoming/outgoing mail Weekdays - more than 30 minutes
  Week-ends - more than 4 hours
- Virus is spreading out of control or is threatening business operations
- Virus classified as very harmful by anti virus companies
- Several users cant log-in
- Several computers are down in the business critical areas

APPENDIX 2

Incident detection

Efficient Securities Transactions



Incident detection

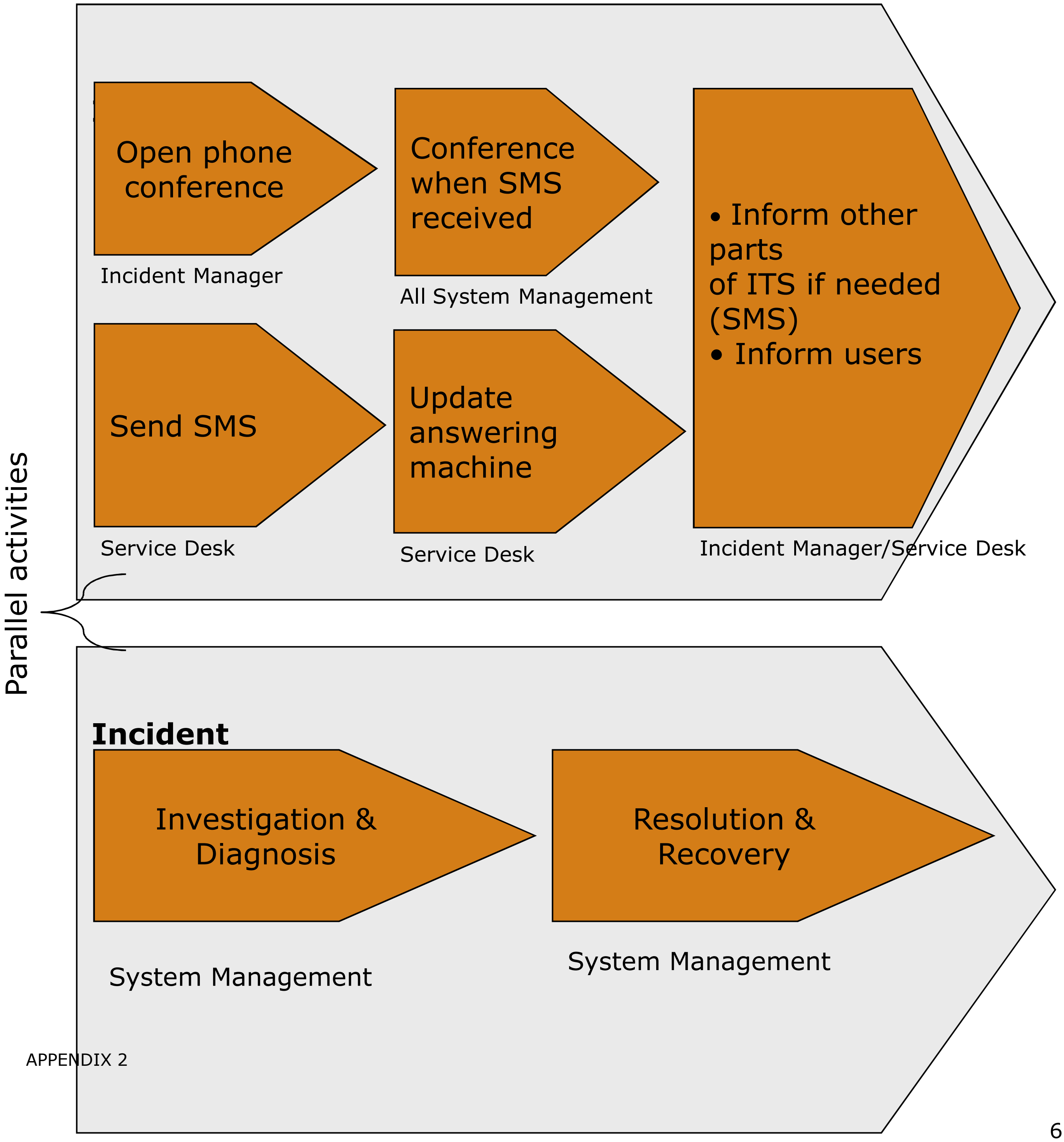
Incident classification & initial support

- Alert ROC (Responsible-on-call)

Responsible on call:

- Decide if Major Incident
- Inform the Service Desk and other on-call line.
- Inform the Incident Manager

During incident



Open phone conference

Incident Manager

Conference when SMS received

All System Management

- Inform other parts of ITS if needed (SMS)
- Inform users

Incident Manager/Service Desk

Send SMS

Service Desk

Update answering machine

Service Desk

Parallel activities

Incident

Investigation & Diagnosis

System Management

Resolution & Recovery

System Management

APPENDIX 2

Major Incident - closed

Efficient Securities Transactions

- Mail service is restored and is not effecting daily business operation
- If mail service is restored, but long queues exist in the system, the Incident Manager might reduce the staff working with the incident and close the phone conference. The incident will however be regarded as open until normal operation is restored
- The virus is identified and it is known how it is spreading
- It is known how to clean computers and the information is disseminated to affected offices/sites
- All currently connected computers have been cleaned

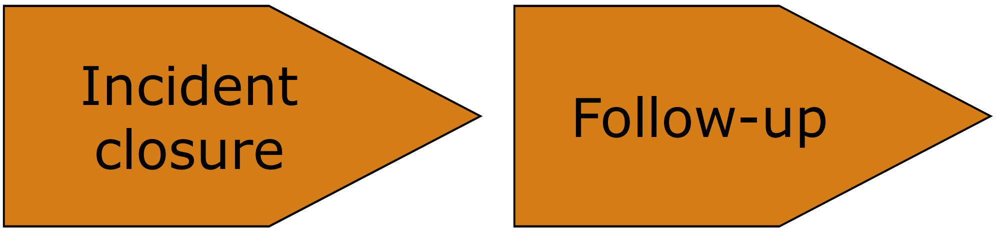
Major Incident - closed

Efficient Securities Transactions

- There are personnel available at other affected offices/sites with information, competence and tools to handle laptops the following working day. Information to users is set up in all entrances to affected OMX offices.
- Users are switched to use another network equipment
- Log-in is possible again
- Broken equipments are repaired/replaced or the plan repairing/replacing them is done
- Network connections are working again

APPENDIX 2

After Incident



Incident Manager

- Information to all

Service Desk

- Register incident in Remedy

Incident Manager

- Create Major Incident report
- Conduct follow-up meeting

Manager of Office IT

- Follow-up actions until solved.

