NTNU

Norwegian University of
Science and Technology

Digitalization of Exams

A study of how digitalization can improve the examination processes at NTNU

Jonathan Brusch N Trapnes

Master of Science in Computer Science
Submission date: August 2017
Supervisor: Guttorm Sindre, IDI

Norwegian University of Science and Technology
Department of Computer Science

Jonathan Brusch Nielsen Trapnes

Digitalization of Exams

- A study of how digitalization can improve the examination processes at NTNU

Master thesis in Digital Enterprise Development

Asker, August 2017

Supervisor: Guttorm Sindre

Norwegian University of Science and Technology

Faculty of Information Technology and Electrical Engineering

Department of Computer Science

This page is intentionally left blank

ABSTRACT

Digital examination and assessment are increasingly sought after in tertiary education. Due to new technological innovations and new requirements from both the society and the stakeholders associated with the digital examination process, we see a shift in universities trying to acquire the technology to support a digital process. The educational landscape in Norway is in transformation, where different universities are in different stages of the process of digitalizing the complete assessment process.

At NTNU, the predominant form of examination is the traditional pen and paper exam. The exam is typically taken in proctor controlled environments. When we want to transform the paper system we cannot simply put it into a digital solution and expect everything to be as wanted. The processes need to be reengineered, and accepted by the stakeholders. When the reengineering takes place, we need to maintain the core activities. In this thesis, we will see how digitalization can support process improvement through i.e. simplification, exclusion, and automation of current processes.

With a digital exam comes a digital solution. This solution needs to be secure and robust, especially since new technology means new ways of exploiting vulnerabilities. The thesis will account for several new security threats that can exist because of a digital environment, pertaining to unwanted behaviour in the form of cheating. After assessing the new threats, the reader can find proposals to safeguards that can mitigate some of these threats. As the threat picture is quite complex and vast, we want to assure the reader that this is an incomplete overview of both the security threats and countermeasures.

When transforming organizations, it is important to have a clear strategy, and align this strategy with the practices and services associated with the transformation. A strategy is the organizations way of describing how they create value. The thesis therefore presents a value creation template known as Value Proposition Design, and attempt to address how it can drive the digitalization of the process improvements.

This page is intentionally left blank

SAMMENDRAG

Digital eksamen og vurdering blir stadig mer etterspurt i høyere utdanning. På grunn av nye teknologiske innovasjoner og krav fra både samfunnet og interessentene knyttet til den digitale eksamensprosessen, ser vi et skifte i universiteter som prøver å skaffe seg teknologien for å støtte en digital eksamen. Utdanningslandskapet i Norge er i forandring, der ulike universiteter er i ulike stadier av digitaliseringsprosessen.

Hos NTNU er den dominante eksamensformen den tradisjonelle penn- og papireksamen. Eksamen er vanligvis tatt i kontrollerte miljøer. Når vi ønsker å forandre papirsystemet, kan vi ikke bare sette det inn i en digital løsning og forvente at alt skal være som ønsket. Prosessene må omstruktureres, og aksepteres av interessentene. Når omstruktureringen finner sted, må vi opprettholde kjerneaktivitetene. I denne oppgaven vil vi se på hvordan digitalisering kan støtte prosessforbedring gjennom forenkling, ekskludering og automatisering av nåværende prosesser.

Med en digital eksamen kommer en digital løsning. Denne løsningen må være sikker og robust, særlig siden ny teknologi betyr nye måter å utnytte sårbarheter på. Avhandlingen skal redegjøre for flere nye sikkerhetstrusler som kan eksistere på grunn av et digitalt miljø; sikkerhetstrusler knyttet til uønsket oppførsel i form av juksing. Etter å ha vurdert de nye truslene, kan leseren finne forslag til mottiltak som kan redusere noen av disse truslene. Ettersom trusselbildet er ganske komplekst og stort, vil vi forsikre leseren om at dette er en ufullstendig oversikt over både sikkerhetsrisikoen og mottiltakene.

Når man forvandler organisasjoner, er det viktig å ha en klar strategi, og justere denne strategien med oppgavene og tjenestene knyttet til transformasjonen. En strategi er organisasjonens måte å beskrive hvordan de skaper verdi på. Avhandlingen presenterer derfor en mal for verdiskaping, kjent som Value Proposition Design, og forsøker å redegjøre for hvordan den kan drive digitaliseringen av prosessforbedringene.

