Well Structured, Secure and Efficient Alert Notifications

Merete Ask

Master's Thesis
Master of Science in Information Security Management
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2014

Abstract

This thesis assembles and presents a set of organization generic, but alert notification specific recommendations. Recommendations any arbitrary organization may consider to establish and continuously improve well structured, secure and efficient alert notifications to relevant stakeholders.

Alert notifications are only vaguely covered in traditional, generic and holistic change management, incident response and business recovery processes. Incident response, business (emergency) recovery, business contingency and crisis management is covered in general by several "best practices", standards and recommendations. Relevant fragments can be drawn from some, but none of them provide detailed, specific recommendations as to how alert notifications can be used as a business beneficiary communication tool.

Several organizations are required by law to alert notify authorities in certain situations and have developed their own solutions for the purpose. Solutions typically later improved and expanded, based on organizational experience gained, end user demands, expectations and requirements. Societal, corporate and governmental dependency of telecom and data services has been and is increasing. Increased dependency leads to increased expectations and demands towards service providers in general. The current general expectation is that telecom and data services are resilient, stable and available for use, at all times, everywhere. No matter how resilient, robust and secure these services are designed to be though, incidents will happen and they do. When they do, service providers are expected to handle them efficiently, professionally and in a predictable manner (including an expectation to keep relevant stakeholders informed). Alert notification is a simple communication tool that can support the service provider, keeping relevant stakeholders informed about the progress in a professional manner. Informed stakeholders are enabled to "workaround" occurred incidents and maintain "business as usual" more efficiently. Alert notifications also provide a common situational awareness amongst receivers, relevant to stakeholders expected to take more active action should the situation escalate further (e.g. members of internal crisis management team) and/or enable stakeholders to make more correct decisions (e.g. how long the undesirable effect of the situation can be endured before end user has to initiate own internal business recovery and/or contingency processes).

The current and quite mature alert notification solution[1] of the thesis topic provider, Telenor, is used as a case basis for the thesis. The current limited but publicly available relevant literature, combined with knowledge and experience collected from Telenor internal alert notification stakeholders and external expert contributors, is utilized by the master candidate, to provide a set of generic but alert notification specific recommendations, through this master thesis. The thesis is aimed to provide any arbitrary organization and stakeholders of the topic with thorough understanding of the topic. The thesis provided organization generic, alert notification specific set of recommendations, provides a basis for any arbitrary organization to establish and continuously improve well structured, secure and efficient alert notifications.

[1] Term "solution" here refers to the current complete and combined set of systems, procedures and resources utilized by Telenor for alert notification purposes.

Preface

The original Telenor provided two line topic description provided the opportunity to approach the topic broadly with different perspectives. This represented an interesting challenge to the master candidate, with the ability to approach the topic quite freely and (in close dialog with Telenor) start to define and scope the topic, sculpting it into something that could be a suitable and relevant master thesis of current interest.

The journey through to the completion of this master thesis would have been much more troublesome, had it not been for the different and good support from the master candidate's professional and social network. I want to thank Telenor Operations for the provision of an interesting topic, their consistent engagement and enthusiastic support of the candidate's work on the thesis. Telenor Operations gave a warm welcome and had a very open minded approach towards the candidate. Combined with their lack of fear to challenge the candidate's opinions and state their own that provided a good environment for discussions making this thesis better than it would have been without them.

I would especially like to thank my external supervisor, Martin Onstad (Telenor), for his efforts in getting a hold of relevant alert notification stakeholders in Telenor and his constant challenges to keep the thesis operationally oriented, usable and of current interest. At the same time I would like to thank my GUC internal supervisor, José Gonzalez, for keeping an (at times) very operationally oriented candidate within a certain level of scientifically acceptable boundaries. His constructive scientifically oriented feedback provided this thesis (all though quite scientifically challenging) with a stronger scientific standing than it would have had without his feedback. I would also like to thank experts within the field, for openly sharing their knowledge, thoughts and perspectives, providing me with valuable "in the field experience" based feedback on alert notifications.

Finally, I would like to thank friends and family for their joint support, providing me with much needed breaks during the work on this thesis, e.g. serving me dinner at times when cooking was "far off" my agenda and their contribution to take my mind off the thesis for some time putting it to work other "mind occupying activities" such as quiz, card-playing and shooting pool.

Thanks to you all, it was much appreciated!

Gjøvik, May 2014

Merete Ask

Contents

List of figures

List of tables

1. Introduction

This document constitutes the master thesis report, prepared and delivered by Merete Ask at Gjøvik University College (GUC) 01-07-2014. The topic provided by Telenor is prepared and delivered by the master candidate (Merete Ask), supervised by Telenor (Martin Onstad) and GUC (José Gonzalez).

1.1. Thesis structure and target audience

This thesis has been structured to comply with relevant scientific requirements, i.e.:

- In addition to this structure description, this ***section 1*** introduces the thesis topic, its background, scope, limitations and illustrates it in context of a broader perspective. It also includes overview of different terms and abbreviations utilized in the thesis.

- ***Section 2*** presents the main problem statement and corresponding research questions defined for this thesis.

- ***Section 3*** describes the methodology chosen for this thesis and it was applied.

- ***Section 4*** presents the complete result of this thesis in terms of a resolution to the main problem statement and its corresponding research questions.

- ***Section 5*** discusses the utilized methodology and its corresponding results.

- ***Section 6*** provides the thesis conclusion and suggested future work.

- ***Section 7*** provides the bibliography listing all literature referred to from this thesis report.

Information added for additional insight, not necessarily directly relevant to the main content of the thesis (as outlined above) has been included in appendixes as found relevant.

The thesis structure, content and formulations are aimed to suit its target audience, i.e. fellow students and people working in the industry with the interest to gain more insight into the topic of alert notification. Its content is further aimed to be adequate enough[2] for any arbitrary organization to utilize, regardless of topic specific maturity as an aid in any effort to establish and/or improve alert notification.

1.2. Background, scope and limitations

Few documents found during the research for and work on this thesis mention alert notifications more often than the report from the 22-07 commission of inquiry [1, chapter 8, p.153], which define alert notification as follows:

> *"A main purpose of alert notifications is that the notification should lead to the receiver performing an action. One type of action may be as simple as the receiver's consideration if any measures should be initiated."*

This master thesis takes a closer look at alert notifications, from the perspective that alert notifications are messages sent to alert/inform different relevant stakeholders about planned maintenance activities or incidents deemed severe enough when they

[2] *I.e. thesis content supported by thesis referenced literature if required.*

occur to require alert notification. Here, alert notifications are messages issued by those supervising planned maintenance (e.g. change managers) and those supervising event and incident response teams (e.g. incident response managers) to keep relevant stakeholders informed about the situation[3], as further detailed in section 2 of this report. Alert notifications in the form of messages are, as such, a communication tool that can be added to the traditional change management (CM), incident response (IR) and business recovery (BR) processes of an arbitrary organization.

To put incident alert notification into context it is useful to look at it from the traditional IR and BR processes point of view. The illustration below provides a traditional overview of such processes [2, Chapter 1, Page 27, Figure 1-5 Contingency planning timeline].

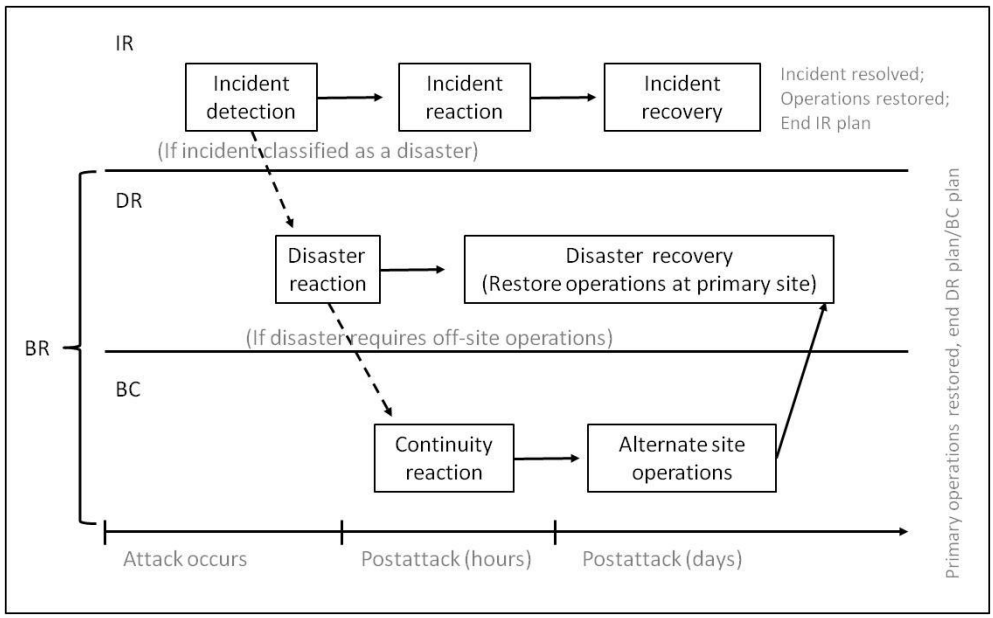

Figure 1: Traditional IR and BR processes

The above illustration is focused on security incident handling (i.e. use of term "attack" in figure), but the processes and their outlined interaction (as illustrated) is incident type generic. The figure shows a high level view of the IR and BR processes relevant to an arbitrary organization in relation to events and incidents, their detection and subsequent handling. As the top of the figure shows, some events are severe enough to be classified as incidents which require incident reaction and recovery. If the detected incident is found severe enough to be classified as a disaster, one or more processes may be required to be initiated. I.e. the disaster recovery (DR) process, with, depending on occurred incident type and severity, the parallel initiation of the business continuity (BC) process. Together, the DR and BC processes constitute the business recovery process (BR). The IR, DR and BC processes are overlapping and parallel at a certain extent, when incidents severe enough initiate one or more of them. The severity of the incident occurred and the risk tolerance level of the organization determines how fast one or more of the

[3] *Note that different commercial off the shelf (COTS) solutions exist, which include functionality to provide alert notifications. Evaluation and analysis of such tools are not part of this thesis. In this thesis context, alert notification should also not be confused with system generated events, warnings, alert or failures (e.g. Windows Even Log, application change logs or similar). As important as such may be to those monitoring a system to maintain required level of quality of service (QoS), this is not considered alert notifications in the context of this thesis.*

processes have to be triggered and handled in parallel. Risk tolerance level and corresponding time aspects of escalation to initiate processes are individual to the organization and the threat the occurred incident pose towards it.

Figure 2 below is similar to Figure 1 above, with some simple additions made by the master candidate, to provide an initial illustration of incident alert notifications, in relation to the traditional IR and BR processes.

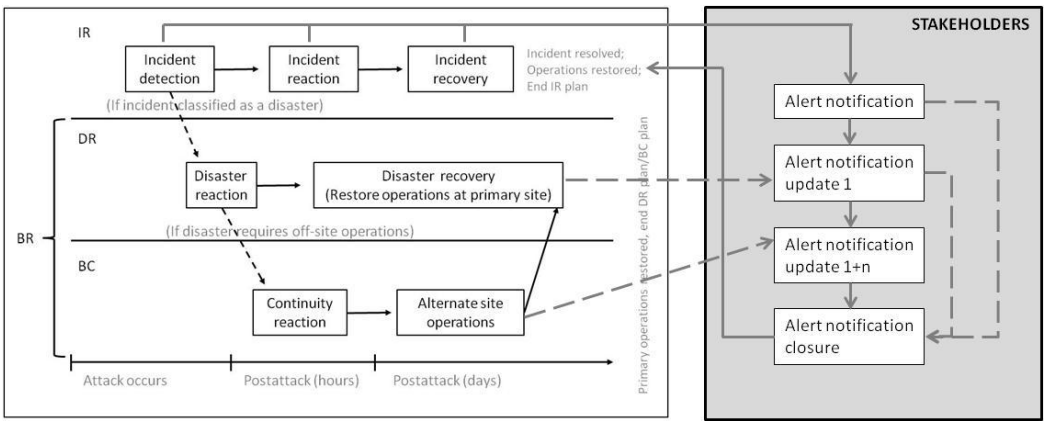

Figure 2: Traditional IR and BR processes with alert notification addition

At some point in an incident response process it may become clear (as illustrated above) that the incident is severe enough to require incident alert notification sent to relevant stakeholders. Alert notification is sent to defined stakeholders and they are kept updated on progress through a number of subsequent alert notification updates until normal operation has been restored and alert notification is closed[4].

In addition, alert notifications can be used to alert/inform relevant stakeholders about planned maintenance activities to be performed on the monitored infrastructure/networks. In this case, the alert notification would be an addition to the organizations generic change management (CM) process. The CM process would typically include the task to send alert notification to stakeholders, when the risk assessment of the planned maintenance activity shows a risk level high enough[5] to require an alert notification sent. In its simplest form, this would typically be one (or more) message(s) to inform relevant stakeholders about the maintenance activity planned executed and when it is planned executed, so that stakeholders know about it in advance and may plan own actions accordingly.

Based on the above, the scope of this thesis is to take a closer look at two types of alert notifications, maintenance and incident alert notifications, as described below:

[4] Please note that alert notifications closure should not be confused with incident resolution in terms of incident closure. Alert notifications are typically only sent until normal operation has been restored. Normal operation may be restored by the means of a workaround or mitigation which restores normal operation by reducing the consequence of a failure, i.e. root cause of failure may not have been corrected yet. With workaround/mitigation in place, incident severity may be reduced to a level no longer requiring alert notifications, but the incident is not resolved and closed until the root cause resolution has been implemented. This will also be looked at in more detail later in this report, only included here for initial informational purposes.

5 The term "high enough" here means high enough in terms of the planned activity's ability to adversely affect quality of the infrastructure and/or services when performed.

- ***Maintenance alert notification;*** Proactive alert sent to inform relevant stakeholders about planned maintenance activities which could affect infrastructure functionality or quality of service adversely when executed. Typical element relevant to add to the organization's existing change management (CM) process.

- ***Incident alert notification;*** Reactive alert sent to inform relevant stakeholders about an occurred incident, followed by update alerts to keep relevant stakeholders informed about the progression in relation to incident response. Typical element relevant to add to the organization's existing incident response (IR)/business recovery (BR) processes.

Looking at the current status and trends, the general public is getting more and more familiar with the concept of alert notifications (whether they are aware of it or not). Several providers of different services (e.g. organization internal and/or external IT and service providers, online banking service providers etc.) now provide alert notifications. In its simplest form it is typically provided as an informational note on a website (for instance in relation to a service logon site such as online banking) and in this case, both maintenance (M) and incident (I) alert notifications may be seen at times, e.g.:

- ***M:*** *"Please note that the service may be unavailable or unstable from <date and time> to <date and time> due to planned maintenance activities being performed. We apologize for any inconvenience this may oppose to our users."*

- ***I:*** *"Please note that we are currently working to resolve a detected instability with the service. We apologize for any inconvenience this may oppose to our users."*

The above examples are not too different from typical information services provided by the transport sector where the provider may have billboards and/or online services where passengers can receive information about expected transport arrivals, delays etc. Many people also receive informational notes via sms and/or e-mails from other service providers regarding planned maintenance or "known issues being worked on within their area" etc. These are typically services provided by suppliers of energy (power), television, Internet and in some cases also municipality provided services (e.g. scavenge, recycling etc.).

Alert notifications with the purpose to be posted for the general public and be visible to a broad audience, most often are quite generic in wording including little detailed information (e.g. regarding actual cause and effect). Still, with the public becoming increasingly familiar with being kept informed, that contributes to the generic, steadily increasing expectation and demand to be kept informed within the general public.

Providers of critical infrastructure (e.g. telecom and data services) have to adhere to different requirements governed by law to provide alert notifications to the authorities in certain situations. With experience, however, the aspect of alert notification is most often utilized broader than the minimum law governed requirements to alert authorities. Alert notification, when done well, can support communication, establishment and maintenance of common situational awareness for efficient coordination and resolution of unwanted situations in (and across) critical complex infrastructures and environments. Not limited to telecom and data services, but for organizations in general, including other complex infrastructures and environments such as corporate banking, transport, power, oil and gas etc. Experienced providers, most often do (or have the ability to) provide more extensive

alert notification services based on requirements defined in Service Level Agreements (SLA), with corresponding Non Disclosure Agreements (NDA) allowing for the provision of more detailed information. Most often signed between the provider and end users/organizations with a high level of dependency towards the service provided. Often recognized by the fact that available windows for planned maintenance activities are few and strictly defined, and any event may escalate fast in terms of criticality should it turn into an incident with adverse effects. In such environments, the incident handling process may also be quite complex, since it may require several stakeholders with different responsibilities to be included actively to efficiently resolve the situation and get back to normal operation (or at least "for now acceptable" operation).

The thesis topic provider, Telenor, own and is responsible to maintain the complete Norwegian Telenor operational infrastructure of telecom and data services. Telenor handles approximately 1.5 million events on a daily basis. Efficient event handling requires efficient system and process support in event detection, reporting, root cause identification, consequence analysis and resolution. Most received events are handled and resolved efficiently as part of usual round-the-clock (24/7/365) operation. Events which turn into incidents classified critical enough are more closely monitored by operation managers also responsible to provide corresponding incident alert notifications to relevant stakeholders. Telenor also issues proactive maintenance alert notifications to inform relevant stakeholders of planned maintenance work on the operational infrastructure and services. The main purpose of Telenor alert notifications is to provide relevant information to relevant stakeholders efficiently, enabling them to maintain "fact based business as usual" and establish common situational awareness, should further actions require their cooperation.