Decisions

Efficient Securities Transactions

During the incident there might be important decision to make, so we have created an authorization list

If several roles are listed it means that the decision can be made by **anyone** of the listed roles.

This procedure is necessary to avoid situation that no-one can't make the decision on a critical moment.

APPENDIX 2

Decisions

Efficient Securities Transactions

Authorized: Incident Manager, OIT Manager,ROC

- Stop or delay incoming/outgoing mail
- Close mail servers
- Restart mail system
- Restore (when/if and to what extent)
- Close user accounts
- Close VPN connection
- Replace broken equipments on business hours
- Close down the domain controller server

Decisions

Efficient Securities Transactions

Authorized: IT Security Manager, Manager IT Services,

Head of group security

- Close down the Fire Wall between Office and Production environment
- Close down all connections to the Internet
- Terminate connection to other offices
- Activate pre-scan on selected/all computers.

APPENDIX 2

Roles responsibilities

Efficient Securities Transactions

ROC (System Management)

- Informing the Incident Manager:
  ✓Ask for resources that are needed
  ✓Keep close contact
  ✓Inform possible problems
  ✓Inform all actions that are taken

- Delegating tasks to resources and sees to it that they are executed

- Log all actions with corresponding timestamps during the Incident

Roles responsibilities

Efficient Securities Transactions

Incident Manager

- Inform customers about the status, severity and impact from both technical and business perspective
- Log all actions with corresponding timestamps during the Incident.
- Write the Incident report and conduct the follow-up meeting

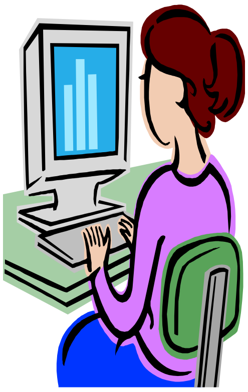
The Incident Manager has the authority to call in and use any needed resources within IT Services during a Major Incident

APPENDIX 2

Roles responsibilities

OIT Personnel

- Call in on conference when you have received Major Incident SMS
- Assist/participate in incident resolution if necessary

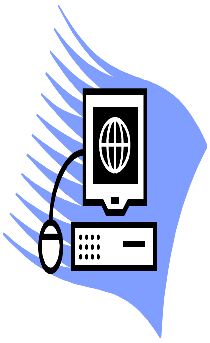


Service Desk

- Inform users
- Assist Incident Manager if necessary

Information channels

Efficient Securities Transactions



Technical staff

- SMS, sent when Major Incident is detected
- Phone conference

End-users

- OMX Intranet – News scroll
- Information displayed on screen in the reception area
- Mail to all employees
- SMS to all employees

OMX
Efficient Securities Transactions

TOGETHER – We can do it!

APPENDIX 2

HOW TO USE SMS TOOL

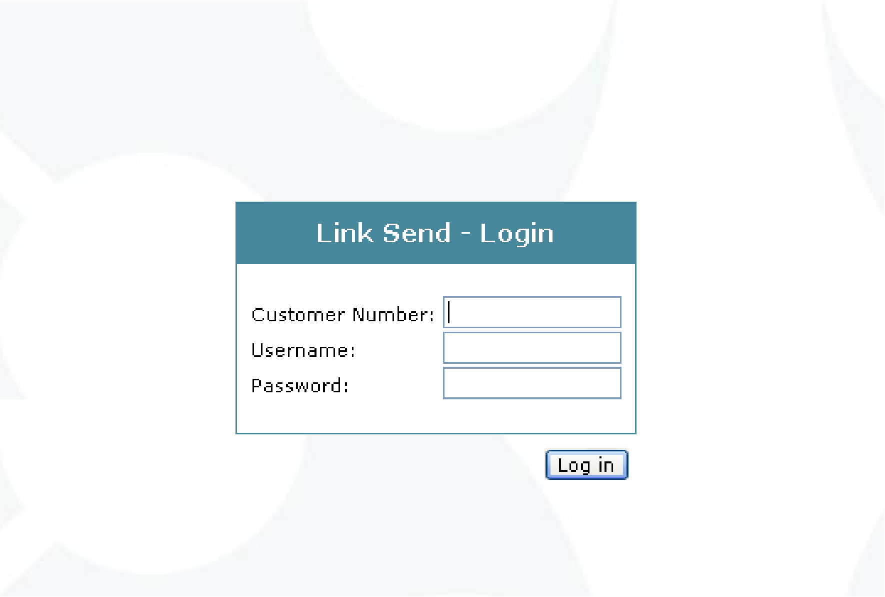
1. Log in to the system

You can find SMS tool from:
https://send.telenorlink.com/send/action/loginPage?unique=1164123489642

Customer Number:
Username:
Password:

You can select language from the login page (left corner down)
Available languages are: English, Svenska, Norsk and Dansk