This page is intentionally left blank

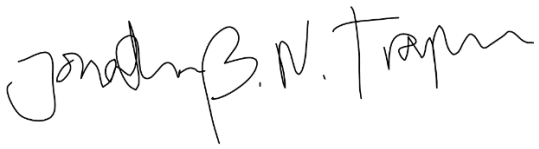
PREFACE

This paper constitutes the finalization of 19 years of schooling in the form of a Master Thesis. The Master Thesis is the culmination of the Master's degree in Computer Science offered at the Norwegian University of Technology and Science (NTNU). It is not only the completion of the degree, but a closure to 6 fantastic years of student life in the city of Trondheim.

I would like to thank my parents, all four of them, for providing support and guidance throughout the easy and difficult parts of the degree.

I would like to thank my supervisor Guttorm Sindre for giving me the opportunity to work with the interesting field that is computer security and process improvement.

Torstad, August11 2017



Jonathan Brusch Nielsen Trapnes

This page is intentionally left blank

CONTENTS

This page is intentionally left blank

List of Figures

This page is intentionally left blank

LIST OF TABLES

This page is intentionally left blank

CHAPTER 1

INTRODUCTION

This chapter presents the motivation behind the research, scope of the thesis and the outline of the thesis.

1.1 MOTIVATION

Pen and paper examinations have been used for assessing a candidate's competence since 605 AD [1]. It was adopted as a way of assessment in higher education in the beginning of the 19th century. The examination functions as a way for the students to express their knowledge of a certain subject or topic. For more than a century, written examination has been conducted with pen and paper at NTNU. During the recent decades, we have seen a rise in new technology, mainly digital technology. It permeates many aspects of our daily life. As the digital boom happened, Norwegian students and teachers began using technology more and more in their education: exercises, writing reports, delivering assignments, distributing information et cetera.

With the rise of technology, the new generation of Norwegian students and faculties have been familiarized with Learning Management Systems and using computers for most aspects of their education. As computerization has become increasingly more important for higher education, students do most of their formative coursework on computers. The digitalization of the education has been a great success, but universities and other higher education institutions are still struggling to develop a fully digitalized examination process. The predominant form of examination conducted at the Norwegian University for Science and Technology is therefore still pen and paper exams. There are several drivers for digitalization of end-of-term examinations at NTNU:

- the headmastership at NTNU want full digital assessment by 2022 [2]
- Employers and society want ICT literate graduates [3]
- Increasing number of students
- Cater to change in curriculum and expected learning outcomes. [4]
- Cost efficiency
- Resources affiliated with managing paper are released to do more value creating work

In digitalizing the assessment, the students are exposed to more relevant and realistic tools and ways of working than an ordinary pen and paper exam. Increasing relevance and realism will contribute to securing a better quality of education for the university.

With pen and paper exams, the handwriting "fluency" is a critical factor. This is determined by the rate of speed of which a person can demonstrate their knowledge by handwriting. The demonstration of knowledge through this media is therefore a critical factor for a student. Because we live in a digital era, technology is slowly and steadily taking over tasks related to manual and physical work. Students tend to write more and more on digital tools, and a research conducted by Connelly, Dockrell and Barnett is summarized as follows: "*undergraduates were very slow writers [hand-writers] whose writing speed was equivalent to published fluency data on 11-year-old schoolchildren*" [5]. This was done under a pressurized environment meant to mimic that of an examination. In 1995**,** Connor also found that the rate of output under simulated examination conditions declines [6]. The difference is so vast in the handwriting fluency of university students, that Parr, Levi and Jacka proposes examinations without time constraints. Their argument was based on a survey which found that approximately 35% of the students at a university in New South Wales, Australia, did not have enough time to finish their exams [7]. In addition to the handwriting fluency declining, the fluency of keyboard-typing is increasing to the point where it affects the motor skills related to handwriting [8].

Paper has been grounded in our culture through centuries. Through the upbringing, humans are exposed to paper in many forms, as drawings, a place to solve your homework and math problems, through post-it notes, shopping lists, doodling, writing birthday and thank-you-cards. One of the main functionalities with paper which have made it so important is how easy it is to use, and it is in terms, the most user-friendly interface we can interact with. It is instantaneously available, and through its physicality the user has mobility when using it. But when you want to digitalize a paper system and process, you cannot just add electricity (technological solutions) and expect it to work. The processes need rework and reengineering in order to maintain the core activities of the system, and a way to guide this rework is to look at how digitalization affect the processes and improve them. This can eventually help ground the change management throughout the organization.

"*A shortcut to success*" is how M.A Steiner describes cheating back in 1932 [9]. The supervising principal wanted to inform teachers that cheating promotes an undesirable behavioural pattern. This academic dishonesty can cause deprecation of the integrity of an educational institution. Two main factors for cheating on a high-stakes examination: stress and bad preparation.