Telenor has had a solution to comply with law governed alert notification requirements towards the authorities for several decades. In 2005, Telenor initiated a large improvement program for its operation department, focused on business importance of efficient operation management and alert notification. As part of this, operational management became responsible to alert notify (in a more broad and business focused way than before) and the currently used alert notification solution was established. Through continuous improvement and focus on alert notification as a business beneficiary tool the latest decade, Telenor has obtained competence, experience and maturity in relation to the topic of alert notifications. One experience is, however, that there is a lack of alert notification specific recommendations published (e.g. detailed "best practices"/standards), i.e. how to establish and maintain good solutions for it. Although relevant elements can be found and utilized on the basis of different literature, "best practices" and standards, little is specific as to how, what, when and why one should alert notify. This lack of specific, generic recommendations prompted Telenor to provide alert notification as a topic and is the main rationale behind this thesis. This thesis utilizes Telenor, as an experienced and mature case basis, combined with available relevant, publicly available literature[6] and experience shared by relevant third party competent sources. This, further combined with the master candidate's twelve years work experience with information security services, functional system and software safety, and the competence gained from the GUC information security master studies, constitutes the complete knowledge basis behind this thesis, aimed to present an organization generic, alert notification specific set of recommendations.

6 The term "literature" here includes topic relevant publicly available literature in general, e.g. books, "best practices", standards, recommendations etc.

1.3. Terms and abbreviations

The list below summarizes and shortly describes different terms and abbreviations used in this master thesis report.

Term	Description
APT	Advanced Persistent Threat
Alert notification	Messages sent to alert/notify/inform different relevant stakeholders about planned maintenance activities or events that turn into incidents severe enough to require notification.
ATC	Air Traffic Communication
ATM	Air Traffic Management
BC	Business Continuity
BR	Business Recovery
CERT	Computer Emergency Response Team
CM	Change Management
CPDLC	Controller Pilot Data Link Communication
DR	Disaster Recovery
eTOM	Enhanced Telecom Operations Map
Event	An occurred situation that could have the potential to escalate into an incident.
External alert notification	Alert notification sent to inform/notify/alert organization external stakeholders.
GUC	Gjøvik University College
Internal alert notification	Alert notification sent to inform/notify/alert organization internal stakeholders. Note that depending of the organization this may include stakeholders "external" to the organization, made "internal" through contracts, e.g. contractors responsible to respond to incidents on behalf of the organization (i.e. the incident owner).
Incident	An occurred situation deemed severe enough to be classified as an incident requiring corresponding incident response procedures to be initiated.
Incident alert notification	Reactive alert notification sent to inform relevant stakeholders about an occurred incident, followed by update alerts to keep relevant stakeholders informed about the progression in relation to incident response. Typical element relevant to add to the organization's existing incident response (IR)/business recovery (BR) processes.
IR	Incident Recovery
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LEAN	Lean manufacturing/Lean enterprise/Lean production or simply "LEAN"
Maintenance alert notification	Proactive alert notification sent to inform relevant stakeholders about planned maintenance activities which could affect infrastructure functionality or quality of service adversely when executed. Typical element relevant to add to the organization's existing change management (CM) process.
NPTA	Norwegian Post and Telecommunications Authority
PS	Problem Statement
RQ	Research Question
SMS/sms	Short Message Service
QoS	Quality of Service

Table 1: Terms and abbreviations

2. Problem statement and research questions

This section state the defined main problem statement (PS) to be resolved by this thesis and the corresponding challenges justifying its definition. This section also shows the PS broken down into a set of research questions (RQ) relevant to resolve the main PS. The following thesis main PS was defined in close dialog with Telenor as the thesis topic provider:

- ***PS:*** Is it possible to define a set of alert notification specific recommendations that any arbitrary organization can utilize to establish and continuously improve a well structured, secure and efficient alert notification solution?

With Telenor as an experienced and mature case basis for the thesis, Telenor early mentioned one specific challenge they encountered in their work on this topic. Namely that alert notification elements relevant to utilize could be found in different literature, "best practices" and standards, but little of this was specific as to how, what, when and why one would choose to alert notify. Preliminary research done by the master candidate in the master thesis pre-planning phases to determine the applicability of the Telenor provided topic [3], confirmed the challenge outlined by Telenor and was therefore used to define the main problem statement of this thesis.

All suppliers of telecom and data services in Norway are required by the Norwegian Post and Telecommunications Authority (NPTA) to provide them with alert notifications, should they detect incidents which may or already have resulted in reduced availability of e-communication services, as warranted by the Ecom Regulation[7] [4]. Other industries providing critical infrastructure and services (e.g. energy, transport, oil and gas etc.) are governed by similar laws to alert notify authorities in given situations. Being Norway's biggest supplier of telecom and data services, Telenor also holds the ownership and responsibility to maintain the core critical telecom infrastructure of Norway. This puts a special pressure upon Telenor to maintain high quality services. Not only from authorities, but customers[8] in general with a constantly increasing expectation and demand that services they become steadily more dependent upon are professionally monitored and controlled by the provider. This includes expectations and demands that the provider behaves predictably when incidents occur, that incidents are handled efficiently and that relevant stakeholders are kept informed.

Due to the lack of publicly available, organization generic, alert notification specific methods/models/sets of recommendations, most current, mature solutions for alert notification are historically based on solutions implemented merely to comply with legal requirements. Over the years such solutions are often expanded and improved based on experience, internal requirements for increased efficiency and increased from end users/customers (e.g. included as requirements in Service Level Agreements). Some also provide alert notification as a payable service end

[7] *The Ecom Regulation is the short name for the Norwegian "Regulations on electronic communications networks and services" which in §8-5 states (translated into English by the report author):*
"Supplier is required to alert the Norwegian Post and Telecommunications Authority about events that may or have reduced the availability of electronic communication services considerably.
The Norwegian Post and Telecommunications Authority can define more detailed alerting procedures"

[8] *As a thesis relevant example it can be mentioned that Telenor has approximately 5.4 million corporate and private customers.*

users/customers can get assigned to. “Made as one goes”, the main challenge with these solutions may be to efficiently keep up with increasing information expectations from end users/customers, adjust efficiently for rapid technological development of infrastructure and services and at the same time maintain the desired level of alert notification quality.

Based on the above and through initial discussions, the following research questions (RQ) were defined, relevant to solve to resolve the main problem statement (PS):

- ***RQ1:*** Find a way to define a generic set of recommendations that can be utilized by an arbitrary organization[9].
- ***RQ2:*** Research, identify and utilize as found relevant, the limited, little alert notification specific, but relevant elements of available literature, “best practices” and standards.[10]
- ***RQ3:*** Collect mature alert notification experience and include it to support limited published relevant material, making the most out of Telenor as a case basis for the thesis.
- ***RQ4:*** As found relevant, research, collect and include recommendations from other experienced third party actors and relevant experience gained from other documented crisis/disaster investigations.
- ***RQ5:*** To cover both the aspect of establishment and improvement, make sure the generic set of recommendations include recommended/suggested ways to measure improvement.

The above research questions (RQ1-5) outlines elements relevant to resolve to resolve the above defined main problem statement (PS) and is the basis of the work performed as part of this thesis and the methodology defined (ref. section 3) to provide the PS resolution requested result, i.e. a set of organization generic, topic specific recommendations.

9 This requires the ability to take the most complex into account without limiting the simpler and, as such, enable tailoring of the generic with any individual organization’s purpose, needs and capabilities.
10 Such information is relevant to ensure anchorage and justification for efforts made in relation to alert notification within an arbitrary organization.

3. Methodology

This section describes the chosen methodology used as a basis to perform the thesis. The section also describes how the methodology was applied to resolve the defined problem statement, corresponding research questions (ref. section 2) and its justification.

3.1. Chosen methodology

Preliminary research done by the master candidate in the master thesis pre-planning phases to determine the applicability of the Telenor provided topic [3], confirmed challenges early stated by Telenor. These challenges can be summarized as follows:

- Although alert notification relevant elements can be found and utilized from different literature, "best practices" and standards, these are most often not specific as to how, what, when and why one should alert notify.
- Several, different suppliers within different industries are required by law to alert notify and have working alert solutions for that purpose, but their extent of structure, security and efficiency are not publicly known and also only limitedly shared amongst suppliers and across industries.
- Due to law governed requirements, alert notification receiving authorities have defined some regulations and guidelines, but these are only based on the information they expect to receive (i.e. represent a least required minimum for organizations required by law to alert notify).

The above summarized results of the preliminary research justified the applicability of the provided topic in general, but also put some implications towards the choice of methodology. It led to the acknowledgement that large parts of this thesis would have to rely quite heavily upon Telenor available knowledge, being a mature and experienced user of alert notifications. That acknowledgement enhanced the importance of utilizing Telenor as a case basis for this thesis.

Telecom and data service providers are, together with different other industries, decreed by law to alert notify authorities when incidents deemed severe enough occur. This implies that most organizations within the industry and across different similar industries have solutions to handle this. The extent of solution structure, security and efficiency is, however, not publicly known in detail. There is no, at least not yet, known established tradition to share actual gained knowledge and experience on the topic, between industries and companies within the industry. For now, there may be competitive good reasons for this, but forward, given the trends of steadily increased dependency, expectancy and requirements towards providers in general, this may change. This current situation did, however, further enhance the acknowledgement of the importance of Telenor as a case basis for this thesis.

Based on the above, the following methodology was chosen to gain the knowledge basis relevant to solve the main problem statement and corresponding research questions defined for the thesis (refer section 2):

- Broad literature[11] search for alert notification relevant elements to utilize

[11] *The term literature here includes books with potential alert notification relevant content, "best practices", standards and results/papers/reports from previously performed similar and/or related research and incident investigation result reports. Collected, utilized and referred to as found relevant throughout this master thesis report in accordance with the listed bibliography presented in this report section 7 listed.*

- Interviews with Telenor key personnel in terms of internal alert notification stakeholders, supported by interviews with third party experts on the topic of alert notification.
- Observation of Telenor Operation Management at work and operation management alert notifications

The chosen methodology for this thesis took a qualitative approach [5, Chapter 6, page 140] with the aim to be descriptive (i.e. reveal the multifaceted nature of alert notifications as a topic) and interpretative (i.e. allow for the researcher to gain insights into alert notifications as a topic), to allow for the master candidate to provide an organization generic but topic specific set of recommendations.

3.2. Methodology applied

The broad literature search was performed by searching through a series of alert notification related topics, to find alert notification relevant elements of content to include in a set of organization generic but topic specific recommendations. The literature search covered topics such as (but not necessarily limited to):

- Information security management
- Incident management, response and recovery
- Business (emergency) response and recovery
- Disaster response and recovery
- Emergency preparedness
- Crisis management and communication
- High reliability organizations
- Investigation results and lessons learnt from occurred major incidents

The figure below illustrates the main activities undertaken in the work to complete this master thesis during the spring of 2014, aimed to resolve the main problem statement and provide a set of alert notification recommendations.

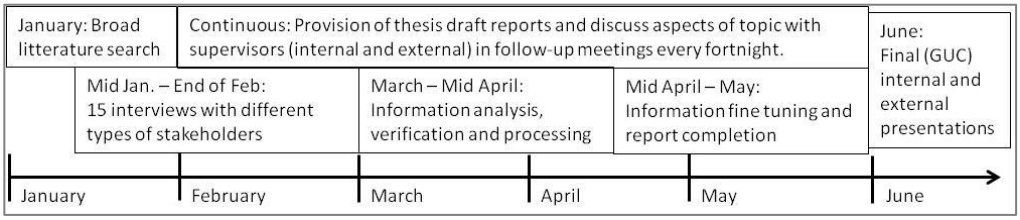

Figure 3: High level timeline overview – 2014 spring semester

The knowledge gained from the broad literature search was supported by empirical data collected though a total of 15 interviews, all conducted during the first third of the thesis project period (as illustrated above). The interviews were conducted by the master candidate interviewing Telenor internal key personnel, i.e. Telenor internal alert notification stakeholders, and relevant third party sources. Interview subjects were chosen by the master candidate in close dialog with the thesis external supervisor (i.e. Telenor). The interview subjects were chosen based on the strategy to provide the candidate with the broadest possible insight into general and Telenor specific aspects of alert notification, aimed to cover the following two main objectives:

- Gain broad and adequate insight into Telenor alert notification to utilize Telenor as a case basis for the thesis.
- Draw relevant elements from interviews that could be reformulated into generic recommendations related to alert notifications (i.e. with specific interest to elements related to “how, when, why and what”).

The interview subjects were Telenor alert notification stakeholders (12) and third party experts (3), all with different perspectives on alert notification as a topic, i.e.:

- Telenor representatives responsible for 7 different parts of the Telenor complex hierarchy of operational infrastructure and services
- Telenor operation manager representatives
- Telenor change manger representatives
- Telenor top level management representatives
- Telenor customer service management representatives
- Telenor customer satisfaction index representatives
- 3rd party representatives with perspectives such as:
    - Telenor internal IT systems management
    - Experienced auditors of IR and BR processes across different industries
    - Representatives establishing alert notification for other organizations

The interviewer allowed for the interview subjects to quite freely approach the alert notification topic based on their own relation to it and, as such, the interviews were quite open-ended. Based on the interview subject's approach, the interviewer utilized different semi-structured follow up questions [5, Chapter 6, page 154, "Interviews"]. The semi-structured follow up questions mainly related to get the interview subjects perspectives related to what they (from their perspective) thought was the main importance in terms of alert notifications, the main challenges and the main relevant aspects to improve. This interviewing method provided flexibility in that the interviewer gained relevant information not necessarily asked for, though with a certain disadvantage that the results would not be directly comparable given the different perspectives and approaches of the interview subjects. All meetings were recorded in minutes of meeting by the interviewer. The actual minutes are not revealed in detail in this thesis, since they include personal opinions, business internal and confidential information that would prevent for this thesis to be published. Instead, the candidate has utilized gained generic knowledge from interviews to provide a set of generic recommendations (i.e. the result as presented in this thesis section 4).

Gained knowledge from literature search and interviews was supported by additional information and clarification provided by the external supervisor (Telenor) upon direct questions asked by the candidate. A group discussion of (at the time) key findings of the thesis work in a Telenor operation managers meeting, also provided interesting views and perspectives relevant to different aspects of the thesis. Additional support and insight during the five months work on the thesis, was gained by the fact that the candidate had access to office space in the Telenor Operations department. This enabled the candidate to work close to and observe a thesis relevant environment. Throughout the course of the thesis, the candidate also received Telenor Operation Management alert notifications for observational purposes. These observation opportunities, generated questions that led to several different, topic relevant and interesting discussions between the master candidate and the thesis external supervisor (Telenor) during the course of the thesis completion.

Refer this thesis section 5 for a more detailed discussion about the chosen methodology and its appliance to resolve the main problem statement. In addition, Appendix 1 of this thesis provides a summarized overview of the correspondence between the thesis results (ref. section 4) and how these contribute to resolve RQs and PS (ref. section 2) through the application of the methodology here described.

4. Thesis results

This section presents the detailed results of this master thesis, in terms of a set of assumptions (ref. section 4.1) and a set of recommendations (ref. section 4.2). The purpose of this section is to present the results, justify their inclusion and provide additional information as seen relevant to increase general understanding as a basis for organization individual tailoring of them[12]. Throughout the following subsections presenting the results, research questions (ref. section 2 RQ1-RQ5) are referred in the result text as found relevant (i.e. where presented results contribute to resolve different RQs). When it comes to RQ2 alert notification elements from other available literature, reference to relevant literature is included. This contributes to the resolution of RQ2, even if no additional RQ2 reference is made in the text besides the relevant literature reference. Combined, the complete set of here presented results contribute to the resolution of this thesis main problem statement (i.e. PS, ref. section 2). Refer Appendix 1 of this thesis for eased evaluation purposes. Appendix 1 contains a summarized overview of the here detailed results and how different elements of these contributes to the solution of different RQs and subsequently the main PS. The Appendix 1 presented metric provides an illustrative overview, based on RQ references included in the here presented detailed results. Refer this thesis section 5 a detailed discussion of these results in relation to the chosen and applied thesis methodology.

4.1. Assumptions for provided recommendations

To keep presented recommendations organization generic, but possible to tailor to the individual organization utilizing them (ref. RQ1 in section 2) a set of assumptions had to be defined. These also aid in maintaining focus and scope on alert notifications as an addition to an arbitrary organization's CM or IR and BR processes. The table below list the assumptions made with a short description, followed by textural additional information to justify their inclusion and contribute to an increased understanding of the assumptions in general.

#	Assumptions	Description
A.1	IR and BR processes are in place	This thesis assumes some form of IR and BR processes are in place within the organization and can be used as a basis to apply incident alert notification.
A.2	CM processes are in place	This thesis assumes some form of CM process is in place within the organization and can be used as a basis to apply maintenance alert notification.
A.3	Alert notification provision tool is available	This thesis assumes some form of provision tool[13] in place within the organization, which can be used to provide alert notifications as found relevant.
A.4	Alert notification trigger is in place	This thesis assumes some form of trigger is in place within the organization, to receive events that can become incidents triggering IR and BR processes (including alert notification if deemed critical enough).
A.5	Ability to tailor generic recommendations to the need and purpose of the organization.	This thesis assumes the organization has (or can obtain) the ability to tailor presented generic recommendations to be utilized to the best benefit of their individual organizational needs and defined purpose for alert notification.

Table 2: Assumptions

12 Note that the section 4 presented results are generic and is required to be tailored individually to suit any arbitrary organization utilizing them.

13 Note that this thesis does not make any assumption towards type of provision tool available. This could be anything from a quite simple possibility of posting a message on a webpage or a social media profile, to utilization of e-mail or sms to send specific alerts to predefined receivers or it could be any commercial off the shelf tool that include functionality that can be utilized for alert notification purposes.

This thesis fully recognizes the fact that when it comes to alert notifications different organizations have individual needs, resources and capabilities. It is, however, assumed that the organization has some form[14] of CM, IR and BR processes established (ref. A.1 and A2 in Table 2 above). Processes which can be utilized as a basis to apply maintenance alert notifications (CM) and/or incident alert notifications (IR and BR). The state and complexity of these processes vary quite much between individual organizations and the type of standard the organization base its quality system upon most often contributes to this difference. A difference which may include differences all the way down to the organization's internal utilized terminology.