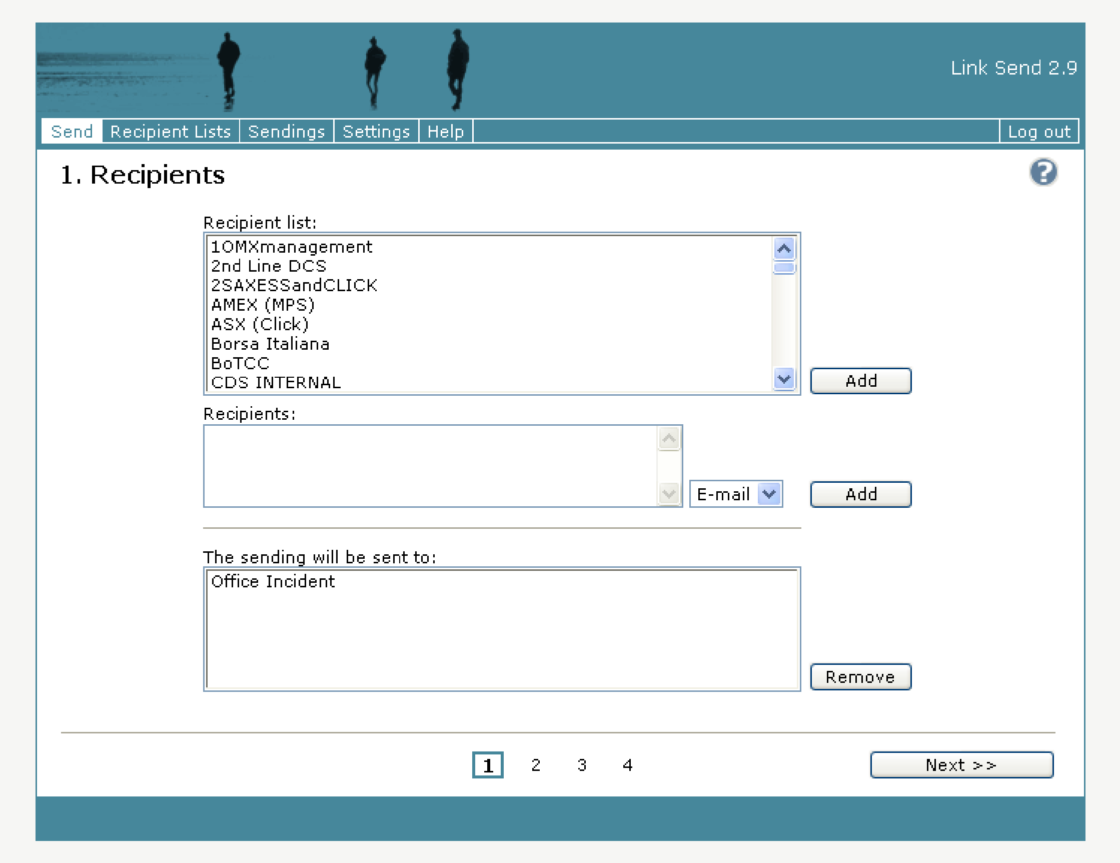
Log –in using the information below



2. Sending an SMS Message

1. First view is the Recipients list

- ➢Select list/lists you need, click add
- ➢Choose Next>



1. Recipients

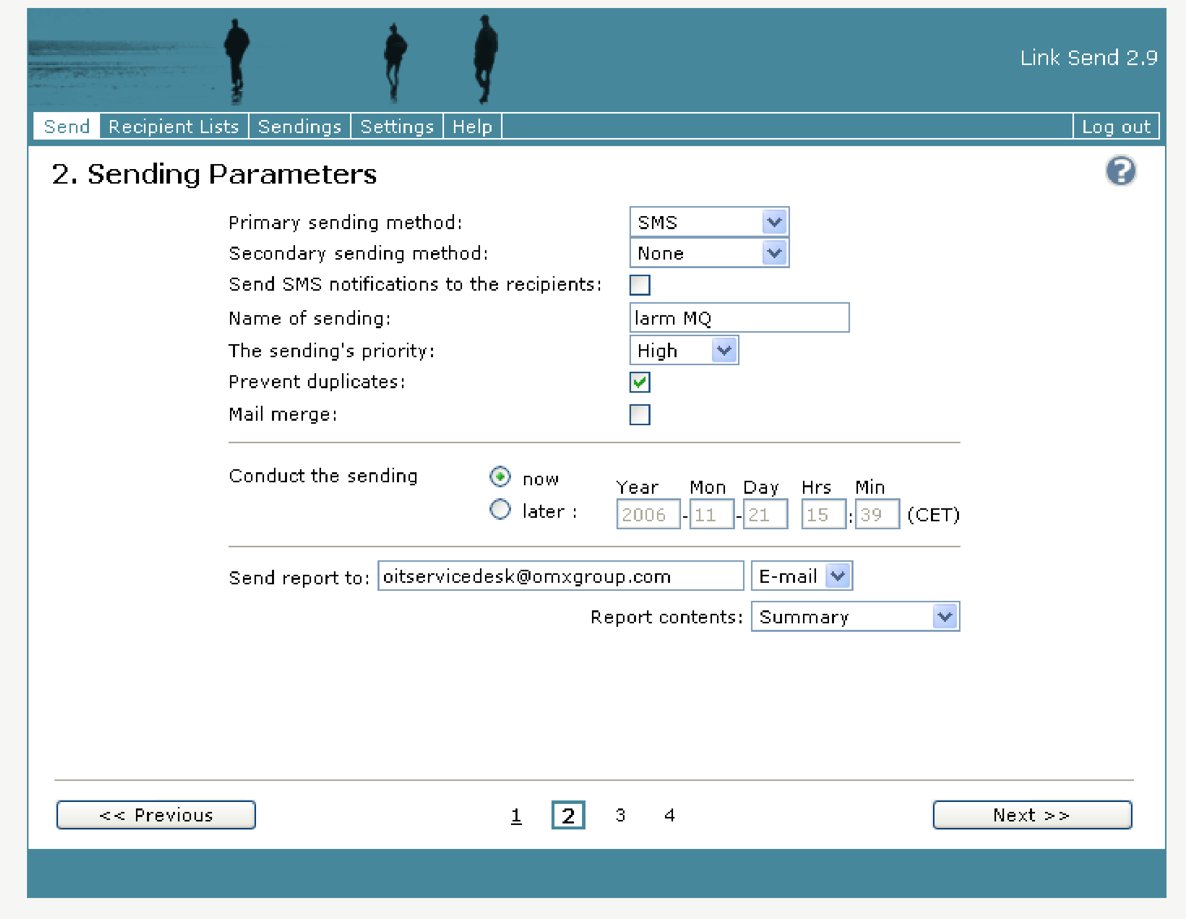
Recipient list:
1OMXmanagement
2nd Line DCS
2SAXESSandCLICK
AMEX (MPS)
ASX (Click)
Borsa Italiana
BoTCC
CDS INTERNAL

Recipients:

The sending will be sent to:
Office Incident

2. Second view is the Sending Parameters

- Primary sending method: SMS
- Secondary sending method: None
- Send SMS notifications to the recipients: NO
- Name of sending: MAIL, VIRUS, NETWORK etc. (subject)
- Priority: High
- Prevent duplicates: YES
- Mail merge: No
- Conduct sending: Now
- Send report to: oitservicedesk@omxgroup.com / Choose Email
- Report contents: Summary
- Choose Next>


Link Send 2.9
Send | Recipient Lists | Sendings | Settings | Help | Log out

2. Sending Parameters

Primary sending method: SMS
Secondary sending method: None
Send SMS notifications to the recipients: □
Name of sending: larm MQ
The sending's priority: High
Prevent duplicates: ☑
Mail merge: □

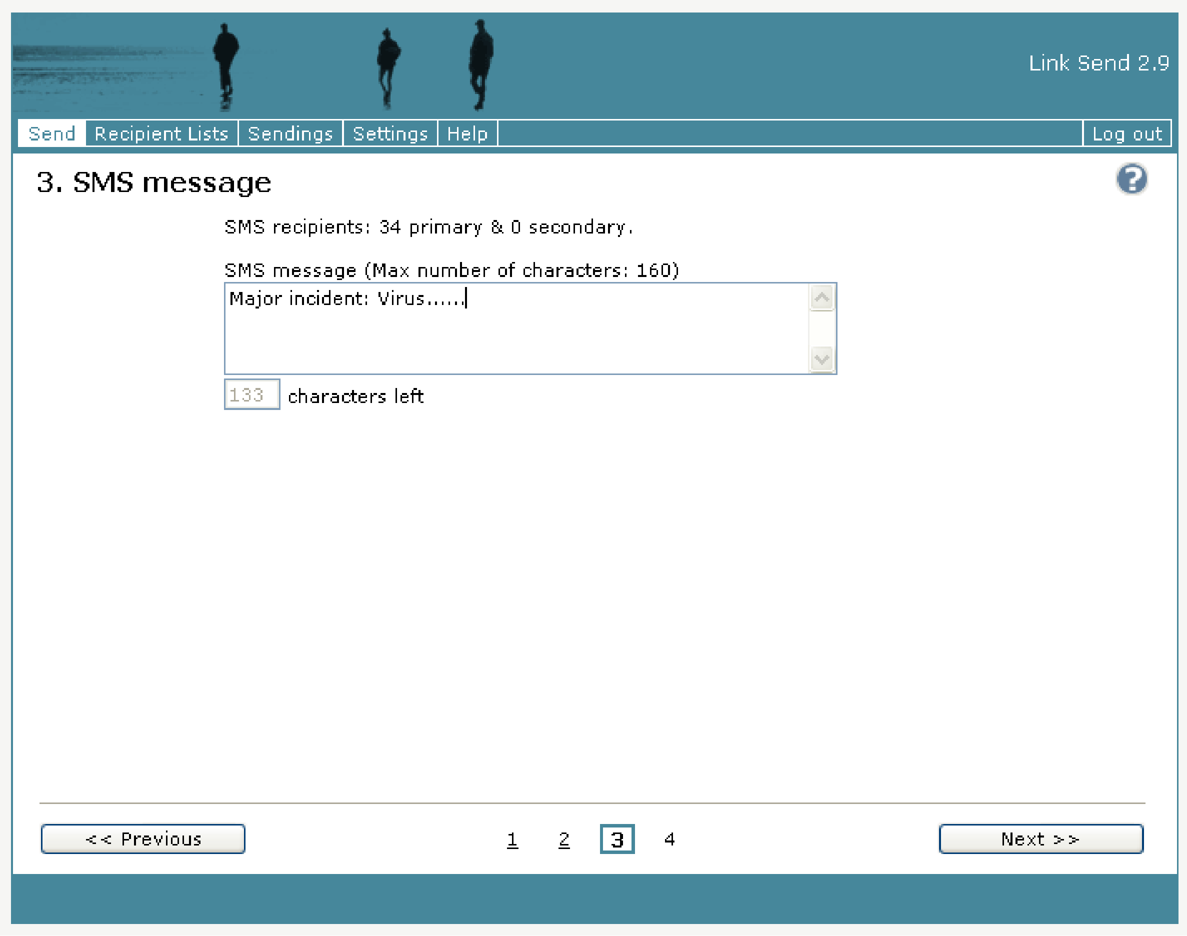
Conduct the sending ● now ○ later : Year 2006 - Mon 11 - Day 21 Hrs 15 : Min 39 (CET)

Send report to: oitservicedesk@omxgroup.com E-mail
Report contents: Summary

<< Previous
1 2 3 4
Next >>

3. Third view is SMS Message

- ➢ SMS Message: Choose message from the Major Incident Procedure
- ➢ Choose Next>



3. SMS message

SMS recipients: 34 primary & 0 secondary.

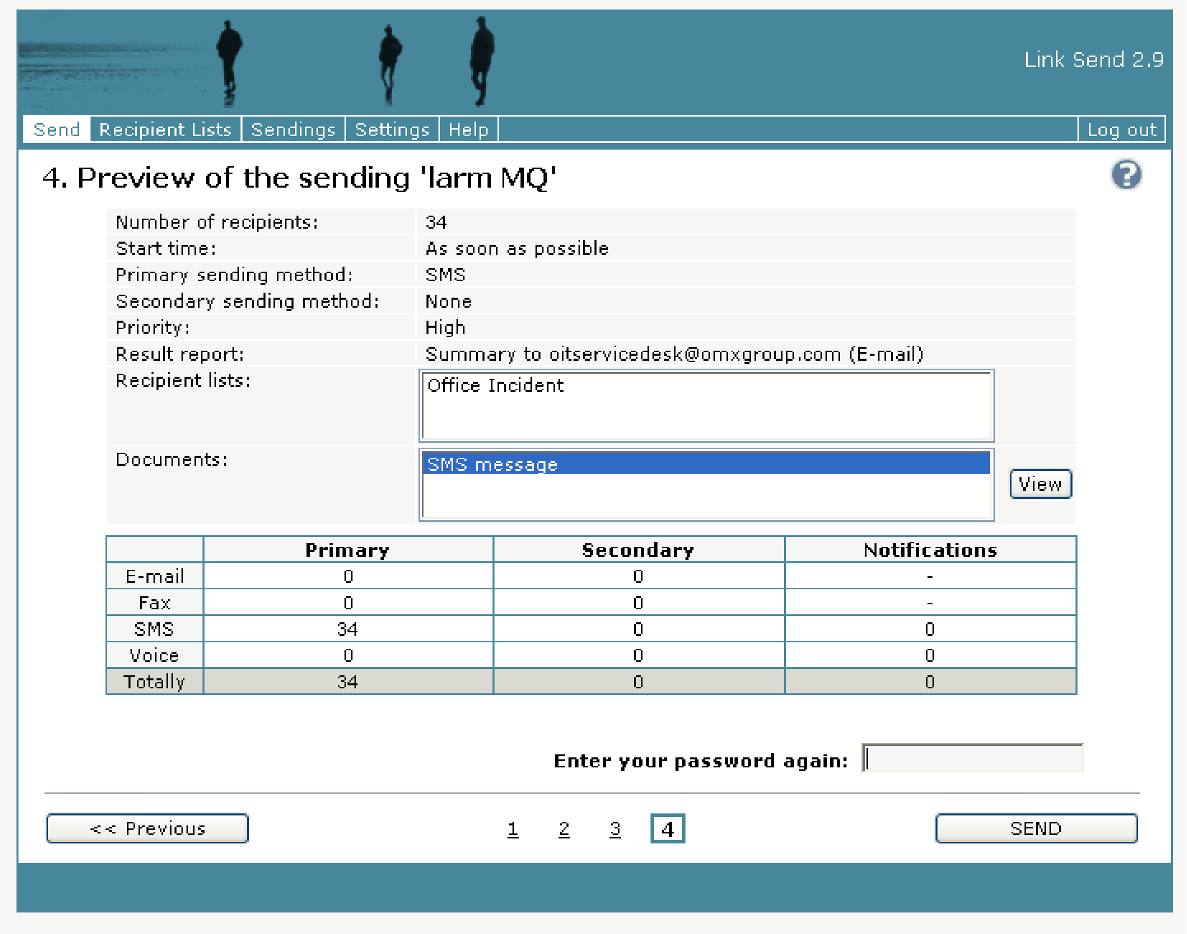
SMS message (Max number of characters: 160)

Major incident: Virus......