To exemplify (ref. RQ2 and RQ3 in section 2), Telenor's internal terminology is influenced by the collection of different frameworks they utilize to efficiently handle different aspects of operation (e.g. eTOM, ITIL, LEAN etc.). This much similar to other organizations which terminology may be influenced by other utilized frameworks (e.g. ISO 9001, COBIT etc.). In terms of Telenor Operations Management, the case basis for this thesis, their "way of work" is mainly based on and influenced by the Information Technology Infrastructure Library (ITIL) [6]. When it comes to alert notifications, these are mainly anchored and covered within the following ITIL defined processes (tailored to the needs and purpose as defined by Telenor):

- Event Management
- Problem Management
- Incident Management
- Change management
- Release management

The three first ones of the above are covered in ITIL book 4 "Service Operation" and mainly relates to incident alert notification aspects. The two last ones are covered in ITIL book 3 "Service Transition" and mainly relate to maintenance alert notification aspects. Telenor's experience in direct relation to Operation Management is that the above are processes relevant to be viewed in coherence since they are tightly connected and often affects each other (especially Problem, Incident and Change/Release) [7]. In the case of Telenor their maintenance and incident alert notifications are therefore related to the corresponding relevant ITIL processes (mainly Incident and Change/Release). The figure below has been included to illustrate how the mentioned relevant ITIL books and processes relate to the overall ITIL life cycle perspective.

[14] *Note that the term 'some form' here not at all has to be something very complex. Also note that examples utilizing Telenor as a case basis in this thesis represents examples from the way things are done in a quite large organization (with corresponding complexity). Telenor examples are not in any way meant to be a 'generic solution' it is just one, out what could be several different examples, to show how it has been done there. I.e. an example aimed to increase general understanding by putting assumptions and recommendations into one organizational context (i.e. a context not necessarily suitable for other organizations).*

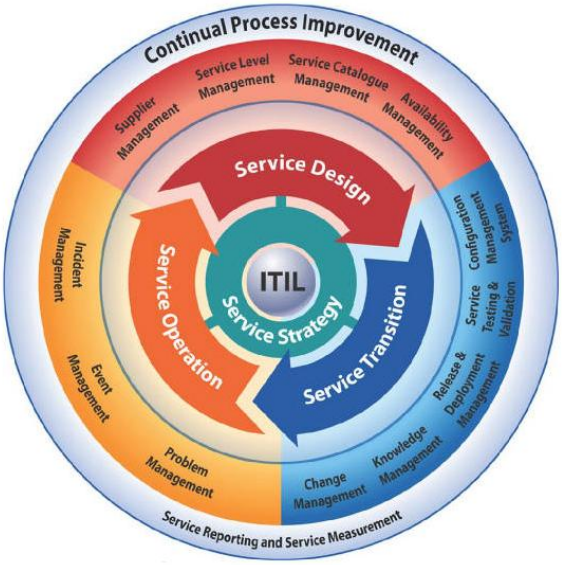

Figure 4: ITIL life cycle [8]

This thesis assumes system support tools in place that can be utilized to alert notify (ref. A.3 in Table 2), but it does not assume anything regarding the type of tool (ref. RQ1 in section 2). The level of tool complexity is individual to the organization and most organizations have one or more tools that can be utilized. As outlined and exemplified in this report introduction section and as a foot note in relation to the assumption listed above, one may utilize one or several types of tools, depending on organizational needs and purpose for alert notification, e.g.:

- A very generic (i.e. no specific details), standardized informational message posted on a publicly available webpage (and/or a company social network profile, e.g. Facebook or similar).
- A restricted available webpage such as a logon service for specific registered users (and/or a company internal webpage, e.g. on the company intranet)
- A service where alert notifications are distributed directly to a predefined set of relevant stakeholders via e-mail, sms and/or other types of individually addressed messaging.
- A separate tool/application of which allows for the organization to define and distribute different types of messages through different channels to different relevant stakeholders.

This thesis assumes some sort of such tool in place that can be utilized to distribute alert notifications (ref. A.3 in Table 2). Company individual needs and defined purpose for alert notification will provide some framework to choose amongst available tools possible to utilize. The organization should, however, also take into account in considerations that an occurred incident may also affect the alert notification provision tool (i.e. may not be able to provide notifications in some cases)[15]. Risk of this happening should be taken into account in the organizational considerations to choose amongst available tools.

To further exemplify (ref. RQ3 in section 2), Telenor Operations Management provides several different telecom and data services over a complex company owned infrastructure. They have different tools for alert notification on different levels for

15 Note (ref. RQ4 in section 2) that one of the more embarrassing findings documented in the Norwegian report from the 22-7 commission of inquiry [1, chapter 2, p. 22] was that (for several different reasons): "the first national alarm was actually not received nor registered by any relevant police districts this day".

different purposes. In this case, however, it is useful to focus specifically on the alert notification issued by operational managers. As previously mentioned, incidents classified critical enough, are tightly monitored by operation managers. Such critical incidents require incident alert notifications issued by the operation manager, to inform relevant stakeholders about the occurred incident and keep them updated on the incident response progress. In terms of the maintenance perspective, Telenor change managers are responsible to keep an updated overview of planned maintenance activities and issue maintenance alert notifications, to proactively inform relevant stakeholders about their planned execution time. Telenor change and operation managers have special tools to provide alert notifications to relevant stakeholders via e-mail and/or sms in accordance with stakeholder's requirements. Tools, that support these managers to perform efficiently in accordance with relevant requirements and responsibilities.

This thesis assume interfaces are in place for the organization to receive event reports that could become incidents triggering the IR and BR processes, including incident alert notification if found critical enough (ref. A.4 in Table 2). The thesis does not, however, assume anything about the complexity or sophistication of these interfaces (ref. RQ1 and RQ2 in section 2). As described by ENISA good practice [9], the interface may in its simplest form merely rely on a third party raising an alarm. I.e. the assumption does not necessarily mean a complex, highly mature and sophisticated solution with corresponding interfaces monitored by a large internal team. It merely assumes that the organization has some form of interface to receive information that can (if found critical enough) trigger the IR and BR processes should that be required.

To further exemplify (ref. RQ3 in section 2), Telenor Operations Management utilizes an internally defined way of classifying all registered incidents in accordance with their level of criticality. As previously outlined in this report, this classification regime will, dependent of incident severity classification trigger their IR and/or BR procedures. Incidents classified critical enough (without necessarily triggering BR procedures in addition to IR), will be closely monitored and alert notified by operation managers.

Although relevant to mention, it should be quite "as expected" that this thesis assumes the organization has the ability to tailor the presented generic set of recommendations (ref. A.5 in table 2). In this case tailoring means to tailor generic recommendations (ref. RQ1 in section 2) to the organization's best benefit based on organization individual needs and defined purpose for alert notification. This tailoring may involve to choose recommendations relevant (or not) in accordance with the organizations defined purpose for alert notifications. E.g. if maintenance alert notifications are defined as the only type the organization is to issue, recommendations specifically related to incident alert notifications may not be applicable. Tailoring may also mean to adjust some recommendations to better fit the organization's purpose for alert notification. As tailoring is performed, however, it will be of benefit to document changes made and the justification for them (e.g. recommendations deemed not applicable or adjusted recommendations). This, to ensure that the tailoring can be reviewed based on gained experience over time and changed if found relevant moving forward. Without a documented justification for the tailoring done, it becomes harder to reevaluate if the justification remains valid in future reviews. Tailoring is a quite commonly known critical success factor for efficient utilization of many different standards, recommendations and guidelines for any organization. Some organizations may choose to require external expert support to tailor the set of generic recommendations. However, most often internal resources are required to be heavily involved as well, as a critical success factor for organizational tailoring require in depth insight into organization individual aspects, e.g.:

- Core business objectives and requirements
- Understand the main organizational purpose for utilization (of a standard/"best practice"/guideline/recommendations)
- In depth understand relevant, current "way of work"/processes and its relation to the utilization (of a standard/"best practice"/guideline/recommendations)

To resolve this thesis main problem statement as outlined in section 2, it was early acknowledged that the work would have to rely quite heavily upon Telenor available knowledge (ref. section 3). This required the master candidate to gain in depth insight into areas similar to those mentioned in the list above, e.g.:

- Telenor business objectives and requirements (including security) in relation to alert notifications.
- Understand currently utilized procedures and solutions, its important elements of coordination, control and alert notification distribution (in relation to main business objective and defined purpose of alert notifications).

Based on the above, the master candidate had to have the ability to extract this current knowledge, combine it with relevant elements from other sources and from that draw a set of organization generic recommendations.

To further exemplify (ref. RQ3 in section 2), Telenor, the basis case for the thesis, has developed their current alert notification solution to, amongst others:

- Comply with requirements governed by law
- Be organizationally tailored towards business objectives through alignment towards ITIL and other organization internal frameworks
- Be continuously improved and tailored based on organizational needs for increased efficiency, new/updated infrastructure/services, customer/end user demands and requirements (e.g. as defined in SLA)

Organizations utilizing the recommendations provided in following subsections should be aware of the here presented assumptions and how they relate to their own organization. This to ensure the following recommendations can be utilized efficiently in a business beneficiary way[16].

4.2. Alert notification recommendations

This section provides the set of organization generic, alert notification specific recommendations (ref. RQ1 in section 2) defined to aid an arbitrary organization in the establishment and continuous improvement of well structured, secure and efficient alert notifications. The set of recommendations is based on assumptions laid down (ref. section 4.1) and are presented in subsequent subsections covering different key aspects of alert notification as follows:

- Recommended ***preparations***, as outlined in section 4.2.1
- Recommendations relevant to the ***alert notification solution***, as outlined in section 4.2.2
- Recommendations relevant to the ***alert notification message***, as outlined in section 4.2.3

[16] In terms of tailoring it is worth noting that the alert notification solution has to be scaled in accordance with the organizations currently available resources and capabilities. To be an efficient addition to established CM and/or IR and BR processes, it has to have a scale and complexity that the organization is able to handle as part of normal daily operation of such processes. Some creativity may be required to obtain such a tailoring, but the alert notification ability to be a beneficiary support of main business objectives are not defined by solution complexity and sophistication, even a simple solution can be shown to be quite beneficiary.

- Recommendations relevant for ***measurement, justification and improvement***, as outlined in section 4.2.4
- Additional aspects potentially relevant to consider in relation to ***alert notification audits***, as outlined in section 4.2.5

The following subsections present a summarized list of recommendations relevant to each key aspect with generic short descriptions followed by textural information to justify their inclusion and enhance generic understanding of them. The result presentation is finally rounded off with textural reflections related to the opportunity to utilize the set of recommendations to support audit of traditional processes including alert notifications (e.g. CM and IR/BR process audits, ref. section 4.2.5).

4.2.1. Preparations

The table below summarizes the organization generic recommendations (ref. RQ1 in section 2) relevant to prepare the establishment and reviews to improve well structured, secure and efficient alert notifications. The recommendations are provided with a short description, which is texturally detailed and exemplified below the table to justify their table inclusion.

#	Recommendation	Description
R1.1	Define the main purpose of alert notification aligned the organization's main business objectives.	The organization should define and document the organization individual purpose for alert notification, e.g.(but not necessarily limited to): - Compliance with legal requirements - Compliance with end user/customer requirements (e.g. SLA) - Create a bridge of communication between processes (IR and BR) to ensure common situational awareness should situation escalate and require others to take action (e.g. crisis management) - Make receiver more able to make "correct decisions" for themselves based on situational awareness
R1.2	Identify alert notification triggers in current processes	Assuming the organization has alert notification relevant procedures in place (i.e. CM and/or IR and BR processes), identify and/or add alert notification triggers in line with alert notification purpose and organizational needs. This includes triggers for alert notification initiation (CM and/or IR and BR), alert notification updates (IR and BR) and alert notification closure (IR and BR). In this, some sort of a definition of perceived "normal" as opposed to "abnormal" operation is useful as a basis.
R1.3	Define alert notification requirements relevant to fulfill its purpose	Requirements provide additional detail to the purpose "frame" for the alert notification solution. Requirements should be measurable and utilized as input to measurement, justification and improvement covered in section 4.2.4. As outlined more below, start off by defining overall requirements (e.g. type of notifications to provide), continue with more specific requirements (e.g. how to provide notifications, timing requirements etc) and make sure they comply with any relevant third party requirements (e.g. as governed by law, defined in end user/customer SLA etc.).
R1.4	Define alert notification relevant roles with descriptions.	Define roles directly involved in process added activities for alert notification (e.g. alert notification solution maintenance manager). Alternatively extend existing role descriptions to cover it (e.g. operation

		manager/incident manager/change manager etc.). Make sure the role description clearly defines both the role and its corresponding alert notification responsibility and authority. Make sure the responsibilities and authorities described for the relevant roles align with the identified list of stakeholders (as outlined below) and, as such, cover all roles directly or indirectly involved in alert notification.
R1.5	Identify and describe alert notification stakeholders relevant to its purpose.	Unless all stakeholders are provided with the same insight/notifications (e.g. through generic informational alert notifications posted on a website or similar), define the list of different types of alert notification stakeholders (i.e. list of relevant receivers of alert notifications), aligned with its purpose e.g. (but not necessarily limited to): - Authorities (as governed by law) - External emergency response units and rescue centers (when societal safety is "at stake") - The media and the general public - Other external third party (e.g. affected cooperators, customer/end user based on SLA etc.) - Crisis manager/crisis management team (i.e. purpose of communication bridging and common situational awareness) - All operation managers/incident managers/change managers (i.e. purpose of common situational awareness if the personnel holding the role changes during the course of a day or between days, e.g. 24/7/365 monitoring and handling teams where personnel is shifted over time) - Customer front end and press officer (i.e. in cases where these are responsible to inform third party external stakeholders based on internal alert notifications) Describe each defined stakeholder in terms of their relation to alert notifications, how they are to be notified (e.g. by receiving direct messages or through internal stakeholders receiving internal alert notifications) and the triggers relevant to issue alert notification to the different stakeholders (e.g. authorities, rescue units and end users/customers are triggered differently based on type, consequence and criticality).

Table 3: Preparation recommendations

A purpose for alert notification defined in alignment with the organizations main business objectives (ref. R1.1 in Table 3) anchor and justifies the effort made, at the same time providing the overall "frame" for the alert notification solution. The most important element in definition of purpose is for the organization to have an overview of the law governed requirements applicable to alert notification within their own business. These represent the "necessary minimum" of requirements the organization's alert notification solution is decreed to comply with. In many cases, regulatory authorities relevant to the law governed requirements also have defined guidelines which better detail when, how and what to report, even down to expected content of an alert notification message.

To further exemplify and as previously mentioned (ref. RQ2 and RQ3 in section 2), Telenor is required by NPTA to provide alert notifications as follows, based on the Norwegian "E-com regulation" [4, §8-5] (translated into English by the report author):

"The supplier is required to alert the Norwegian Post and Telecommunications Authority about events that may or already have reduced the ability of electronic communication services considerably. The Norwegian Post and Telecommunications Authority can define more detailed alerting procedures."

NPTA has, based on the opening for it in the law, defined a set of more detailed procedures/guidelines [10] for alerting the authorities. This provides more alert notification relevant requirements as to who, when, what and how alert notifications are expected to be provided to NPTA. It also contains their expectations related to alert notification message content (ref. also section 4.3 and 4.4 of this report). In this aspect of preparations, it may be worth noting that NPTA expect the telecom and data services provider to decide when to alert NPTA (i.e. define the NPTA alert notification trigger). NPTA expect the provider to have internal procedures describing in detail when to alert NPTA and that these minimum ensure alert notification when the event has turned into an incident with criticality (or ability to escalate in criticality) to a level where it adversely affects service delivery of societal important functions or other providers quality of service. Given the lack of alert notification specific but generic regulations/recommendations/standards, guidelines provided by any relevant authority may be of aid as a preparation basis for any organization. These are written based on the authority's defined informational needs and expectations to be kept notified in a certain manner and is required to comply with for organizations governed by the corresponding law, but may aid other organizations as a preparation basis as well. The here provided organization generic recommendations expect utilizing organizations to take that into account.

When it comes to define the organization's main purposes for alert notifications, law governed requirements compliance may be a simple minimum for (at least an initial) purpose definition. Such a minimum basis is, however, challenging. Even if compliance with law is required, that purpose itself does not provide any additional economic value generation that can support the establishment and improvement of a solution. That generates the recommendation to define additional purposes aligned with main business objectives. The following example (provided by the report author for illustrative purposes) shows what a broader business objectives aligned definition may look like[17]:

"The main motivation behind this organization's alert notification solution is:

- *To stay in compliance with law governed and other external requirements (e.g. SLA defined).*
- *Stay visible to internal stakeholders and keep these updated should an incident escalate into a crisis situation requiring active contribution from them in any way. At the same time keeping other internal stakeholders informed to avoid the need for incident responders taking time to answer questions about the occurred and, as such, allow them to focus on efficient incident response instead.*
- *Make internal stakeholders efficiently able to inform customers/end users/cooperators etc. This, to better maintain their trust in our ability to handle such situations efficiently. At the same time strengthening their ability to make more correct decisions to maintain "fact based normal operation" during a situation, should it occur."*

17 Note that the purpose defined by the author as an illustrative example does not assume anything about the alert notification solution when it comes to sophistication and complexity. The example is just as valid for sophisticated, complex alert notification solutions as for the simpler ones (e.g. standard messages published on a suitable web page). Note however also that most simple web page publishing solutions are often supported by more sophisticated, complex internal solutions (i.e. published messages are generic, written for the general public to reduce pressure on the provider to reduce amount of end user request to handle while the situation is present, while internally more detailed solutions are utilized to keep internal stakeholders updated and coordinated, focused on efficient handling of the situation at hand).

Based on the above, it is recommended not only include the law governed minimum, but also the business oriented perspective relevant to, e.g.: Business internal increased efficiency, an additional trust builder towards external stakeholders provide them with situational awareness enabling them to make more correct decision based on situational facts.

For further exemplification utilizing Telenor, as the basis case for this thesis (ref. RQ3 in section 2), their main purpose of alert notification is to:

- Comply with law governed requirements
- Keep internal stakeholders updated to handle requests from external stakeholders and the public
- Update internal stakeholders to establish a common situational awareness should any escalation of the situation require involvement of other internal (or external) stakeholders for efficient resolution in accordance with defined procedures

Different internal stakeholders also have different responsibilities while the incident resolution process progress, depending on the type and severity of the incident, this includes responsibilities to inform (or respond to questions from) external stakeholders such as (but not necessarily limited to):

- end users/customers (typically based on SLA requirements)
- emergency rescue units (if a geographically confined incident is severe enough to require it)
- municipality/county emergency preparedness boards (if a geographically confined incident is severe enough to require it)
- authorities as found required
- other affected service providers operating on the infrastructure
- the media (should the incident be of such severity that it is of public interest)

The main policy of Telenor is to keep all relevant internal stakeholders informed at all times to:

- ensure their ability to fulfill their responsibilities to inform external stakeholders
- keep a common situational awareness, should future escalation or change in the situation require internal stakeholders to take a more active approach in support to resolve the incident and regain a normal operational situation

The recommendation to identify alert notification process triggers in the organization's traditional CM and IR/BR processes (ref. R1.2 in Table 3) can be approached in several different ways. No matter the standards, framework or regulations (ref. RQ1 in section 2) the processes are aligned with, most CM processes do require a change risk assessment to be performed to define risk involved with implementing a change. The result of such a risk assessment can be utilized as a trigger to issue maintenance alert notifications given a result that indicates a certain level of risk. One could, off course, decide to send maintenance alert notifications to all relevant stakeholders for each and every change planned implemented, if the organization has the resources to do that in any efficient manner. A more professional approach, however, could be to issue alert notifications to relevant stakeholders only for those planned changes (maintenance activities) that shows a certain level of risk that it could, when performed, affect quality of service adversely.

Correspondingly one could decide to alert notify all incidents recorded (no matter its level of criticality). A more professional approach, however, would be to utilize a

clearly defined incident criticality classification scheme and determine the level of criticality classification required to trigger alert notifications for a detected incident. To provide a broad perspective on professional possibilities as outlined above, one can imagine a typical illustration of a random organization's risk profile (i.e. a snapshot of the risk profile typically included to provide high level perspective of results from a performed risk analysis), similar to the illustration below.

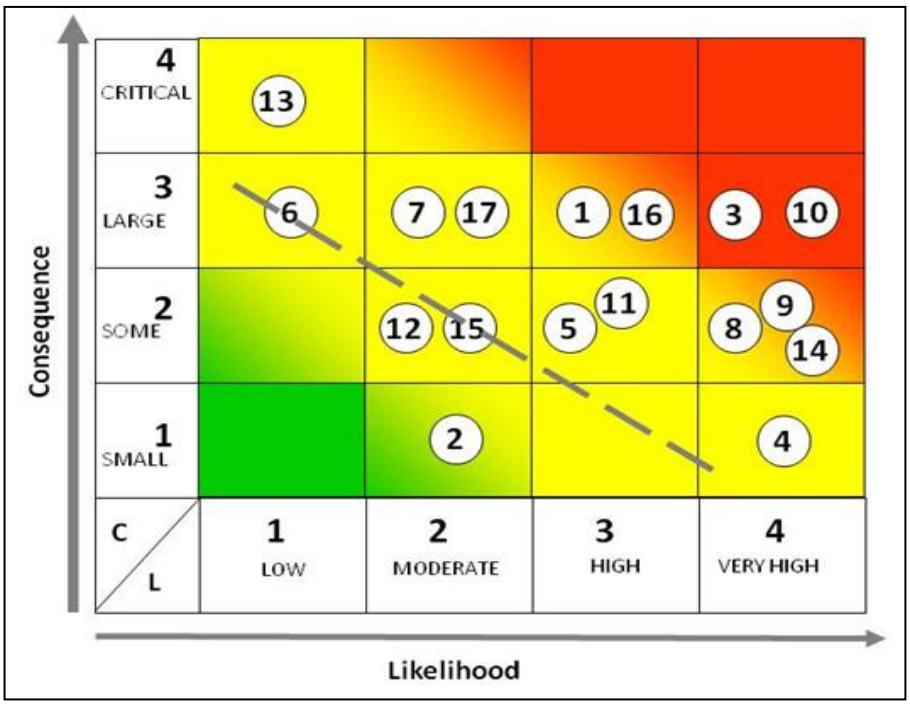

Figure 5: Summarized risk analysis result – illustrated risk profile

The above illustrates a snap shot risk profile of a random risk analysis performed (ref. RQ2 in section 2). The numbers illustrate different risk scenarios included in the analysis, placed in the matrix in accordance with the analysis results. The dashed line included in the yellow field descending from left to right in the above matrix illustrates a random organization's decision of their individual "acceptable level of risk". The area below the dashed line, represent the residual risk the organization is willing to accept, requiring the organization to prioritize with the aim to mitigate all scenarios with results rated above the dashed line to a level below it. The above risk analysis result overview/risk profile is a presentation of risk analysis results of scenarios evaluated against a defined list of values for likelihood and consequences (recognizable from recommendations provided in several different standards and regulations relevant to risk analysis, e.g. different ISO standards, RiskIT from ISACA etc.). Utilizing the above figure, including some adjustments, the same type of matrix can be utilized for incident classification purposes for all types of organizations, as illustrated by the thesis author through the below adjusted figure.

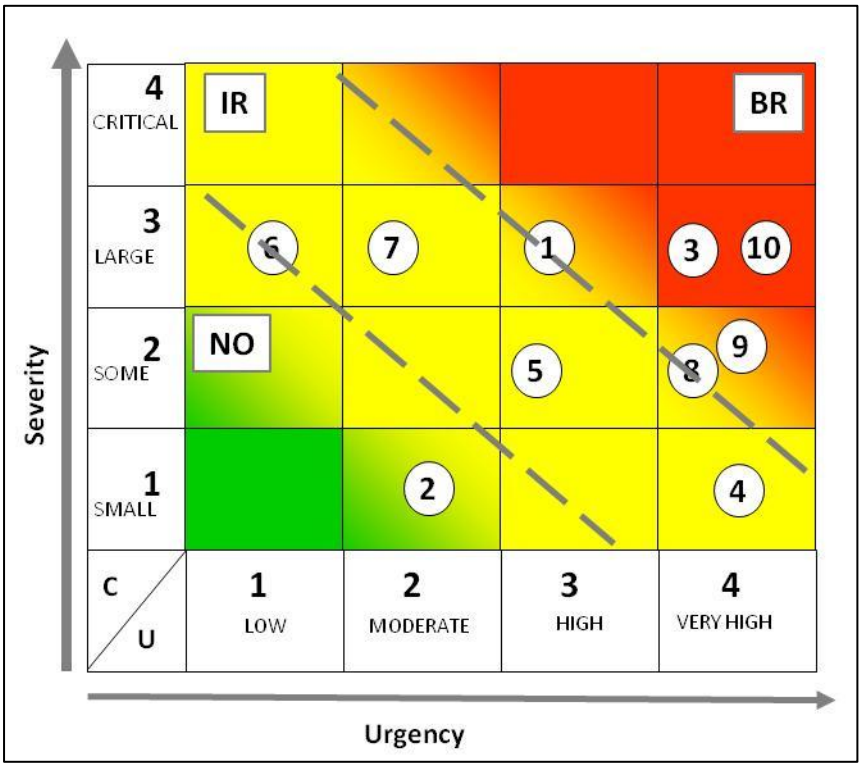

Figure 6: Incident classification illustrated

The above illustration (Fig. 6) is an adjusted version of the illustration shown in Figure 5. The above is a simplified illustration that has its basis in the ITIL [6] way of incident classification by severity and urgency, extended to provide an illustrative view that covers the broader process perspective from normal operation (ref. NO in Fig. 6) escalating into incident response (ref. IR in Fig.6) and further escalation into business recovery (ref. BR in Fig.6). The two lines descending from left to right in the above figure illustrates the trigger points between the different processes which correspond to the process illustrations as presented in this thesis introduction (ref. Fig. 1). An illustrative figure like the one above, can represent a useful tool both in relation to define trigger points between the organization's different relevant processes based on escalation and as such also a basis to define the difference between them. At any given time, any organization will be handling different types of events and problems as part of daily operation. Provided that the organization has taken necessary precautions, most of these events will never be severe enough to trigger an incident response process. From time to time, however, events severe enough to trigger incident response occur and have to be handled accordingly by initiation of the incident response process. Should it escalate further, the organization's business recovery processes are triggered (i.e. disaster recovery, possibly with the supplement of business continuity), as outlined in this thesis introduction illustrated through figure 1.

An organization's endurance in terms of process triggering is individual and depends on the organization's available resources and capabilities. Some organizations may lack or have weaker precautions in place and, as such, have to trigger the IR processes a lot earlier than others. Depending on the capability and resources defined, the triggering of the IR process may mean to trigger a third party supplier's IR process (managed by an organization internal process for that) or trigger organization internal IR and BR processes as found relevant, should the situation escalate to that level. No matter the resources and capabilities of the utilizing organization, the above presented illustration could be a good basis to define trigger points in traditional available

procedures in accordance with the organizations available resources and capabilities (ref. RQ1 in section 2). Somewhere in the here illustrated hierarchy of processes and triggers, individual to the organization, the organization should be able to define triggers for alert notifications issue, updates and closure as well.

In terms of normal operation (ref. Fig. 5 NO), it is important for any organization to have a clear definition of normal operation vs. "abnormal operation". In some organizations this may be a quite easy separation, but according to experts in the field who audit organization's IR and BR processes, most struggle to define normal vs. "abnormal" operation (ref. RQ4 in section 2). A clear perspective on this is important, since in most organizations normal vs. "abnormal" operation typically is the trigger point for the incident response process. Upon direct questioning to different organizations, especially organizations that have resources and capabilities to have internal operation monitoring and incident response teams, this seems to be challenging to define. Most often justified by the statement: *"We are an incident response team and as such handle "abnormal" situations all the time."* This being said, even incident response teams do have normal operation and "abnormal" operation. For instance where normal operation may be the continuous handling of incidents and the threshold for "abnormal" may occur when incident severe enough to require heavy prioritization, requires resources to be removed from "normal operation" to support the efficient handling of more severe (e.g. major) incidents (i.e. moving from a "working smart" situation to a "working hard" situation). Previous research [11] applicable to organizations in general shows that a critical success factor for organizations and teams, is the ability to dynamically go from "working smart" into "working hard" those few times it is required ***and*** efficiently back to a "working smart" situation (ref. RQ2 in section 2). In terms of incident response, a "working smart" situation could correspond with normal operation, where the team handle less severe incidents and at the same time improve their processes and procedures to become even more efficient in future incident response. "Abnormal" operation could correspond with the "working hard" situation, where an incident severe enough to require immediate handling (i.e. pulling resources from normal operations tasks such as improvement, putting improvement on hold until severity is reduced by mitigation back to "normal operation" situation). As previous research has shown, the ability to balance this within the organization is the key success factor to obtain a team that is not only able to efficiently handle more severe incidents when they occur, but also obtain a continuous focus on improvement that making them steadily better over time.

It is recommended to define some requirements for alert notifications (ref. R1.3 in Table 3). In the beginning this might only be a few requirements which can be extended with experience based lessons learnt. It is important, however, that the defined requirements are supported by the systems to enable for efficient extraction of reports for review at certain time intervals. Such report reviews can aid in detection of bottlenecks in the overall alert notification solution and be a valuable basis for input to prioritize actions to improve it. On the same basis it is important that requirements are either specific towards "framing" the solution, e.g. requirements stating what type of alert notifications the organization shall provide or requirements stating how often the defined alert notification should be reviewed for improvement. If not being "framing" the requirements should be measureable so that they can be used to measure performance in terms of how the alert notification solution supports its defined purpose towards the main business objectives. When defining this type of requirements it is worth having a look at suggestions for measurement, justification and improvement as outlined in section 4.2.4.

In addition to several other aspect, timing is of relevance when it comes to alert notifications and requirements for them. Maintenance alert notifications are typically required to be sent to relevant stakeholders proactively a certain amount of time

before the maintenance activity is planned executed. In terms of incident notifications and requirements, timing is also a quite essential aspect. Most often, a customer/ end user will experience the consequences of an occurred incident immediately (i.e. customer/end user experience occurs at the same time as system detection). Efficient sheltering of the team, working to resolve the incident in such a case, requires alert notification sent to alert customer front end contact point as soon as possible after incident detection. Challenge is however that at the time of detection, consequence may still not be clear, but one should at least have some form of requirement to inform within a defined delay after detection, even if some information is still unknown, e.g.:

- *"All incidents classified severe enough to require alert notification should initiate first alert notification no more than X minutes after first detection".*

There are several examples of timing requirements that can be defined and utilized in addition to the one above. Most such requirements are results of third party requirements upon the organization (e.g. customer/end user SLA etc.). Aside from such requirements, however, the following two aspects are recommended included for any incident alert notification solution in addition to the example above:

- A requirement towards the issuing frequency of updated alert notifications, e.g.: *"Incidents requiring incident alert notifications should provide updated incident alert notifications whenever the situation changes and at least every X hours."*

- A requirement towards the alert notification closure, e.g.: *"Incident alert notification closure message should be sent as soon as the incident is mitigated to a level classified too little severe to require continued incident alert notification."*

The requirement regarding frequency of alert notification updates is important to keep stakeholders continuously informed and create important trust. By reassuring the stakeholders (i.e. receivers) that they will not be left without updates "indefinitely" awaiting any actual progress of incident response (i.e. based on situation change alone), they can proceed with "fact based business as usual". It also provides them with a better basis to make their own more correct decisions, e.g. in terms of how long they can endure the situation occurred and ongoing IR processes, before they will have to for instance invoke their own BR processes. When it comes to internal stakeholders (e.g. crisis manager/team), the continuous updates provide a trust that they are continuously updated and share a common situational awareness should the incident severity escalate and require their action. It also provides them with the opportunity to decide to take action, e.g. based on lack of progress over time although severity stays the same, should they determine that the lack of progress itself escalates the severity of the issue. As such the incident alert notifications and their updates provides an efficient communication bridge between processes and different levels of responsibility that can be utilized to take appropriate action efficiently based on visualized progress.

Requirements such as the examples above are relevant input that should be utilized in a beneficiary manner by the organization defining corresponding Key Performance Indicators (KPI). The ability to pull reports on a regular basis allows for the organization to monitor the efficiency of the alert notification solution and adjust requirements to improve accordingly based on documented experience. This combined with some additional directions relevant to use in the context of requirements definition, as outlined in the following subsections regarding alert notification solution (4.2.2) and message (4.2.3), can be utilized as a basis for KPIs and measurement as outlined in more detail in section 4.2.4. At time of establishment

it should be noted that a set of requirements to provide "before and after" measurements are strongly recommendable to support the effort of establishment. In a process of establishment it should also be noted that different types of financial models do exist [12] and could be useful to utilize for additional justification of effort.

The recommendation to clearly define roles (ref. R1.4 in Table 3) is important to adhere to. Roles have to be clearly defined for the CM, IR and BR processes, including roles in direct relation to alert notifications. The role descriptions should clearly defined both responsibilities and corresponding authorities, such as for instance (but not necessarily limited to):

- The role responsible to issue different types of alert notifications (e.g. change manager and/or incident manager and/or operations manager).
- The role responsible quality assure the content of issued alert notification messages (which could be the one issuing them if the responsibility of writing them is delegated to some other role).
- The role responsible to quality assure information provided to external third party (in situations where for instance customer front end resources receive internal alert notifications and on that basis inform customers/end users upon direct request or in line with requirements defined e.g. SLA).

Each responsibility should (ideally) be described with a corresponding authority. One could for instance define that the responsible to issue alert notifications (e.g. change manager and/or incident manager and/or operation manager) also have the authority to decide when to close alert notification. I.e. that the responsible role have the ability to evaluate the situation at the time when the criticality classification of an incident is reduced below required level to issue alert notification, whether or not that justifies alert notification closure, or the criticality classification reduction has been premature. Another aspect of authority relevant to role descriptions is the now quite commonly accepted fact that during abnormal situations (e.g. major incident response/disaster recovery) lower level management has to be provided with the authority to make "bigger decisions than before". This is important due to the fact that time is of the essence in such situations and often requires a relaxation of conventional normal constraints [13, Chapter 7.4, p.145]. In an IR and/or BR situation this could mean that the role responsible to handle the situation have the ability to take on a larger amount of cost in terms of efficient resolution without having to clear this with top level management through formal and slow channels. This could be defined based on boundaries for instance in relation to the classified level of incident criticality. It is important, however, to proactively have this clearly defined and understood within the organization, cause during a major incident/crisis response there is no time to deal with such issues. The provision of alert notifications provide common information basis to a set of stakeholders, but it is important that each role involved understand their role with corresponding responsibilities and authorities to ensure that the alert notification becomes a good additional communication tool without setting off "unexpected actions" in a situation where time and efficiency is of the essence.

A defined list of described stakeholders (ref. R1.5 in Table 3), is important. Defining the list makes the organization aware of different stakeholders and their different types of motivations and expectations in relation to alert notifications received (which will become somewhat apparent by the stakeholder description). As a professional alert notification provider generic insight into these aspects are relevant to provide the best possible service. This consideration is generically relevant (ref. RQ1 in section 2), even in more simple cases where standard alert notifications are made publicly available on a suitable web site or similar. When it comes to more complex solutions, however, where specific, relevant stakeholders are informed about planned maintenance/incidents by directly addressed alert notification messages the

importance of such a defined list of stakeholders increase. This due to the importance of everyone involved having a clear understanding of different types of stakeholders and the triggers relevant to alert notify them, which should be clear from the description of them. Depending on the organization internal strategy utilized to alert notify, there may be different roles internally with different responsibilities to inform stakeholders. Even if some of such things can be sorted by efficient system support (e.g. well defined, controlled databases of stakeholders where alert notification receivers are automatically collected based on planned maintenance/incident to alert notify), some cases may stakeholders may be required to be contacted differently and only when certain specific conditions occur. E.g. rescue units/municipality emergency preparedness teams etc. which may require direct contact by phone or otherwise in cases where public safety may be adversely affected. It is also important to continuously seek to update the defined and described list of stakeholders, to keep up to date with stakeholder's expectations through receiver satisfaction measurements as a basis for continuous improvement as outlined in this section 4.2.4.