133 characters left

4. Fourth view is Preview of the sending "subject for example MAIL"

- ➢ Check that information is correct
- ➢ Enter password
- ➢ Click Send



4. Preview of the sending 'larm MQ'

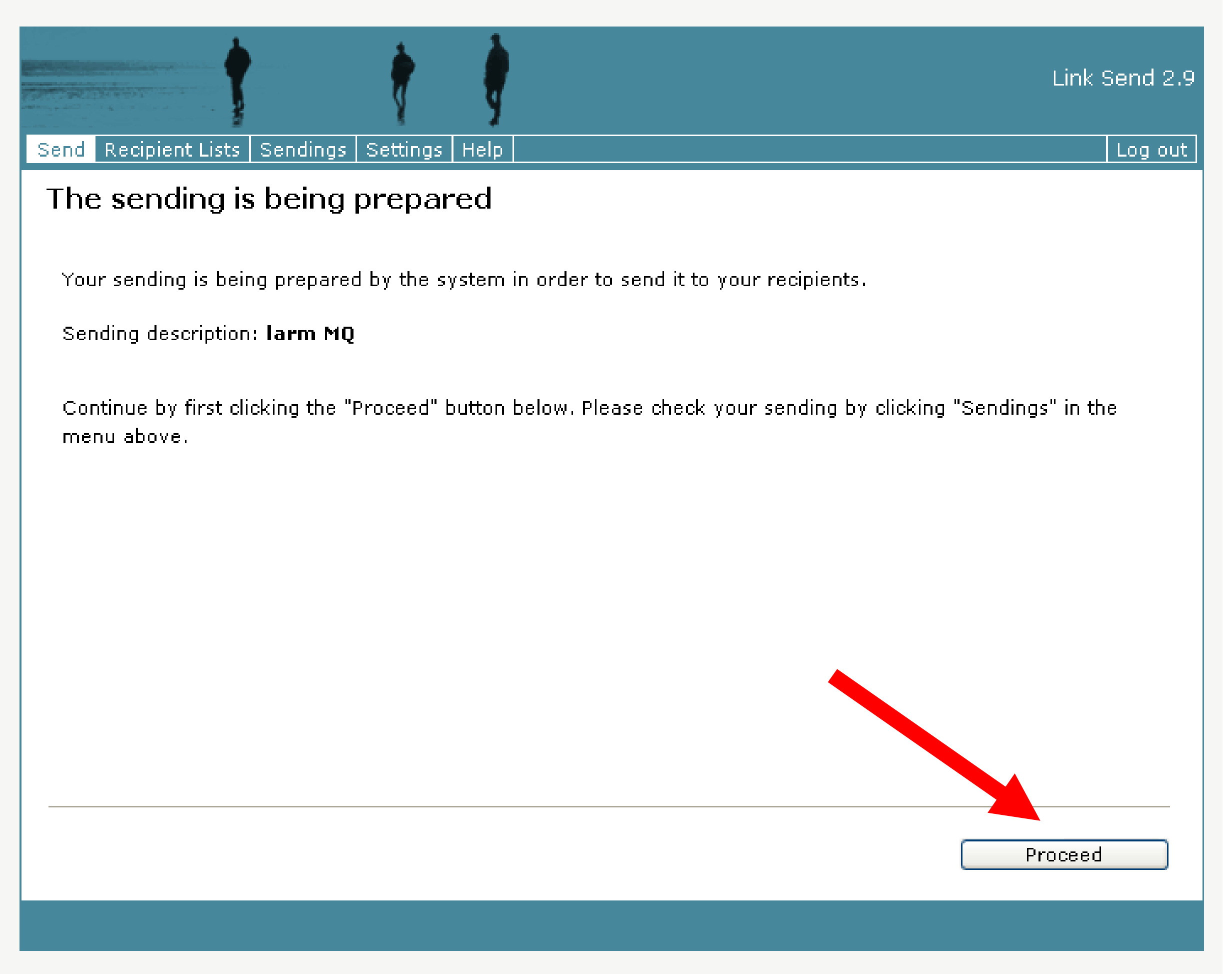
Number of recipients:	34
Start time:	As soon as possible
Primary sending method:	SMS
Secondary sending method:	None
Priority:	High
Result report:	Summary to oitservicedesk@omxgroup.com (E-mail)
Recipient lists:	Office Incident
Documents:	SMS message

	Primary	Secondary	Notifications
E-mail	0	0	-
Fax	0	0	-
SMS	34	0	0
Voice	0	0	0
Totally	34	0	0

Enter your password again:

5. Last view is "The sending is being prepared"

  - Just press Proceed and message will go to recipients



The sending is being prepared

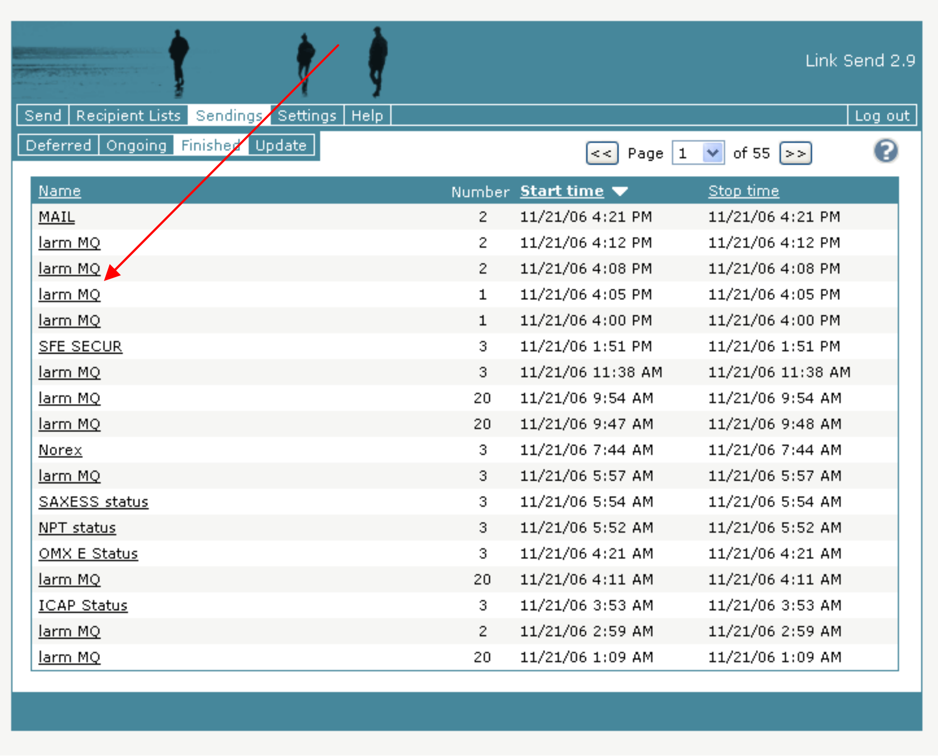
Your sending is being prepared by the system in order to send it to your recipients.

Sending description: **larm MQ**

Continue by first clicking the "Proceed" button below. Please check your sending by clicking "Sendings" in the menu above.

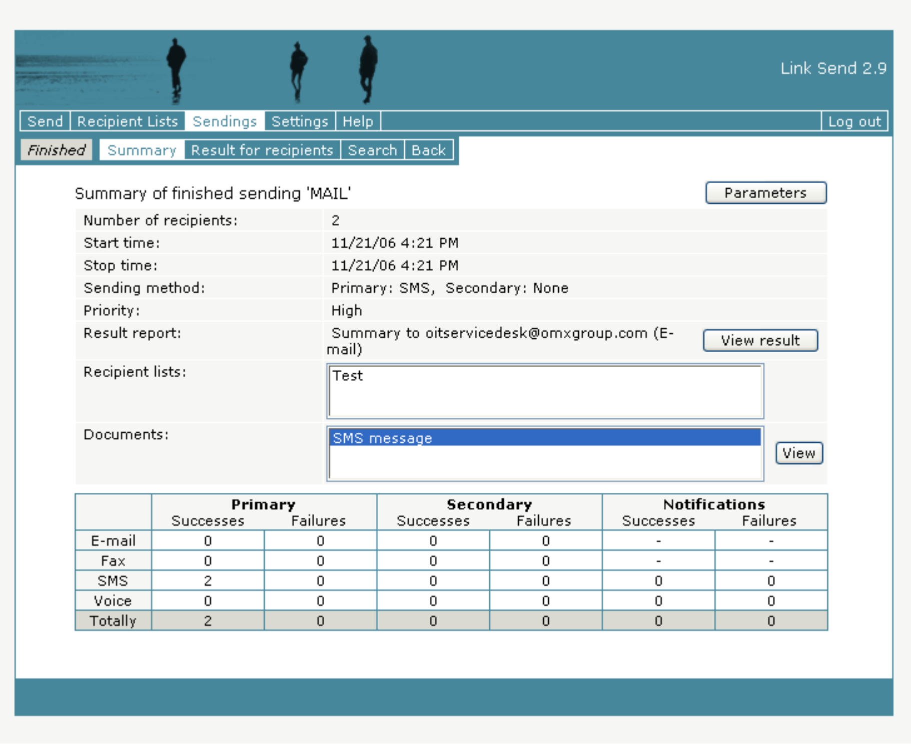
6. After Sending you will receive report by mail, but you can also check sending status

   - Choose Sendings
   - Choose Finished
   - Click “Mail” in name field



Name	Number	Start time	Stop time
MAIL	2	11/21/06 4:21 PM	11/21/06 4:21 PM
larm MQ	2	11/21/06 4:12 PM	11/21/06 4:12 PM
larm MQ	2	11/21/06 4:08 PM	11/21/06 4:08 PM
larm MQ	1	11/21/06 4:05 PM	11/21/06 4:05 PM
larm MQ	1	11/21/06 4:00 PM	11/21/06 4:00 PM
SFE SECUR	3	11/21/06 1:51 PM	11/21/06 1:51 PM
larm MQ	3	11/21/06 11:38 AM	11/21/06 11:38 AM
larm MQ	20	11/21/06 9:54 AM	11/21/06 9:54 AM
larm MQ	20	11/21/06 9:47 AM	11/21/06 9:48 AM
Norex	3	11/21/06 7:44 AM	11/21/06 7:44 AM
larm MQ	3	11/21/06 5:57 AM	11/21/06 5:57 AM
SAXESS status	3	11/21/06 5:54 AM	11/21/06 5:54 AM
NPT status	3	11/21/06 5:52 AM	11/21/06 5:52 AM
OMX E Status	3	11/21/06 4:21 AM	11/21/06 4:21 AM
larm MQ	20	11/21/06 4:11 AM	11/21/06 4:11 AM
ICAP Status	3	11/21/06 3:53 AM	11/21/06 3:53 AM
larm MQ	2	11/21/06 2:59 AM	11/21/06 2:59 AM
larm MQ	20	11/21/06 1:09 AM	11/21/06 1:09 AM

You will get view, where you can check Summary and Results for recipients


Link Send 2.9
Send | Recipient Lists | Sendings | Settings | Help | Log out
Finished | Summary | Result for recipients | Search | Back
Parameters
View result
View

Summary of finished sending 'MAIL'