To exemplify a bit furter, utilizing Telenor as the case basis for this thesis (ref. RQ3 in section 2), Telenor alert notify a series of different stakeholders in different ways, depending on the situation. This is especially relevant to incident alert notifications. Major incident response may for instance require the incident manager to be in direct contact to keep municipality/county emergency preparedness boards updated on progress, while customer front end contact is responsible to call relevant, local rescue units and make them aware of the situation occurred. This in addition to the normal system supported incident alert notifications and updates issued to other stakeholders via e-mail and/or sms. In the case of Telenor, major incidents may also subsequently be required by authorities to be documented in a retrospective report for them to review the total incident response progress, from occurrence and detection to resolution.

4.2.2. Alert notification solution

The table below summarizes the organization generic recommendations (ref. RQ1 in section 2) relevant to consider in relation to the alert notification solution to establish and improve well structured, secure and efficient alert notifications. The recommendations are provided with short descriptions, which are texturally detailed and exemplified below the table to justify their inclusion.

#	Recommendation	Description
R2.1	Maintain and control the list of alert notification stakeholders (i.e. receivers) continuously[18].	It is recommended to handle the complete list of stakeholders (i.e. receivers) in one database to reduce the amount of resources required to maintain it. The list of receiving stakeholders should be limited. I.e. include only internal resources (also those responsible to inform external stakeholders such as authorities, customer/end user based on SLA etc.) expected to act or be prepared to act should the situation escalate further. Maintain list continuously (at least in terms of periodical routine checks) in accordance with relevant internal routines (e.g. HMS routines as part of personnel being hired/leaving).

[18] *List of alert notification receivers has to be continuously updated, it can reduce handling ability severely should these lists be found to be out dated when an incident occurs. As the 22-07 commission of inquiry reported it [1, Chapter 8, p. 157]: "Internal alert notification lists were defective, and the alert notification lists for external stakeholders were not updated".*

		When internal personnel (e.g. customer service/similar) are responsible to alert notify external third party (e.g. rescue units/municipality emergency preparedness teams, customer/end user based on SLA, the general public through the media etc.), make sure they continuously maintain their (part of the) stakeholder's list to the same level of quality.
R2.2	Avoid serial processing as far as practically possible.	Where possible it is recommended to avoid serial processing to increase generic efficiency in incident handling and alert notification. Time is of the essence and any element unnecessary delaying (especially the first alert notification in incident handling) should be removed or "mitigated" accordingly.
R2.3	Automate for increased efficiency, where found possible.	Automation cannot replace humans as an important part in efficient work, but automation to release human resources to focus on areas where human effort actually is required, is recommended. This, wherever such automation can be done without an unacceptable reduced level of processing quality.
R2.4	Operate based on a clearly defined regime for incident classification.	It is recommended only to operate with the number of classifications relevant to utilize. Levels of classification should be described well to reduce risk of faulty classification. In cases where system automated classification of an incident is done, based on an accumulated set of receiver system events by most likely root cause, the overall incident classification should not be lower than the highest classification of all accumulated events. Define and clarify threshold definitions based on classification. E.g. event/issue vs. incident vs. crisis based on low, medium and higher levels of criticality classification, including alert notification initiation/closure and incident response initiation/resolution.
R2.5	Operate under strict change control.	As far as practically possible it is recommended to operate under strict change control, especially when it comes to certain critical changes (e.g. increased/decreased severity classification and mitigation vs. resolution). It is recommended that such critical changes during progression should require a short description/justification. This is valuable in many aspects, e.g. lessons learnt, knowledge sharing, retrospective reporting etc.

Table 4: Alert notification solution recommendations

When it comes to alert notification solution it is important to maintain and control a list of stakeholders (i.e. alert notification receivers) as efficiently as possible (ref. R2.1 in Table 4). This is not to be confused with the list mentioned in preparations (ref. R1.5 in Table 3), but relates to the actual alert notification solution (i.e. database or similar). Here also please note that even if the organization has made a decision to utilize the simple solution to alert the public by alert notifications posted on a web site or similar, this does not exclude the fact that the organization may require internal more sophisticated alert notification solutions to handle operational situations more efficiently and that may require a stakeholder's list of its own (i.e. database or similar). It is recommended that the list of stakeholder's is kept in one database. That reduces the resources needed to maintain and control it, as opposed to several databases with several different responsible parties involved maintaining and controlling different stakeholder's databases according to different routines. The list of stakeholders maintained and controlled in this database should be kept at a necessary minimum. In a reality where the "need" to be kept informed is in general increasing, the organization still should keep a specific focus on the stakeholder's required to be kept informed [2, Chapter 5, Page 188-189 and Chapter 11, first paragraph of section "Managing crisis communications"]. If the organization work based on the strategy

that alert notifications are issued to inform internal stakeholders and different internal stakeholders are responsible to inform different external stakeholders in different ways, these internal stakeholders should be required to maintain and control the list of external stakeholders to the same level of quality as the internal ones. In cases where external stakeholders are alert notified through the same channels as the internal stakeholders, such stakeholders may be included in a stakeholder's database on the same terms as the internal stakeholders. It is probably still relevant though to make internal resources closest to the external stakeholders (e.g. key account manager/customer service/PR contact etc.) responsible to maintain that part of the stakeholder's database as part of their normal follow up routines. The same way it is important to reduce efforts required to keep the database of internal stakeholders maintained and controlled, by aligning it with normal internal procedures. E.g. make a small addition to the HMS procedures for personnel leaving/being hired to make sure internal alert notification stakeholder's lists can be continuously maintained accordingly. This provides increased efficiency in maintenance by utilization of procedures already present, as opposed to create additional resource demanding ones. In this it is also important to remember the security aspects in maintenance and control of receiver lists. E.g. if stakeholders are replaced/leave, their internal e-mail address is most often deactivated as part of HMS routines, but most often they bring their cell phone number with them. I.e. in a case where HMS routines are not aligned with routines to maintain the stakeholder's database, people no longer internal may still receive alert notifications on their cell phones and depending on where they move too (e.g. competitor) this may have a very adverse effect upon the organization. The same is most often the case when it comes to external stakeholders. I.e. no matter the choice of solution, it is important to maintain and control a solution included list of stakeholders (ref. RQ1 in section 2).

The recommendations to avoid serial processing (ref. R2.2 in Table 4) and automate where possible (ref. R2.3 in Table 4) are closely related and mainly included based on experience gained by Telenor as a case basis (ref. RQ3 in section 2). This is important to keep in mind no matter the alert notification solution (ref. RQ1 in section 2), but becomes more and more relevant the more complex and sophisticated the surrounding system support solutions become.

To further exemplify, utilizing Telenor as a case basis (ref. RQ3 in section 2), Telenor Operations ability to handle the approximate 1.5 million events reported from their infrastructure and services on a daily basis is heavily increased by their front end receiver system for such events. The front end system receive, accumulate and link events, based on most likely common cause (i.e. likely root, since root cause most often generate a large series of events/alarms from affected infrastructure/its surrounding infrastructure). The front end system then establish a number of actual events relevant to be handled by Operations in another system, which issue the events to the relevant response team based on most the likely common cause of the system accumulated event. Combined with registered customer reported events in the same system, the number of actual events to be handled by Operations on a daily basis is approximately 300-600 events. Most events are resolved as part of usual 24/7/365 operation, but when events classify as incidents severe enough, their resolution are more closely monitored by operation managers also responsible to provide corresponding incident alert notifications for them. These are alert notifications provided in addition to alert notifications about planned maintenance. The front end event accumulating system contributes quite much to Telenor's ability to handle a large number of events and corresponding incidents efficiently. The front end system automated event accumulation as such represent an example of both the recommendation to avoid serial processing (ref. R2.2 in Table 4) and system automation for efficiency where possible (ref. R2.3 in Table 4). This being said, however, there are several aspects that

can be utterly improved over time and Telenor is working to improve their "way of work" even more when it comes to efficiency.

As an event reach a response team, the team has to verify the root cause deemed most likely by the front end system through root cause analysis. The team also have to do an analysis of the accumulated event to gain an overview of the actual consequence and on that basis also determine if the criticality level set on the event by the front end system represents reality or if it has to be changed. This type of analysis may be performed manually by the team and in some cases that may be most efficient, but in many cases large parts of these analyses may be system automated with a subsequent verification of results performed by the response team. Such automation will in many cases make the process of analysis more efficient without unacceptable level of quality reduction. In this essence it is also worth noting that if system support is of such low quality that different engineers/response teams work in parallel until a root cause can be determined, this is less efficient than the ability to reach a likely root cause quite fast and, as such, involve only relevant resources in the response. In general and in terms of any procedures changed from manual to system automated, the following is relevant to be extra cautious about:

- Make sure quality assurance aspects (including security) embedded in manual routines are maintained (i.e. not lost with automation, e.g. by manual verification etc.)
- Make sure to focus on automating manual routines that are resource demanding but quite systematical (i.e. automation of routines that change much from case to case are much harder to automate beneficiary than routines relevant to perform the same way in every case)
- If some sort of quality assurance aspects are embedded in the automation, make sure to monitor it to make sure it is to the level of quality expected when the organization starts to work on the basis of the automation.

To exemplify in relation to the above one could imagine having a front end event accumulating system similar to Telenor. As part of the event accumulation, the system link all related events to the event deemed the most likely root cause of all the events. If severity classification of the accumulated event is initially set by the system as part of the system automation, the accumulated event severity classification should be more severe or similar to the most severe classification of the accumulated events. The alternative would most likely be that the front end accumulation system accumulates events without changing any severity classifications. This could represent a risk of erroneous classification difficult to detect by the receiving response team. I.e. they receive an accumulated event with a medium risk level (e.g. not requiring alert notification) but later on, through manual analysis, find the classification level to be set too low. E.g. due to the fact that the accumulated event is a low level infrastructure issue (by itself not deemed very critical), but it has occurred in a way that it affects a series of very critical services (i.e. linked events which by itself are more critical than the root cause event). The critical events "hidden" in the linked events of the accumulated event is not directly visible to the response team. In such a sense where time is of the essence, it would be much less problematic for the response team if the accumulated event was classified more severe (or at least as severe as) the most severe linked event. This way one could have ensured alert notifications triggered quite immediately and be updated until the incident was mitigated sufficiently enough to close alert notification. Most often it is better to initiate early alert notification and rapidly reduce than to start escalation (and alert notification) way later when manual analysis/verification determines erroneous system automated classification (or maybe this is not detected at all until end user/customer reported events reveal that to be the case). The above outlined is a typical example of "worst case" automated system decision, often used within security and risk management in general to ensure that no

potential high level criticality remains "hidden" and as such is erroneously prioritized in terms of efficient handling.

It is important that (event and) incident handling is prioritized based on a well defined and documented common classification scheme (ref. R2.4 in Table 4). This is relevant in relation to alert notification efficiency, no matter the level of sophistication and efficiency of system support available for handling it (ref. RQ1 in section 2). It is individual how organizations handle this in practice. Some may have one system for event handling (e.g. "normal operation") where events that turn into incidents are transferred for handling into another system (e.g. "abnormal operation") and even further into yet another system if the incident turn severe enough to require business recovery (BR) procedures to be initiated (e.g. "crisis management"). In other organizations, one system may be suitable for all of these aspects (just controlled by severity classification level), e.g. where "events" are classified within a very low severity and when they through escalation pass a threshold in classification, they become incidents initiating IR procedures. If escalated even further they become major incidents initiating BR procedures and corresponding handling. In all aspects of solution, the organization should have a clearly defined classification scheme and corresponding threshold definitions for procedure initiation (including the initiation, updates and subsequent closure of alert notifications), not too different from what's illustrated previously in this report (refer section 4.2.1, Figure 6). The defined classification scheme enables a structured approach to operation ("normal" as much as "abnormal") and alert notifications. It also provides support in handling prioritization and a basis reducing the likelihood of erroneous classification, provided that those handling events/incidents have a good understanding of the classification scheme. In specific relation to alert notifications it is important to (in the classification scheme) identify the classification criteria requiring alert notifications. Incidents that are classified with that severity level (or higher) will typically result in the issue of alert notification and updates through the response progress, until the incident is mitigated back down to a classification level no longer requiring alert notification. When that happens, alert notifications are closed (issuing a "closure message") and will remain closed, unless the incident for any unfortunate reason should re-escalates again, to a criticality level requiring alert notifications to be re-initiated. In this aspect, please note that the classification regime may have more levels of classification than those requiring alert notifications. This is also recommendable because it creates the opportunity to trigger alert notifications based on classified severity level. At the same time, the closure of alert notification merely means that the consequences of the occurred incident are mitigated adequately enough to reduce the incident level of criticality to a level where alert notifications are no longer required. The work to actually resolve the incident will remain ongoing after alert notification closure and in this, it is important that the organization maintain focus to resolve root cause (i.e. not stop at consequence mitigation) to ensure future improved resilience. Unless the organization maintain focus to resolve root cause before actual incident closure, the organization remains in a constant risk of reducing their resilience in such a way that, at some point, normal, low risk, planned maintenance activities (or others) could result in a severe cascading failure situation, difficult to handle, understand, control and efficiently "bounce back" from [14, The Ninth Link: Achilles' heel, section 7, Page 119-121].

Strict change control is a recommendation included (ref. R2.5 in Table 4). In many cases, different organizations utilize several different incident response/alert notification tools to support them but the level of system support in these to require a level of change control vary. Strict change control is therefore recommended to a certain level, no matter the solutions utilized (ref. RQ1 in section 1). In this relation it is especially recommended that changes that could prove critical towards handling (e.g. severity classification changes) are required documented/justified with a short

informational note. The here recommended change control relates to make sure that there is a certain level of enforced change control for some elements of change for instance embedded in the tool utilized to handle incidents. It is recommended that system enforced change control is implemented for the most critical aspects of incident handling to ease retrospective documentation of an event. An example of a critical change that could benefit from system embedded forced change control is change of incident classification (i.e. incident severity level). When such a change is performed by any incident response team member, the tool could enforce a requirement to add a couple of lines of text to justify/explain the change made. A few required lines of justification does not put incident handling to a halt (documenting) and even if such a requirement "in the heat of the moment" may seem "unnecessary time consuming" this is outweighed and balanced out by the retrospective benefit. This required documentation enables the organization to track changes during the course of incident handling and utilize this for learning, with the purpose of improving efficiency and correctness in the future. This is sometimes required by authorities (e.g. post incident report requirement), but is also very beneficiary in terms of review of incidents for the purpose of lessons learnt. The here provided recommendation is quite commonly used in event and incident handling systems used within certain high reliability organizations, since changes of critical elements such as severity level have the opportunity to adversely affect the whole process of prioritization and handling should erroneous changes be done.

Also note that in terms of recommended documented change control (ref. R2.5 in Table 4), a record of all the issued maintenance and incident alert notifications themselves are relevant. This, both in relation to retrospective documentation of a certain issue and in terms of review for lessons learnt purposes.

In relation to Telenor, the case basis for this thesis (ref. RQ3 in section 2), worst case of an erroneous incident classification could delay its priority quite much and as such also allow for the actual situation (in the mean time) to escalate to a level that require a lot more efforts to respond and handle than it would have, had it been correctly classified in the first place. This risk could off course be somewhat reduced by the fact that affected customers have the ability to report their experience as well and that could trigger the relevant attention, but that would still be "delayed attention". Lack of/late prioritization due to "misleading classification" such as this also often result in a much more costly response process and could also result in authorities attention in such a way retrospective reporting back to them is ("unnecessary") required and further increase the total cost related to incident resolution.

4.2.3. Alert notification message

This section takes a closer look at recommendations relevant to alert notification messages in terms of content (generic, maintenance specific and incident specific content) and generic additional recommendations regarding alert notification messages.

This thesis provides recommendations regarding alert notification content, but does not assume anything about the chosen communication medium for alert notifications (ref. RQ1 in section 2). This being said, however, it is worth noting that even if the type of information to include is generic, the actual amount of information included in an alert message has to be adjusted in line with the chosen communication medium (e.g. an sms cannot include the same amount of characters as an e-mail etc.).

The table below list information typically relevant to include in generic alert notifications, both maintenance and incident alert notification messages (ref. RQ1 in section 2). The recommendations are provided with a short description, followed by

some textural additional information for inclusion justification and examples for increased understanding.

Type	Recommended content	Description
Maintenance and incident	From	The message should identify the maintenance alert message issuer (e.g. Telenor Incident Manager/Telenor Change Manager/Telenor Operation Manager or similar).
	To	Depending on the solution utilized to issue alert notifications this field should either identify the actual receiver (assuming message is sent "one by one") or just show information of type "undisclosed list of receivers".
	Title	Title should be "easily recognizable" for the receiver, e.g. "Telenor Maintenance/Incident Alert Notification – CaseIDxxx"

Table 5: Alert notification message

It is recommended to clearly identify the sender of the alert notification. In this it is recommended to identify by role, rather than actual person (i.e. employee). This is relevant to provide a shelter for actual employees and avoid a situation where they are contacted (by response to message) directly, as this will take focus away from their primary managing role of the situation. In addition, the identification of role, as opposed to the actual employee, ensures the sender can be identified similarly no matter what employee is holding the role at any point in time. This is useful in general, but especially useful in larger teams where the managing role may change during the course of a day or between days depending on the defined shift schedule.
Messages typically identify the receiver, but depending on the solution, this is recommended done in different ways. For solutions that send one message for each receiver, the actual receiver should be visible to enhance communication trace in a situation. For solutions that send one message to all receivers (i.e. a list of different receivers) it is recommended that the "To-field" in the message do not identify each and every receiver but instead list e.g. "undisclosed list of receivers" or similar. The reason behind this recommendation is that there is no well founded justification to disclose the identity of different receivers amongst the receivers of a message. An agreement to provide alert notifications to specific receivers in specific situations is an agreement between the provider and the receiver that should be protected with the same level of discretion as any other agreement. The actual list of receivers is still known to the provider, just with the difference that this information is not being disclosed by the provider between the different receivers.