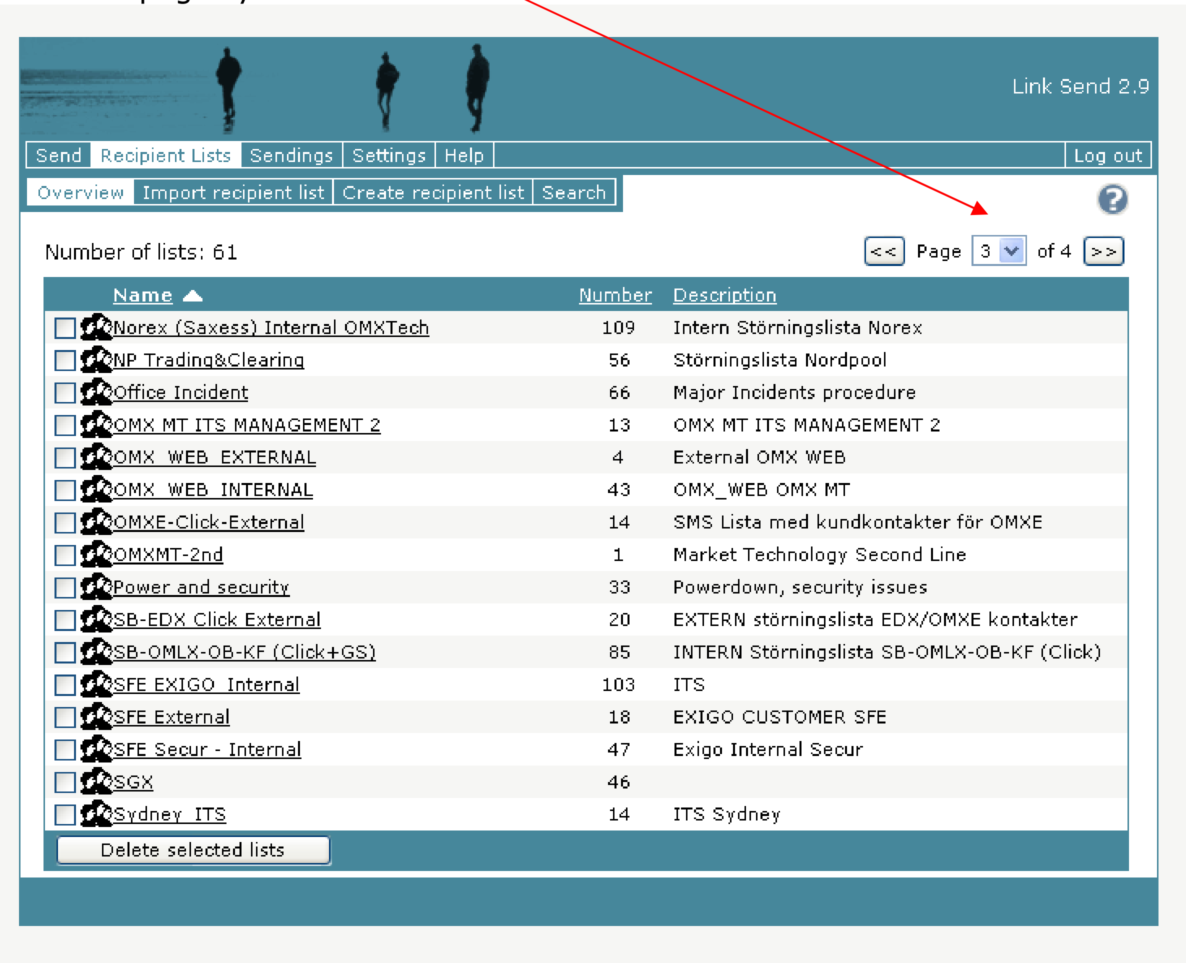
Number of recipients:	2
Start time:	11/21/06 4:21 PM
Stop time:	11/21/06 4:21 PM
Sending method:	Primary: SMS, Secondary: None
Priority:	High
Result report:	Summary to oitservicedesk@omxgroup.com (E-mail)
Recipient lists:	Test
Documents:	SMS message

	Primary		Secondary		Notifications	
	Successes	Failures	Successes	Failures	Successes	Failures
E-mail	0	0	0	0	-	-
Fax	0	0	0	0	-	-
SMS	2	0	0	0	0	0
Voice	0	0	0	0	0	0
Totally	2	0	0	0	0	0

3. Adding recipients to SMS list

1. Select Recipients List from the main menu
2. Select the list you want to modify by clicking it

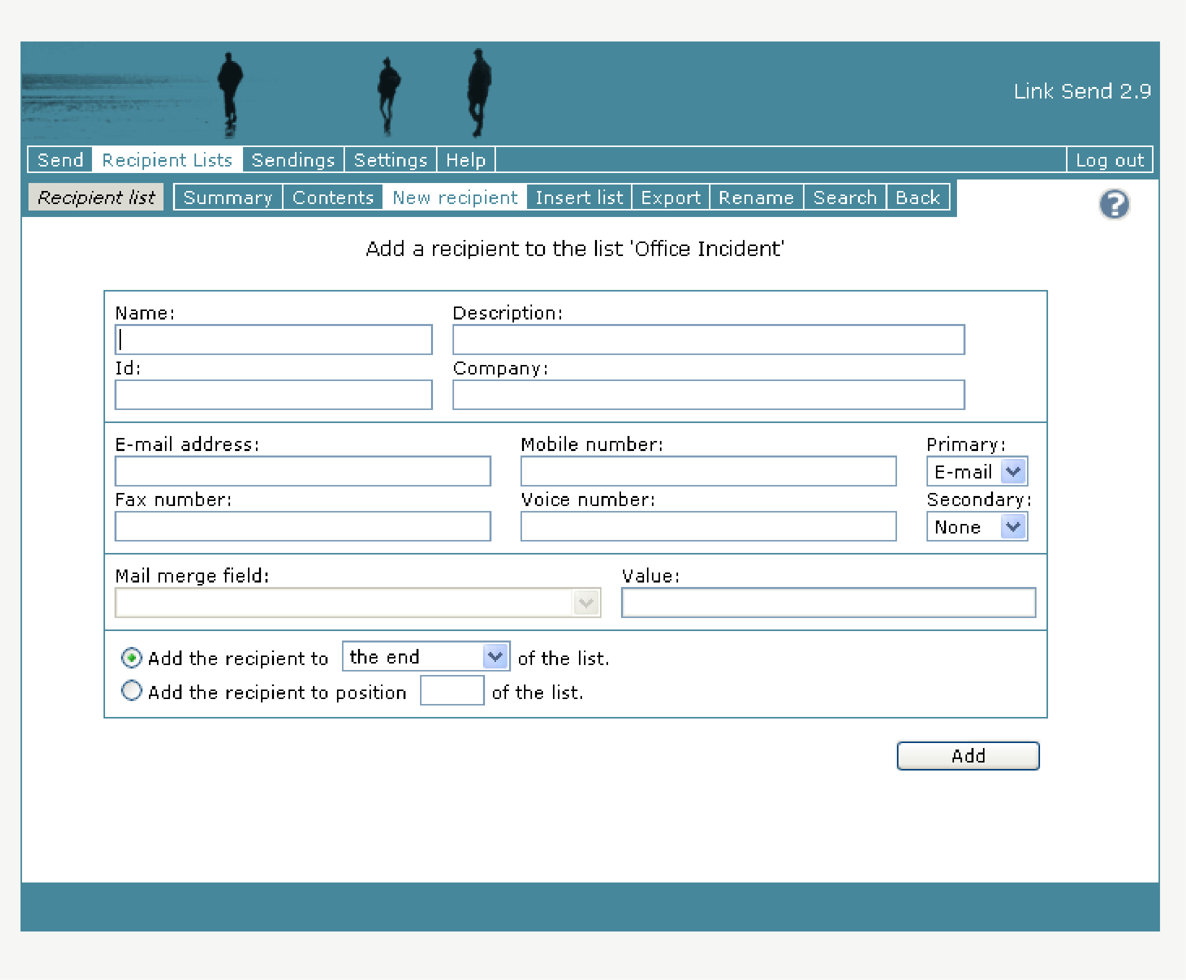
Different pages you can choose from here