The message is recommended to have an "easily recognizable title". It is recommended that maintenance and incident alert notifications from the same provider are easily identifiable (by title) in terms of who the provider of the message is, what type of alert it is and some form of identification. This way, a lot of information will be immediately visible to the receiver. In particular, it is important for the receiver to know the type of alert notification received (i.e. maintenance/incident) since it may be more urgent to follow up on any incident occurred than a proactive informational alert about a future planned maintenance activity. In addition, it is important that the title include some form of identification of the actual case (i.e. CaseIDxxx). This is especially important for the receiver if the receiver for instance monitor progress on more than one incident at the time. Should that occur, the receiver can keep track of incident progress on difference incidents based on the identification. This recommendation is also important for the provider, since the identification enable the provider to trace progress in incident response based on the identification. This identification is on that basis also helpful to the provider, should authorities require retrospective report on a

specific incident, the provider should be able to pull relevant documentation to produce the report efficiently by use of the identification number.

In addition to the above (ref. Table 5) generic recommendations regarding alert notification messages, some additional type specific recommendations are relevant to provide for the different types of alert notification messages, i.e. maintenance and incident. These recommendations are provided for each specific type below, followed by an additional small set of generic message relevant recommendations.

The table below list information typically relevant to include in a generic maintenance alert notification (ref. RQ1 in section 2) with a short description, followed by some textural additional information to justify its inclusion and exemplify to increase understanding.

Type	Recommended content	Description
Maintenance	Time interval	Identify maintenance window, i.e. date and time interval for when the maintenance task is to be performed (e.g. dd.mm.aaaa during the time period 02:00-06:00).
	What	Clearly state what maintenance activities are planned performed during the stated time interval
	Consequence	If known, clearly state any adverse consequences the planned activities may have on infrastructure and/or services.

Table 6: Maintenance alert notification message

In addition to the alert generic content recommendations provided in Table 5, the above Table 6 includes maintenance alert notification message content recommendations. It is recommended that the maintenance alert notification message clearly identifies the time interval (i.e. by date and time) of which the planned maintenance activity is to be performed. In addition, the message should state what type of maintenance activity that is planned to take place (e.g. update, equipment exchange etc.) and inform about any adverse effects that may be experienced while the maintenance activity is being executed. When it comes to consequences, these should be clearly stated if known, but only vaguely stated if not clearly known. I.e. some changes such as for instance exchange of equipment will for instance require the old equipment to be taken out of service and a “hot swap” may not be possible. In such a case it is known that some equipment will have to be taken down (i.e. result in services unavailable) and be replaced with other equipment (i.e. result in services again available). When such “easily predictable consequence” changes are planned, the stated consequence can be made quite clear accordingly (i.e. this will make the services unavailable while the maintenance activity is being performed). In other cases, a planned maintenance activity may have no or little effect (in terms of adverse consequences), yet one does know that any maintenance activity could possibly have adverse effects (even if not specifically known for the planned maintenance task). In such cases it may be proactively correct to inform about consequences in a more vague way (e.g. service availability and stability may be reduced while the maintenance activity is performed). By making some sort of statement regarding time interval, task to be performed during that time interval and inform about (possible) consequences, the receiver has the ability to plan own activities accordingly. At the same time (provided that maintenance tasks are completed successfully according to plan), the maintenance executing team and the change managers are sheltered from having to respond to questions about what is ongoing, and can focus efficiently on the maintenance task at hand. In addition to what has already been mentioned it may be relevant to include some response control information in the alert notification message as further outlined below (ref. R3.1 in Table 8).

In some cases, a planned maintenance task may not execute in accordance with plan and could then become an incident. In such a case, that should trigger incident response and corresponding incident alert notifications. Together with alert notification generic recommendations in Table 5 above, the table below provides the complete list of content recommendations relevant to incident alert notification messages (ref. RQ1 in section 2). Recommendations are listed with a short description, followed by some textural additional information to justify its inclusion and exemplify to increase understanding.

Type	Recommended content	Description
	Type of alert with case number reference	Clearly identify (with reference to case Case IDxxx) what type of incident alert notification the message is, i.e. new, update or closure.
	Consequence	Describe the consequences of the incident occurred, i.e. how affected parties may experience the known incident being worked on to resolve.
	Expected correction time	Clearly state expected correction time (i.e. expected time until consequences are reduced back to "normal operation" and alert notification can be closed). If this (e.g. due to unknown cause) is uncertain, it is better to early set quite some time and then rapidly reduce time based on increased knowledge. An alternative may be to state expected correction time to "unknown" for a while and update based on new gained knowledge.
	Detection time	Time of incident detection
	Mitigations implemented	Inform about actions taken to mitigate the situation and bring situation back into normal operation. This could include actions in a broad aspect, e.g. technological, procedural, organizational actions etc.
	Cause	As soon as the cause of the incident is known, clearly state it.
	Additional info	It is recommended to have some room for additional information in the incident alert notification message. This additional information may include information such as: - when to expect incident alert notification update - suitable response control information (ref. R3.1 in Table 8)

Table 7: Incident alert notification message

In addition to the alert generic content recommendations provided in Table 5, the above Table 7 includes incident alert notification message specific content recommendations. Note that the Table 7 recommended identification of incident alert type differs from type reference in message table (ref. Table 5) which relates to alert type (i.e. maintenance/incident). Table 7 recommended type identification relates to incident alert type. I.e. if the incident alert notification is new (first alert notification of a new incident), an update (updated information about a previously alert notified incident) or a closure (alert notification to inform that the incident is adequately mitigated and alert notification for the incident will be closed/stopped). As long as the incident is identified (e.g. CaseIDxxx) as recommended in the message title (ref. Table 5), the here mentioned incident identity reference can be argued covered but depending on the content structure of the message it may also be relevant to include the identity reference with this type information. The incident alert notification type information makes it easier for the receiver to determine if the received alert is related to a new (previously not known) incident, if it is an update about a known incident or if it is a closure (both updates and closure information is relevant for the receiver to make more correct decisions on their own, e.g. related to own ability to endure

situation until new information can be provided or if alternative measures have to be initiated).

It is also recommended to include updated information about consequences. This part of the incident alert notification message can in some cases be quite challenging. It is, however, important to create a good decision basis for the receiver by being as accurate as possible in consequence description. The challenge relates to the fact that the incident response team most often responds to some sort of event/failure/alarm/incident reported by some element within the infrastructure. This "issue" has to be "translated" into actual experienced consequence (e.g. unstable service, unavailable service, etc.) to make any sense as a decision making basis for the alert notification receiver. That requires an efficient consequence analysis to be performed since time is of the essence. It may be ok to state consequence as "unknown"/"uncertain" in the early stages of incident response, but that will make any receiver uncertain and could result in increased pressure upon customer front end with questions regarding experienced affects (which may not even correspond to the incident in question and as such may become "red herring confusions" unnecessary delaying the team's actual response). A described consequence ease the receivers ability to recognize received incident alert notification to any experienced abnormalities and as such may contribute to reduce the pressure upon customer front end. With the received information the receiver may be fine (at least until further) and as such can focus effort on other more prominent tasks at hand. It is recommended that consequence description is updated in accordance with implemented mitigations (to clearly indicate that implemented mitigations have an effect on the incident consequence, i.e. constantly reducing it until alert notification can be notified "adequately mitigated to be closed").

Timing is of essence, both for the provider and any affected parties, when it comes to incident response. It is therefore recommended that the incident alert notification message includes both detection time (i.e. time of incident detection) and expected correction time (i.e. the estimated time set as to when the incident is expected resolved/adequately mitigated). It should be noted that for affected parties, expected correction time is of essence in terms of providing them with a good basis to make correct decisions on their own. As previously mentioned, affected parties ability to endure an incident situation will be individual and as such, updated incident alert notifications can be a great contribution towards the decisions they will have to make in terms of how to handle the situation based on known progress. In the overall evaluation of endurance, the noted incident detection time (together with the expected correction time) is important to the receiving party. A situation where incident alert notifications constantly extend the expected correction time of an incident creates receiver uncertainties which the provider should seek to avoid. If expected correction time has to be extended due to new information about the incident, this should preferably be supported by some logical justification in the alert notification. E.g. due to a changed cause (what was first defined to be a cable breach was in fact a cable weakness, possibly requiring more work to be properly corrected than a simple cable splice). Note that in some cases early in the process of incident response, the actual expected correction time may be relatively difficult to determine. It should however be required to include an expected correction time. That does however not disqualify the one preparing the alert notification to make some comment about any uncertainty related to expected correction time, as long as such a note is also updated (preferably the time is then set with a higher level of confidence) in later alert notification updates for the incident. From the alert notification receiver's point of view, the provider is expected to have expertise and experience enough to be quite correct in their estimation of expected correction time. Errors may be justifiable based on logical reason from time to time, but a provider who is steadily quite correct in their stated

expected correction time will provide the alert notification receiver with predictability in a less predictable situation and as such build important trust.

It is recommended to include updated information about implemented incident mitigations in incident alert notifications. This provides visibility in terms of showing incident response progression and shows that the team is actively working to mitigate consequences of the incident occurred. When it comes to alert notification updates it is important to show progression in this area, even if showing that progression may be to "provide less good news" (e.g. previous implemented mitigation informed about is found not to work as well as intended, additional/other mitigations are being implemented to counter this). Such "less good news" could also be "valid" justification for a changed expected resolution time, as long as it does not happen too often since such changes are of high importance to the receiver's decision processes and as such can contribute to reduce trust towards the provider in general.

It is recommended to include information about the cause of the incident in incident alert notifications. The importance of cause may be more relevant in keeping internal alert notification stakeholders updated, both to have a common situational overview should additional actions be required of them, but also to enable them to answer third party questions and sheltering the incident response team so that they can focus on incident solution. This being said however, it may in some cases be quite difficult to determine root cause and focus in early stages of incident response is to mitigate third party experience consequence (e.g. by re-routing traffic within the infrastructure etc.). This way, the actual root cause may not be known while alert notifications are issued (i.e. the team may mitigate consequences so that the incident severity can be lowered to a level where issuing of alert notifications is closed before actual cause of incident in known). I.e. third party experienced consequences are reduced and their situation returns to "normal operation" and issue of alert notifications is closed, but the incident response team continues to work to find the cause of the incident and resolve it properly (so that consequence mitigating actions can be removed and the infrastructure can be moved back into actual normal operation). If, and as soon as, it is known, however, during the course of alert notification being issued, the cause of the incident should be clearly stated in the alert notification message.

In addition to the above, it is recommended to have some room to include additional information. The information provided here can be of various types depending on the incident, but a couple of recommended additional inclusions are listed. It is recommended to include some information about incident alert update intervals. Such an inclusion should reflect internal requirements defined for alert notifications. The main aim with the recommendation to include such information is that the worst possible position for a receiving party of incident alert notifications is to be unaware about when any updates can be expected receiver (at the latest). No matter the expected correction time, should the incident be severe enough, information about expected updates can be of great value as a decision basis. The here recommended addition can be made "standard note" based on provider internal alert notification requirements, e.g.:

"Incident alert notification update will be sent upon any situational change but no later than X hours from now."

This way receiver can decide if X hours (at most) can be endured "for now" or if additional measures have to be taken immediately (even if "just in case"). In addition to the information about incident alert notification update intervals, it is recommended to include some "response control relevant information" as additional information (as outlined in relation to R3.1 in Table 8 below).

Finally, there are some generic relevant recommendations regarding alert message content in general (ref. RQ1 in section 2). These recommendations are summarized in the table below with description, followed by some textural detailed information for justification of inclusion and exemplification for increased understanding.

#	Recommendation	Description
R3.1	Include suitable response control	It is recommended that the ability to respond to alert notification messages is removed (and informed about). Further it is recommended to accompany this with the inclusion of suitable response control (i.e. controlled path of communication in terms of providing the receiver with a point of contact).
R3.2	Ensure only fact based content is included	It is important to make sure that the alert notification message is based on pure facts (i.e. no subjective opinions, just pure facts and nothing that could sound like a "blame" orientation for justification purposes). Anything other than wording based on pure facts have a tendency to "not sit well" with receivers and the receivers interest is merely facts.
R3.3	Content structure	The defined list of different types of stakeholders and their description (ref. R1.5, Table 3, section 4.2.1) should provide some insight into alert notification message receiver's expectations. This, combined with feedback (ref. section 4.2.4) should provide a good basis to structure content based on receiver's expectations (i.e. easy to read/get an overview of with the most important information first). Note that some may have third party requirements (e.g. from authority guidelines/SLA) that goes into this level of detail although such should be avoided as far as possible so that the provider can structure content in the standardized manner found most suitable by the provider.
R3.4	Alert notifications content quality control	Alert notifications (in general but specifically in relation to external receiving stakeholders) should be quality controlled. A rule of thumb in this relation is that there should be no unacceptable risk involved, should the content of the alert notification be "first page news" in the newspapers the following day. If that is not the case, content should be adjusted accordingly.
R3.5	Utilize available, relevant guidelines and knowledge for support	Guidelines regarding content do exist to some extent, such as this one and guidelines provided by authorities when an organization is required by law to alert notify authorities. In addition it is recommended that organizations, as far as practically possible, seek to more openly share their knowledge and experience with alert notifications with other organizations to commonly increase each other's knowledge basis on the topic.
R3.6	Adapt language to target audience	Messages are most often intended to create a common situational awareness and be a basis for decision making. Use a terminology and language that is suited for the audience (e.g. managers, customer front end, authorities etc.) and as far as practically possible avoid provider internal and/or low level technical terms and abbreviations.

Table 8: Additional alert notification message recommendations

In relation to the generic recommendation to include suitable response control, this is relevant to remain in communication control when performing alert notifications. Normal human reaction (unless informed otherwise) in a situation where for instance an alert notification message is received, is to try to respond to it if the receiver has additional questions. If that opportunity is unavailable, the receiver will typically contact whatever contact point the receiver finds "most likely to be able to provide some answers". The receiver's chosen point of contact may not be the point of contact of which the provider would like the receiver to use. To avoid these situations it is recommended to include some additional information in terms of a contact point the receiver may utilize if the receiver has additional questions related to the received alert notification. Here it is also important to note that in some cases the provider may be bound by requirements detailing the structure and content the alert notification is expected to include (e.g. third part requirements from authorities, defined in SLA or similar). The provider must then decide if it is feasible to include this in general (standard for all messages) or if the requiring party should be handled differently than the others. No matter third party requirements however, it is generally recommended to include some sort of "response control information" (i.e. point of contact for questions/information requests from receivers) in the alert notification message.

Most other recommendations included in Table 8 above are assumed quite well described in the table. It is worth noting though in particular the importance of content structure (R3.3) and audience adapted language (3.6), which are the main recommendations relevant to control how the receivers perceive the information received. Although a lot of errors can be made in alert notifications, assuming most other recommendations are followed and tailored to the individual organization's purpose, the two here mentioned generic recommendations are recommendations were small adjustments can have quite large effects in terms of how the receiver perceives the messages.

Taking a closer look at Telenor, as the case basis (ref. RQ3) for this thesis, Telenor states to have defined the structure and content of their alert notifications based on employees experiences from alert notification in the Norwegian Army. This experience is combined with the NPTA issued detailed procedures/guidelines [10], which also contains their expectations related to alert notification message content. The NPTA guidelines are quite detailed, all the way down to specifying that the alert notification message shall provide a contact person with certain contact information, the NPTA may choose to contact if they have additional questions (ref. R3.1 in Table 8 and corresponding textural information below the table). Due to the generic lack of alert notification specific details, the recommendations in this section are heavily based upon Telenor's experience and "current way of work". As such, the recommendations may suit some communication mediums better than others, but no matter the medium chosen by an organization, the aspects included in the recommendations are accordingly relevant to consider. The wording of the recommendations has been set up with the purpose to be generic and as such possible to tailor in accordance with an arbitrary organization's defined needs and purposes.

4.2.4. Measure, justify and improve

Efficient measurements as a basis to justify invested effort in establishment and improvement, is a generic challenge we face in all aspects of our organizations these days. This is a "hot topic" one can see are being discussed in all kinds of different forums with a corresponding set of different sophisticated solutions. It is, however, one simple basis in all of these discussions. To be able to have a measurement one has to have an idea of where one wants to be (i.e. a goal) and a pretty good idea of actual status (i.e. ability to pull statistical data reports related to defined goals). For measurement purposes goal defining Key Performance Indicators (KPI) should be

defined. These are powerful tools used as indicators to measure the ability to deliver in accordance with defined goals. However, as outlined in an article by Bernard Marr [15] this year:

> *"(…) if KPIs become the goals, then they turn into toxic material that will inhibit performance improvement."*

Requirements defined for alert notifications (ref. R1.3, Table 3 in section 4.2.1) are typical input that can be utilized as alert notification goals. Corresponding KPIs are recommended defined to measure the organization's ability to deliver in accordance with their own goals. Alert notification goals should (as requirements) be tied into alert notification purposes, and as such be founded towards the organization's main business objectives. The list below contains a generic but alert notification topic specific set of suggested elements (ref. RQ5 in section 2) that, depending on the organization's defined requirements, can be converted into KPIs for measurement reasons. The following list is not to be viewed as any complete list covering all interesting measurement aspects for all organizations, but is a set of suggestions that typically will be a relevant basis to consider for organizations in general:

- ***Proactive maintenance alert notifications issued in accordance with time requirements?***
  As previously mentioned it is recommended that the organization has a requirement as to how early (i.e. prior to a planned maintenance activity) a proactive alert notification is issued. A KPI should be defined for the organization to pull statistics at certain time intervals showing how many (of all issued) maintenance alert notifications where sent within their time requirements. Deviations (or unexpected large deviations based on experience) can be looked into in more detail with aim of future improvement.