Number of lists: 61

	Name ▲	Number	Description
□	Norex (Saxess) Internal OMXTech	109	Intern Störningslista Norex
□	NP Trading&Clearing	56	Störningslista Nordpool
□	Office Incident	66	Major Incidents procedure
□	OMX MT ITS MANAGEMENT 2	13	OMX MT ITS MANAGEMENT 2
□	OMX_WEB_EXTERNAL	4	External OMX WEB
□	OMX_WEB_INTERNAL	43	OMX_WEB OMX MT
□	OMXE-Click-External	14	SMS Lista med kundkontakter för OMXE
□	OMXMT-2nd	1	Market Technology Second Line
□	Power and security	33	Powerdown, security issues
□	SB-EDX Click External	20	EXTERN störningslista EDX/OMXE kontakter
□	SB-OMLX-OB-KF (Click+GS)	85	INTERN Störningslista SB-OMLX-OB-KF (Click)
□	SFE EXIGO_Internal	103	ITS
□	SFE External	18	EXIGO CUSTOMER SFE
□	SFE Secur - Internal	47	Exigo Internal Secur
□	SGX	46	
□	Sydney_ITS	14	ITS Sydney

3. Next you will get Contents view from the list
4. Select New Recipient



Add a recipient to the list 'Office Incident'

Name:

Description:

Id:

Company:

E-mail address:

Mobile number:

Primary: E-mail

Fax number:

Voice number:

Secondary: None

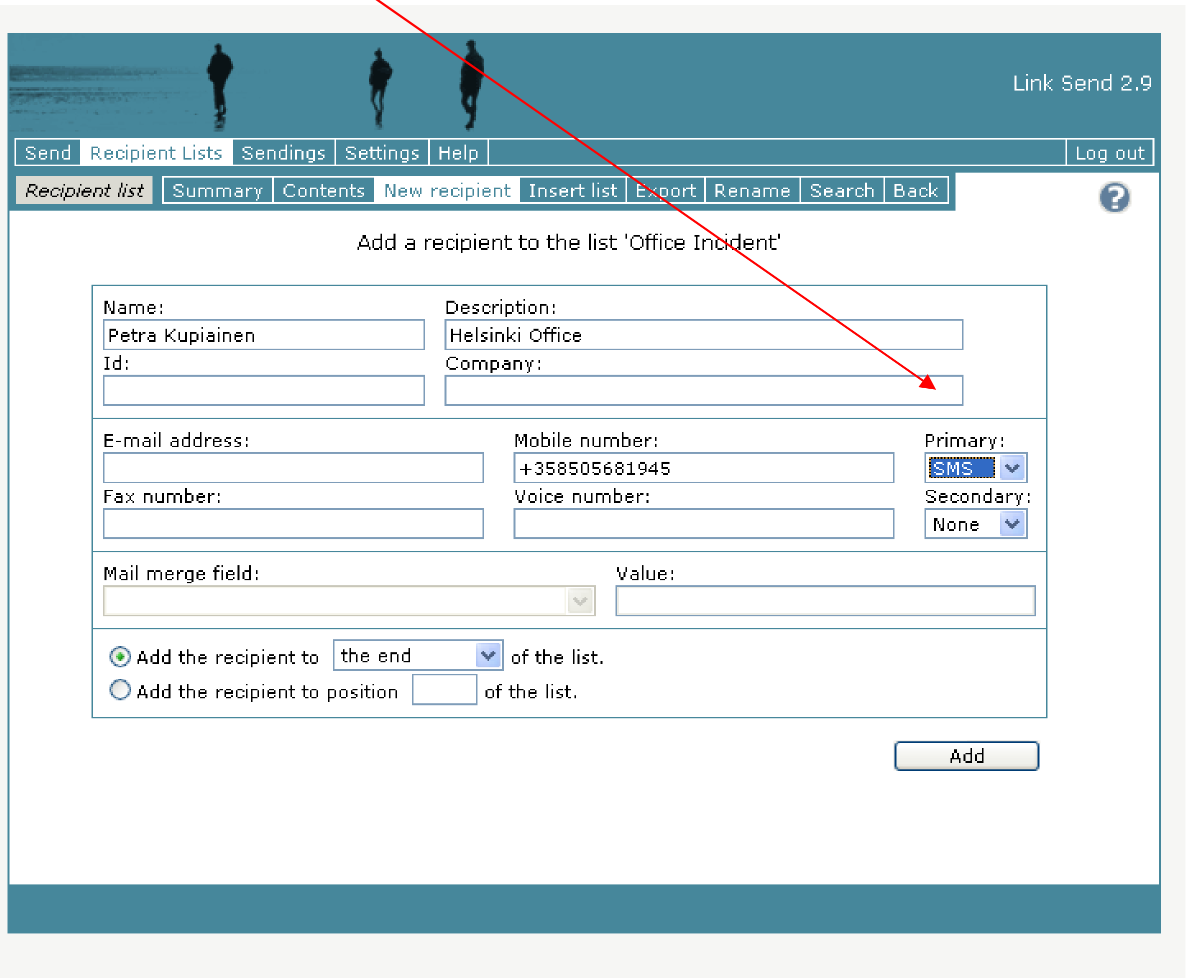
Mail merge field:

Value:

● Add the recipient to the end of the list.

○ Add the recipient to position of the list.

5. Add recipient name, mobile number and description (location, title)
6. Choose SMS
7. Click Add, you will return to contents menu



Add a recipient to the list 'Office Incident'

Name: Petra Kupiainen

Description: Helsinki Office

Id:

Company:

E-mail address:

Mobile number: +358505681945

Primary: SMS

Fax number:

Voice number:

Secondary: None

Mail merge field:

Value:

● Add the recipient to the end of the list.

○ Add the recipient to position of the list.