- ***Maintenance activities completed successfully within alert notification defined maintenance window?***
  As previously outlined, maintenance alert notifications define the time window of which maintenance activities are planned completed. A KPI should be defined for the organization to be able to pull statistics at certain time intervals showing how many (of all alerted and executed) maintenance activities that were actually successfully completed within the defined time window. Deviations (or unexpected large deviations based on experience) can be looked into in more detail with the aim of future improvement.

- ***Planned maintenance activities that turned into incidents?***
  Planned maintenance activities may sometimes not complete successfully and in such situations unsuccessfully completed planned maintenance may turn into incidents that require incident response and corresponding incident alert notification if determined severe enough. A KPI should be defined for the organization to be able to pull statistics at certain time intervals showing how many of all completed planned maintenance activities turned into incidents. One would typically not want to have any planned maintenance activities turn into incidents, but if they do those activities should be looked into in more detail with the aim of future improvement.

- ***New incident alert notifications issued within time requirement from detection?***
  As previously outlined, time is of special essence when incidents occur. It is recommended that the organization has a requirement as to how soon after detection the first alert notification is expected to be issued (assuming the incident is classified critical enough to require alert notification issued). A KPI

can be defined to allow for the organization to pull statistics at certain time intervals to find out how many (out of all issued incident alert notifications) where issued within the expected time interval. Deviations (or unexpected large deviations based on experience) can be looked into in more detail with the aim of future improvement.

- ***Update incident alert notifications issued at least within defined time interval?***
  As previously outlined, incident alert notification updates are recommended issued at every change in the situation or at least within a specific time interval defined by the organization. The reason for this is to provide predictability in terms of knowledge on expected updates for the receiving party. A KPI can be defined allowing for the organization to pull statistics at certain time intervals to find out how many (out of all issued updates) where issued within the least defined update interval. Deviations (or unexpected large deviations based on experience) can be looked into in more detail with the aim of future improvement.

- ***Incident alert notification closed within first defined expected correction time?***
  As previously outlined, the incident alert notification included information about expected correction time is important in terms of the alert notification receiver's decision basis. A KPI can be defined allowing for the organization to pull statistics at certain time intervals to find out how many (of all issued incident alerts) changed first defined expected correction time (typically extended it) throughout the process of incident resolution (i.e. in update messages sent between the first issued incident alert notification and the incident alert notification closure message). Deviations (or unexpected large deviations based on experience) can be looked into in more detail with the aim of future improvement.

- ***Precision in incident classification level definition?***
  As previously mentioned, the ability to correctly classify incident severity is important to ensure correct prioritization and efficient incident handling. Assuming the organization is working (as recommended) based on a clearly defined incident classification regime a KPI could be defined to provide relevant measurements in relation to accuracy. For instance the organization could pull statistics to show how many (out of all) recorded incidents had the incident classification level changed and how many times was it changed during the incident response process. Note that depending on the "way of work" within the organization, it is typically normal for the classification level to change during incident response process. It may, however, not be normal that it changes very many times for instance during a period of alert notification (i.e. several classification level changes between first issued alert notification, its following updates and alert notification closure message). If a KPI taking corresponding incident alert notification into account is defined, this may provide a more correct indication as to the team and its ability to accurately classify incidents. Any deviations (or large deviation based on experience) can be looked into in more detail with the aim of future improvement.

- ***Stakeholder's made able to utilize alert notifications in accordance with its defined purpose?***
  A lot of measurements can often be pulled as statistics from different types of support systems, but in that mix it is important not to forget the most important part of this equation, i.e. the stakeholders. When the organization actually makes an effort in the establishment and improvement of alert notifications,

feedback from the stakeholders are utterly important to justify the effort made and prioritize future improvements. KPIs can be defined to measure customer satisfaction in relation to alert notification defined purposes and deviations (unexpected large deviations) can be looked into in more detail with the aim of future improvement. E.g. does the provided alert notifications actually provide the receiver with a common situational awareness to the level intended and does it in fact provide the stakeholder with a better basis to make own decisions? The indicators to measure will depend on the individual organization's defined purpose for alert notification, but there is little (or nothing much) that can justify any effort made if the provided alert notification is not viewed to be a value adding addition to the stakeholders receiving them. It may be recommended to approach the stakeholder's in person through interviews or as part of normal follow up meetings (e.g. account manager's regular follow up meetings with customer/end user based on SLA) since this provides more flexibility and open up to receive information not necessarily planned for. With experience this may be supported by some regular questionnaire or others, but the topic of alert notification may not be suitable for use of questionnaires since it is important for those issuing alert notifications to get some insight in the emotional aspect of the receiver (e.g. does it make the receiver feel more confident in uncertain situations, does it make them more comfortable decision makers, does it build the required level of trust, etc.). Each arbitrary organization will have to find the way they see most suitable to get this feedback, but such feedback is crucial in terms of alert notification improvement and beneficiary effects.

For all suggestions outlined above, keep in mind that these are some suggestions which can be a basis to tailor to the needs and capabilities of any arbitrary organization. The list is not a complete list and can probably be extended quite much, depending on available capabilities within the utilizing organization. The most important thing is, though, that the KPIs the organization defines should correspond with defined alert notification requirements (i.e. different defined requirements require correspondingly different KPIs defined). In utilization of KPIs like this it is important to keep in mind that these only show a small piece of information compared to the reality [15]. Periods sometimes include the handling of more major incidents (than "usual") or more complex incidents (than "usual"), such periods will most likely be recognizable from the pulled statistics (i.e. KPIs). Such aspects should also be quite easy to determine in the process of looking into deviations in more detail with the aim of future improvement. There is however a potential for future improvement in that as well, for instance to review such special incidents for lessons learnt with the aim to handle it more efficiently should a similar incident happen later.

4.2.5. Additional basis for audit purposes

The recommendations related to alert notifications presented in the previous subsections of this section 4 are not only relevant in terms of establishment and improvement of well structured, secure and efficient alert notifications. The same set of assumptions and recommendations may also represent a beneficiary additional basis to those auditing processes that have the added feature of alert notification. It may be a beneficiary addition for audits in general, as long as the recommendations are seen as organization generic and are used as a basis, while the actual audit takes individual organizational tailoring into account.

The figure included below illustrates the potential addition the here presented recommendations can provide to an audit looking in more detail into an organizations defined procedures for business emergency preparedness.

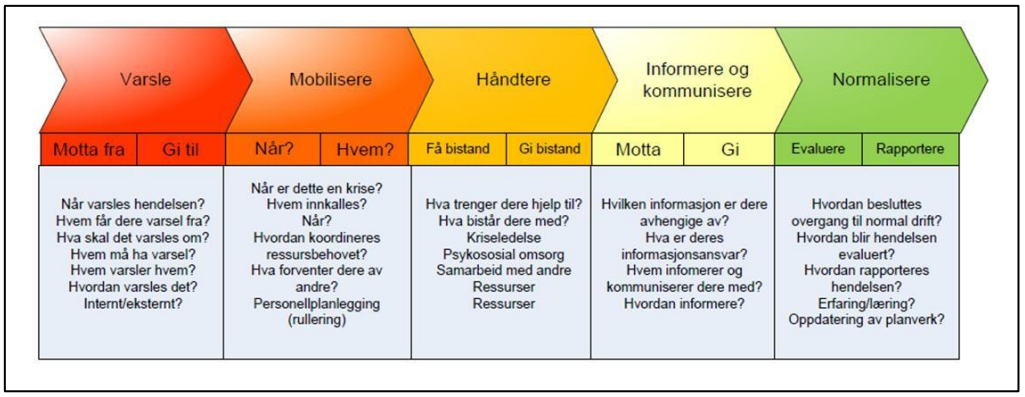

Figure 7: Alert notification audit relevant illustration [16]

Although kept unchanged (i.e. in Norwegian) as provided by a third party experienced auditor, the above illustration provides a simplified overview on the aspects the audit typically covers in a business emergency preparedness audit. The top, left, first block in the presented series of blocks in Figure 7 above adheres to the aspect to alert notify (i.e. "varsle" in Norwegian). The above illustrative figure shows that the audit typically concentrates on aspect of alert notifications in terms of received alert notifications and alert notifications to be forwarded to others. This is looked at in further detail based on different relevant aspects visualized through a small list of relevant questions, which for the block "alert notify" (Norwegian: "varsle") translates as follows:

- When is the incident alert notified?
- Who alert notifies you?
- What shall be alert notified?
- Who must be alert notified?
- Who alerts who?
- How do you alert notify?
- Internal/external?

The above clearly shows that the first block in the audit illustration is alert notification oriented. An organization who has established alert notification in accordance with this thesis defined recommendations, will have well documented and quite clear answers to most of the more "high level" questions of an audit as illustrated above. At the same time, to increase level of detail of the audit, an auditor may choose to improve the auditors own audit procedures by adding relevant alert notification elements from the here presented generic set of recommendations. Due to the current lack organization generic, but alert notification specific, standards/"best practices"/guidelines etc., the here presented generic set of recommendations could be tailored not only for use in arbitrary organizations to establish and improve alert notification. It could also be tailored and utilized as the auditor may see relevant, as a beneficiary addition to their own established audit procedures.

To exemplify further, utilizing Telenor as this thesis case basis (ref. RQ3 in section 2), the master candidate did an evaluation of Telenor. This evaluation was performed by comparing the thesis presented set of recommendations (i.e. section 4) with information collected though interviews with different Telenor key personnel. This cannot be claimed to be an actual audit, since an audit typically would go deeper than a simple comparison if potential weaknesses were seen, to determine actual weakness. The actual evaluation results are not included in this thesis in detail, since it contains business confidential information and details that could make it impossible to publish the thesis. For the purpose of exemplification, however, the following high level summary of the overall evaluation results can be shared:

- This thesis is heavily based on Telenor and as such, several aspects were found to be adequately covered in the evaluation. Aspect related to assumptions and message content as recommended was quite adequately covered, only with some recommendations to consider a few adjustments.
- Main possible weaknesses recommended for Telenor to re-evaluate to determine if actual or not, was typically found in relation to "level of formality of things". I.e. the clarity relevant aspects of preparation and solution recommendations were documented. In addition, several aspects related to measurement, justification and improvement were highlighted as relevant to consider for implementation and/or improvement to make Telenor alert notifications even more structured, secure and efficient.

Appendix 2 provides a copy of the basic audit metric the master candidate made as a basis to perform the Telenor evaluation, which can be a useful tool for others to get an overview for more in depth audit of current alert notification solutions. The above summarized high level results show that the complete result of this thesis (section 4) can be used as a beneficiary basis, not only to support the novice to the thesis topic, but also to evaluate and improve those regarded highly experienced and mature in alert notifications (ref. RQ5 in section 2).

5. Discussion of applied methodology and results

This section discuss the thesis applied methodology and its validity, opportunities for replication, potential weaknesses and lessons learnt. This is discussed in relation to the presented results in terms of its ability to resolve defined main problem statement and corresponding research questions (as outlined in section 2), its level of usability and generalization. The discussion also covers a broader discussion in relation to alert notifications including some aspects of adverse effects "not so structured, secure and efficient" alert notifications may have upon the utilizing organization.

The lack of alert notification specific relevant elements to be found and utilized in different literature, "best practices" and standards, led to an early acknowledgement that large parts of this thesis had to rely upon Telenor available knowledge. Although Telenor is regarded an experienced and mature user of alert notifications, this could affect the validity [5, Chapter 4, page 101, "Considering the Validity of Your Method"] of the research project as a whole (i.e. its accuracy, meaningfulness and credibility). The same lack of alert notification specific available information verified the thesis applicability and meaningfulness. This enhanced the importance of utilizing Telenor as a case basis for the thesis to increase its general credibility.

The qualitative approach [5, Chapter 6, page 140] chosen with the aim to be descriptive (i.e. reveal the multifaceted nature of alert notifications as a topic) and interpretative (i.e. allow for the researcher to gain insights into alert notification as a topic), was necessary to allow for the candidate to resolve the main problem statement of the thesis (i.e. provide an organization generic but topic specific set of recommendations).

The large number of interviews (15) performed by the master candidate interviewing different interview subjects in the first third of the project period, resulted in a huge amount of relevant input of different aspects that had to be "digested" by the candidate. The interview type chosen (i.e. quite open ended but with different semi-structured follow up questions, ref. section 3), is quite challenging and its output quality rely a lot upon the interviewers skills and abilities. The method, however, provided the high level of flexibility relevant to reach the main purposes of the interviews (ref. section 3). At the same time it provided relevant information not necessarily asked for, even if there were certain disadvantages in the fact that the results (i.e. recorded minutes) were not directly comparable. The candidate did, however, ask follow up questions and had discussions with the thesis external supervisor (Telenor), to clarify instances where interview results seemed to be in direct conflict. All in all, the chosen method had disadvantages and relied much upon the skill and ability of the interviewer. The risk in this relation, however, was deemed reduced, given the method's similarity to the approach taken by skilled sales and advisory representative in the field, an area the master candidate has 12 years of working experience from.

The fact that recorded minutes of the interviews are not included in full in this thesis, may be viewed to be a weakness in terms of this thesis opportunities for replication. I.e. it may be considered more difficult for a peer to perform a series of similar interviews and get to the same result as this thesis. That may be a weakness, but compared to a result where the thesis (with the minutes included) would not be possible to publish, the actual minutes were deemed less important. In addition, given the interview type utilized, and the way the result rely on the skill and capability of the interviewer, it may also be that no matter the number of interviews performed by peers, the recorded minutes might not provide comparable results anyway.

It could have been beneficiary to have been able to show some measurements (ref. section 4.2.4) based on statistics pulled from Telenor. For instance by implementing one quite simple improvement and have "before and after" statistics to show benefit of implementation. This was discussed as a possible way to provide evidence of the "working conditions" of the results (ref. section 4) in addition to the evaluation performed by the master candidate (ref. section 4.2.5). This would, however, have required even more supporting resources from an (at times) already quite busy topic provider. That, combined with the amount of information required "digested" efficiently by the candidate, was determined to be too much of a risk. I.e. risk in terms of additional work to include within the defined scope of the thesis. Compared to the limited additional benefit it would provide, it was found too risky to try to accomplish that addition. I.e. the evidence would have been strengthening in the specific case of the results "working conditions" for the topic provider (i.e. Telenor), but not necessarily in any generalized perspective.

The complete result (ref. section 4) and its referenced literature respond quite well to the research questions (ref. section 2). Given the acknowledgement that the thesis had to rely quite much on Telenor knowledge and experience, a high level of relevance between results and RQ3 is found to be logical. With the focus specifically set to define organization generic alert notification specific recommendations, a high level of relevance between results and RQ1 is also logical. Less frequent relevance between presented results and other RQ's may be seen as a generic weakness, but based on current knowledge and applied methodology that is all in all quite logical. Through its relevance towards different RQ's, the complete set of results (ref. section 4) provides a resolution to the main problem statement defined for the thesis (ref. section 2). For eased evaluation purposes, also refer Appendix 1 that provides a metric overview of the relevance between results, the main problem statement and the different RQ's.

Telenor has already confirmed experienced benefit from providing the thesis topic and being involved as external (Telenor) supervisor. Through performed evaluation activities (refer section 4.2.5), the master candidate has confirmed benefits in relation to utilize the provided set of recommendations from an auditors perspective. This, combined with the confirmed lack of alert notification specific available literature and the generically worded set of recommendations, should make it possible to generalize the results of this thesis. At least as a starting point for an arbitrary organization that wants to set focus on alert notification. Tailoring the presented generic to be organization specific and relevant is, however, a precondition for any arbitrary organization that aim to utilize the here presented recommendations successfully. Actual evidence of the thesis possibility to be generalized, can, however, only be provided through future evidence in terms of organizations tailoring the provided set of recommendations and utilize them successfully. Preferably supported by here recommended measurements made by the organization and audit results from audits conducted by objective auditors confirming it.

All this being said, note that as much as alert notifications provide incident team activities visible, it may backfire quite adversely, if done without the necessary preparation, consideration and organization awareness established. As much as alert notifications may showcase the organization professionally, it also provides visibility in situations handled not so professionally and that could backfire with adverse effects. E.g. reduced trust between the organization and its alert notification stakeholders. Yet, done with adequate level of concern and precision, the visibility can aid organization internal understanding of the incident response team and create common situational awareness for efficient utilization, should a situation escalate beyond incident response. As such, alert notification can provide a perceived value in terms of a basis for stakeholders to make more correct decisions for themselves (i.e. more correct than they would be able to make without the alert notifications). The visibility provided by

alert notifications also build a common understanding of incident response and can serve as a communication bridge between processes and their corresponding responsible (e.g. between incident and crisis manager). This visibility will also have the ability in itself to make weaknesses and bottlenecks in the traditional CM or IR and BR processes more visible and, as such, indirectly trigger or contribute to trigger improvements for these processes as well.

6. Conclusion and future research

This thesis has fulfilled its purpose to answer the main problem statement, i.e. to define a set of alert notification specific recommendations that any arbitrary organization can utilize to establish and continuously improve well structured, secure and efficient alert notifications.

Efficient communication is one of the activities humans have developed most tools to help us handle, still efficient communication seems to be one of the most difficult things we do. Looking at it from a real world example perspective, the report from the 22-07 commission of inquiry [1, chapter 9, p. 208] states that:

"Alert notification, information and communication are essentials in crisis situations."

This not too different from statements heard from several different experts in the field in different forum discussions of related topics during the last year, i.e.:

"Efficient and precise communication is a precondition for efficient incident management."

Well structured, secure and efficient alert notifications could be one major contribution to this, as a cost efficient standardized way of communication, provided that it is tailored to the capability and resources available to the organization utilizing it. Any organization may technologically have the ability to alert notify different stakeholders different ways, but it is the way it is done and the corresponding value perceived by receiving stakeholders that determines its level of success. Done well, alert notifications may for instance contribute to:

- efficiently provide an essential common situational awareness amongst many
- keep relevant stakeholders updated (and ready) should their additional action be required at any point in time
- provide an insight that allows for stakeholders to make more correct decisions (than what they would be able to do without them)
- build communication bridges between processes and those responsible for them
- create a sense of predictability in less predictable situations and, as such, increase trust between parties

All in all, alert notifications can, through increased visibility, contribute to a higher recognition of incident response team importance amongst the organization's top level managers. That could be one strong motivator for top level management anchorage, to ensure well balanced teams kept in place. I.e. balanced teams able to work smart instead of being caught in the previously mentioned work hard capability trap, that too many teams become victims of, according to current, relevant research [11]. Based on an established common situational awareness, informed, relevant stakeholders together with team managers provide a defined basis for Coherent Knowledge-based Operations (CKO) [17, chapter 16, p. 470, "Putting Knowledge Management to Practical Use"]. A term used in information warfare, transferrable into society and organizations in general, which can represent a major strength in ability and capability, should an occurred incident become severe enough to require extra ordinary handling (e.g. escalation from incident to crisis management). For organizations such as Telenor, i.e. responsible to maintain and monitor complex infrastructures vulnerable to weather conditions, predicted climate changes to expect, with steadily more extreme weather conditions, should be yet another motivator to continuously improve ability to efficiently handle incidents in general moving forward.

This thesis presented set of recommendations do not claim to be a complete set and they do require organization individual tailoring for successful utilization in

accordance with their individual defined purposes. It does, however, constitute a set of relevant, organization generic, alert notification specific recommendations. These should (at least) represent a useful basis to focus more in on the topic and the benefits that can be drawn from alert notifications, as an efficient, standardized tool of communication. It will certainly be a relevant tool for the master candidate to add to the candidate's "tool box of tools" that can be pulled out and utilized in different aspects of information security challenges in the future.

Regarding suggestions for future research, there are relevant suggestions to be made both in terms this thesis specific result and alert notifications in general. In addition, there is currently ongoing related research, which could be of interest to follow up on to find out if provided results, in any manner, can be utilized beneficiary, also in the area of alert notification.

In specific relation to this thesis result, it could be interesting to utilize the here presented set of recommendations as a audit basis to audit a set of different organizations that already have some sort of alert notification solution in use, to verify its "working conditions"[19]. This could contribute to (more accurately) determine the set of recommendations':

- Level of usability for an arbitrary organization
- Ability to be generalized
- Tailoring scalability, in relation to individual organizations available resources and capability

This thesis also finds that research regarding the topic of alert notifications is in general marginal at the moment hence any research relevant to the specific topic would be of use for stakeholders of the topic. This, when, at the same time as research is marginal, this is an area of expertise that for some organizations is required by law and most likely also useful to organizations in a much broader perspective, e.g.:

- Internally within arbitrary organizations
- Between infrastructure and service providers and their customers/end users
- Between organizations (for instance within the same industry should incidents occur that may not be organization but more industry specific) and in some such instances, possibly also relevant between industry internal organizations and their industry coordinating stakeholders (e.g. different levels of CERT organizations)

In relation to the above, and as an attempt to further boost creativity, there are some generic trends found within information security that may benefit from a more specific focus towards well structured, secure and efficient alert notification (or at least a serious consideration of possible benefit). Within information security in general, there are tendencies indicating we are moving towards a paradigm shift. This relates to forced changes in security culture, based on the evolvement of the threat perspective. For instance as outlined in the conclusion of a paper co-authored by this thesis candidate during spring of 2013 [18]:

> *"Advanced Persistent Threat (APT) is, and is expected to continue to be, one of the main driving forces, not just as a threat but also in terms of security in general. As outlined in this paper, tendencies may already indicate a forced paradigm shift in this area, by forcing changes to the security culture in general. Traditionally, information security has been something addressed privately within organizations and handled without much focus on sharing. The global*

[19] *Such an exercise could include Telenor and, as such, be a sort of "follow up" activity towards them and at the same time be an exercise in the support to share knowledge and experience between alert notification stakeholders within or across different industries.*

> *challenge of information security and the general network dependency for business continuity, combined with the global sophisticated and well organized threats, such as APT, force a whole other level of sharing. This level of sharing requires a change in how we approach information security in general and a change/adjustment of the security culture. This cultural change has been in motion for a while already in generic terms, but is forced utterly forward by APT. (...) APT is a dynamic threat which requires dynamic countermeasures depending on efficient sharing of relevant information as soon as it can be obtained. APT is a global dynamic threat which requires the corresponding global dynamic security countermeasures."*

One could imagine a holistic alert notification solution utilized for rapid information sharing for instance between different levels and across different types of Computer Emergency Response Teams (CERT, e.g. corporate sector, regional, national etc.). This could for instance be argued to reduce the risk of misunderstandings through the use of short, standardized text messages. The solution could be argued to enhance communication and response control through rapid, continuous share of important information about incidents occurred and the resolution progress, creating common situational awareness between CERTs. The aim of such an approach would be to ensure common situational awareness and updated insight in progress, through a standardized format, to reduce risk of misunderstandings. Such an approach would not be too different from the current drive within the aviation industry to innovate Air Traffic Communication (ATC) with Controller Pilot Data Link Communication (CPDLC) [19]. CPDLC is to be implemented to support voice communication between controllers and airplanes with text messages during flight, to increase Air Traffic Management (ATM) capacity by automating routine tasks whilst improving safety.

Opportunities to find alert notification relevant topics to research are many and most results would be of some contribution to stakeholders of the topic. Currently the potential for beneficiary use of alert notification is broad. Any research that could provide some direction, e.g. towards what alert notifications most likely would be beneficiary for and what it might not be as beneficiary for, would be of great value to those looking more closely into opportunities to utilize it.

This thesis mention getting from a system generated failure message to a description of actual experienced consequences of it as quite challenging. This is typically a challenge that increase with the level of complexity monitored (i.e. the infrastructure and services monitored by Telenor Operations is typically quite complex in this sense). When one issue happens in such an infrastructure, that most often create a flood of messages towards those monitoring the infrastructure. Any tool that can be able to rapidly not just sort the flood of incoming messages reasonably well, but also provide an overview of experienced consequences, would be of great value. In relation to this type of challenges, several ongoing projects that relate to efficient big data analysis (e.g. based on decision theory), may be found possible to utilize to better handle this challenge as well (i.e. even if it is made for other purposes, there may be ways to adjust it for the purpose of consequence visualization or visualization of alternative consequence scenarios, depending on incident behavior over time and the corresponding response efficiency). Done accurately and faster, this could improve the early decision basis available to the operation/incident manager and corresponding decision certainty quite much. In addition, several ongoing research projects on related topics such as smart emergency response (e.g. Norwegian SmartEMIS [20], American SERS [21], GSMA Smart City Resilience [22] etc.), may be interesting to follow up in terms of results, to determine of these could be of interest to utilize in alert notification improvement efforts.

7. Bibliography

[1]A. B. Gjørv et al (2012), *"Report from the 22-07 commission of inquiry"*, NOU 2012:14, ISSN: 0333-2306, ISBN: 978-82-583-1148-2

[2] M. E. Whitman and H. J. Mattord (2007), *"Principles of incident response and disaster recovery"*, ISBN-13: 978-1-4188-366-4, ISBN-10: 1-4188-3663-x

[3] M. Ask (2013),*"Well structured, Secure and Efficient Alerting Systems"*, Master's Thesis Project Description delivered in IMT4601 "Research Project Planning" at GUC, Well_Structured_Secure_and_Efficient_Alerting_Systems_Merete_Ask.pdf

[4] Samferdselsdepartementet, FOR-2004-02-16-401, *"Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)"*, available at: http://lovdata.no/dokument/SF/forskrift/2004-02-16-401?q=ekomforskriften*, URL visited and verified working (May 2014)

[5] P. D. Leedy and J. E. Ormrod (2011), 10th ed., *"Practical Research planning and design"*, ISBN-13: 978-0-13-289950-5, ISBN-10: 0-13-289950-7

[6]Wikipedia about Information Technology Infrastructure Library (ITIL), available at: http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library, URL visited and verified working (May 2014)

[7] M. Onstad et al (2013), *"Major Incident Management - Hvordan håndtere kritiske hendelser, en samling med erfaringer og tips fra Operasjonsledelsen i Telenor"*

[8] ITIL life cycle illustration from Modalisa-Technology, available at: http://www.modalisa-technology.com/competencies/maturity-models/itil/, URL visited and verified working (May 2014)

[9] ENISA (2010), *"Good Practice Guide for Incident Management",* available at: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management, URL visited and verified working (May 2014)

[10] The Norwegian Post and Telecommunications Authority's defined requirements for alert notifications and reporting of incidents in the e-communication network, available at: http://www.npt.no/teknisk/sikkerhet-og-beredskap/kriseh%C3%A5ndtering/varsling-og-rapportering-av-hendelser-i-ekomnett, URL visited and verified working (May 2014)

[11] N. P. Repenning and J. D. Sterman (2001), *"Nobody Ever Gets Credit for Fixing Problems that Never Happened: Creating and Sustaining Process Improvement"*, California Management Review vol. 43, no. 4

[12] X. Su (2006), *"An Overview of Economic Approaches to Information Security Management"*, Technical Report TR-CTIT-06-30, University of Twente

[13] A. Boin et al (2013), *"The Politics of Crisis Management, Public Leadership under Pressure"*, ISBN: 978-0-521-60733-9, Cambrige University Press

[14] A. L. Barabási (2003), *"Linked, How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life"*, ISBN: 978-0-452-28436-5

[15] B.Marr (2014), *"Caution: When KPIs Turn Into Poison"*, available at: http://www.linkedin.com/today/post/article/20140324073422-64875646-caution-when-kpis-turn-to-poison?trk=vsrp_influencer_content_res_name&trkInfo=VSRPsearchId%3A7481276414011929663 44%2CVSRPtargetId%3A585178526577736089 6%2CVSRPcmpt%3Aprimary,
URL visited and verified working (May 2014)

[16] Business Emergency Preparedness Audit Overview illustration, illustration provided and approved included in thesis for illustrative purposes by Eliin Rødal (Feb2014), Senior Security Advisor at Safetec Nordic AS (an ABS Group Company; www.safetec.no)

[17] A. Jones et al (2002), *"Global Information Warfare – How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages"*, ISBN 0-8493-114-4, Auerbach Publications

[18] M. Ask et al (2013),*"Advanced Persistent Threat (APT) Beyond the hype"*, delivered in IMT4582 "Network Security" at GUC.

[19] Eurocontrol's short description of their LINK 2000 + programme, available at: http://www.eurocontrol.int/services/link-2000-programme, URL visited and verified working (May 2014)

[20] Description of the Norwegian SmartEMIS research project, available at: http://ciem.uia.no/project/smartemis--smart-emergency-management-information-systems, URL visited and verified working (May 2014)

[21] Description of the American SERS research project, available at: http://smartamerica.org/teams/smart-emergency-response-system-sers/, URL visited and verified working (May 2014)

[20] Description of GSMA Smart Resilience City research project, available at: http://www.gsma.com/connectedliving/wp-content/uploads/2013/02/cl_SmartCities_emer_01_131.pdf, URL visited and verified working (May 2014)

Appendix 1: PS, RQ and result coupling

RESULTS AND PS/RQs COUPLING		
The thesis section 4 presented results provide a set of assumptions, recommendations and suggestions as summarized in this table. The complete set of presented results resolve the main problem statement (PS) as defined in thesis section 2. The presented results refer the thesis section 2 defined RQ's (RQ1-5) as found suited where the presented contributes to resolve an RQ. The table below presents a summary of the results and the corresponding RQ's referred for different parts of the results in section 4. This metric is set up to provide an overview for eased evaluation of this thesis, in terms of a summarized overview on the coupling between presented results and its corresponding RQ resolution contribution.		
ASSUMPTIONS		
#	**Assumption**	**Relation between assumptions and RQs**
A.1	IR and BR processes are in place	RQ1, RQ2, RQ3
A.2	CM processes are in place	RQ1, RQ2, RQ3
A.3	Alert notification provision tool is available	RQ1, RQ3, RQ4
A.4	Alert notification trigger is in place	RQ1, RQ2, RQ3
A.5	Ability to tailor generic recommendations to the need and purpose of the organization.	RQ1, RQ3
PREPARATIONS		
#	**Recommendation**	**Relation between recommendations and RQs**
R1.1	Define the main purpose of alert notification aligned the organization's main business objectives.	RQ1, RQ2, RQ3
R1.2	Identify alert notification triggers in current processes	RQ1, RQ2, RQ4
R1.3	Define alert notification requirements relevant to fulfill its purpose	RQ1, RQ2, RQ3, RQ5
R1.4	Define alert notification relevant roles with descriptions.	RQ1, RQ2
R1.5	Identify and describe alert notification stakeholders relevant to its purpose.	RQ1, RQ3, RQ5
ALERT NOTIFICATION SOLUTION		
#	**Recommendation**	**Relation between recommendations and RQs**
R2.1	Maintain and control the list of alert notification stakeholders (i.e. receivers) continuously.	RQ1, RQ2, RQ4
R2.2	Avoid serial processing as far as practically possible.	RQ1, RQ3
R2.3	Automate for increased efficiency, where found possible.	RQ1, RQ3
R2.4	Operate based on a clearly defined regime for incident classification.	RQ1, RQ2, RQ3
R2.5	Operate under strict change control.	RQ1, RQ3

ALERT NOTIFICATION MESSAGE (Message type: M= Maintenance, I= Incident)		
Type	**Recommended content**	**Relation between recommendations and RQs**
M&I	From	RQ1, RQ2, RQ3
	To	RQ1, RQ2, RQ3
	Title	RQ1, RQ2, RQ3
M	Time interval	RQ1, RQ3
	What	RQ1, RQ3
	Consequence	RQ1, RQ3
I	Type of alert with case number reference	RQ1, RQ2, RQ3
	Consequence	RQ1, RQ2, RQ3
	Expected correction time	RQ1, RQ2, RQ3
	Detection time	RQ1, RQ2, RQ3
	Mitigations implemented	RQ1, RQ2, RQ3
	Cause	RQ1, RQ2, RQ3
	Additional info	RQ1, RQ2, RQ3
#	**Recommendation**	**Relation between recommendations and RQs**
R3.1	Include suitable response control	RQ1
R3.2	Ensure only fact based content is included	RQ1, RQ3
R3.3	Content structure	RQ1, RQ2, RQ3
R3.4	Alert notifications content quality control	RQ1, RQ3
R3.5	Utilize available, relevant guidelines and knowledge for support	RQ1, RQ2
R3.6	Adapt language to target audience	RQ1, RQ3
MEASURE, JUSTIFY AN D IMPROVE		
#	**Suggestions**	**Relation between suggestions and RQs**
1	Proactive maintenance alerts issued in accordance with time requirements	RQ1, RQ2, RQ3, RQ5
2	Maintenance activities completed successfully within alert notification defined maintenance window?	RQ1, RQ2, RQ3, RQ5
3	New incident alert notifications issued within time requirement from detection?	RQ1, RQ2, RQ3, RQ5
4	Update incident alert notifications issued at least within time defined interval?	RQ1, RQ2, RQ3, RQ5
5	Incident alert notification closed within first defined expected correction time?	RQ1, RQ2, RQ3, RQ5
6	Precision in incident classification level definition?	RQ1, RQ2, RQ3, RQ5
7	Stakeholder's made able to utilize alert notifications in accordance with its defined purpose?	RQ1, RQ2, RQ3, RQ5

Appendix 2: Basic audit metric

The metric presented below is an example of the metric the master candidate prepared to utilize for audit purposes. The metric contains all assumptions and recommendations provided as a thesis result in this thesis section 4 summarized, with an added column to include audit comments for each of them.

ASSUMPTIONS		
#	**Assumption**	**Audit comment**
A.1	IR and BR processes are in place	
A.2	CM processes are in place	
A.3	Alert notification provision tool is available	
A.4	Alert notification trigger is in place	
A.5	Ability to tailor generic recommendations to the need and purpose of the organization.	
PREPARATIONS		
#	**Recommendation**	**Audit comment**
R1.1	Define the main purpose of alert notification aligned the organization's main business objectives.	
R1.2	Identify alert notification triggers in current processes	
R1.3	Define alert notification requirements relevant to fulfill its purpose	
R1.4	Define alert notification relevant roles with descriptions.	
R1.5	Identify and describe alert notification stakeholders relevant to its purpose.	
ALERT NOTIFICATION SOLUTION		
#	**Recommendation**	**Audit comment**
R2.1	Maintain and control the list of alert notification stakeholders (i.e. receivers) continuously.	
R2.2	Avoid serial processing as far as practically possible.	
R2.3	Automate for increased efficiency, where found possible.	
R2.4	Operate based on a clearly defined regime for incident classification.	
R2.5	Operate under strict change control.	
ALERT NOTIFICATION MESSAGE (Message type: M= Maintenance, I= Incident)		
Type	**Recommended content**	**Audit comment**
M&I	From	
	To	
	Title	
M	Time interval	
	What	
	Consequence	
I	Type of alert with case number	

	reference	
	Consequence	
	Expected correction time	
	Detection time	
	Mitigations implemented	
	Cause	
	Additional info	
#	**Recommendation**	**Audit comment**
R3.1	Include suitable response control	
R3.2	Ensure only fact based content is included	
R3.3	Content structure	
R3.4	Alert notifications content quality control	
R3.5	Utilize available, relevant guidelines and knowledge for support	
R3.6	Adapt language to target audience	
MEASURE, JUSTIFY AN D IMPROVE		
#	**Suggestions**	**Audit comment**
1	Proactive maintenance alerts issued in accordance with time requirements	
2	Maintenance activities completed successfully within alert notification defined maintenance window?	
3	New incident alert notifications issued within time requirement from detection?	
4	Update incident alert notifications issued at least within time defined interval?	
5	Incident alert notification closed within first defined expected correction time?	
6	Precision in incident classification level definition?	
7	Stakeholder's made able to utilize alert notifications in accordance with its defined purpose?	