NTNU lists a few examples of cheating on an exam [10]:

- The answer is copied from the internet and is presented as the cheaters own work
- The answer has been used by the student, or another student on a previous exam
- The answer has been prepared by another person
- Quotes and citations without providing sources of origins
- Use or be in possession of illegal aides during exam

Cheating, in all forms and shapes, can lead to severe consequences. For students at NTNU, it can lead to a one-year expulsion, and disown them the right to attend other universities during that time frame. They also get registered in the register for expulsed students, RUST. This is in accordance with the national law for universities in Norway [11] §4-8.

Norwegian universities have seen a rise in students being caught for cheating over the last 6 years [12]. This is not necessarily a result of students being more dishonest, but could be an implication that the systems for detecting cheaters have improved in that period of time [13]. This is mainly related to home exams and other digital exams, and not so much the traditional pen and paper exams. The policies and security measures associated with pen and paper exams have been established and grounded through many years of trial, and now we need to increase the validity of the software systems.

With software systems, we expect them to work as intended. This can be achieved by creating robust and secure systems. Every system is although never perfect, and might include faults. Faults are part of a pathology called the fault-error-failure pathology [14]. In order to eliminate these faults, we want to find strategies that addresses the faults. The faults pose as an imperfection in the system, and can lead to various degrees of consequences. A fault is a defect in the system, i.e. software bugs. When we introduce humans to the system, we get a new source of "error". In this case the humans are classified as threat agents, and impose a threat on the system.

The trend in todays higher education environment is the increase in the need for more technological solutions. It is therefore paramount to have secure and robust solutions for the systems that are intended to substitute the traditional customs. With new solutions appearing, we have also seen a rise in the scepticism of them in relation to the way they enable cheating. The implication is an awareness of needing to find new mitigation strategies, and establish policies and security measures on par with the ones found in traditional exams.

1.2 Scope of the Thesis

The scope of this thesis is focused on how a digital solution to both software and process steps can be supported through changing the traditional pen and paper exam into a digital exam. I will assess the processes in the current situation, and attempt to create a 'to-be' solution of the process steps. The goal of the 'to-be' solution is to identify superfluous steps and show how digitalization can address these steps. Additionally, the research will consider security threats in relation to the digital exams, and attempt to address security controls that can be used to counter the new threats. The security threats discussed will be focused on cheating and how they can give students unfair advantage and enable unwanted behaviour; this means that security threats related to i.e. forces of nature will be neglected in this thesis.

1.3 Research Questions

The motivation for this thesis is based on the rise of new technology and digital solutions, and the various positive and negative aspects they bring to the table. The focus will be on how digitalization can maintain the core activities and through change in processes, address how they can create value and improve the organization. The digitalization means that the exam exists in a digital environment, and when we introduce a digital environment, new security aspects will be prevalent over security aspects found in the paper system. We will consider how cheating can be executed in a digital assessment process, and as an implication of that, how the digitalization can support new countermeasures. To digitalize the organization, we need a clear strategy. A value creation template will be used to address the drive of digitalization.

RQ1: How can digitalization of exams support process improvement?

RQ2.1: What new security threats related to cheating arises when changing/digitalizing the processes of examination?

RQ2.2: What new security measures can be supported through digitalizing the processes?

RQ3: Is it possible to use aspects of Value Proposition Design to drive the digitalization of the examination processes?

1.4 Research Method

This thesis will consist of an empirical study of the processes related with current day practices at NTNU, and a study of security threats that can be applied to the case of cheating. **RQ1** will be based on a literature review, before assessing the findings. This will then be used to design

a ‘to-be’ situation of the processes. The model creation will prove if it is possible to ascertain whether digitalization can support process improvement in the case of NTNU.

RQ2.1 and **RQ2.2** are mostly based on an investigation and analysis of documents related to secure and robust systems. The advantage of basing this part of the research on documents are that they provide great insight into security. Due to the nature of the master thesis only spanning six months, a document-based approach can provide the researcher with a more longitudinal study of the current practices associated with threats and countermeasures. The researcher does not possess any necessary skills related with hacking and pentest information systems, so this part should be based on previous experience. **RQ2.2** will also be answered using risk assessment, to see the impact of the countermeasures in regards to likelihood and consequence.

I am specializing in Digital Enterprise Development at NTNU, and process modelling and strategy are topics I am familiar with. I am very interested in how models and methods can be used to align strategy and IT, and how it can help an organization in achieving its goals. I have previous experience with something called Business Model Canvas, and took a great interest in researching that. Value Proposition Design is in a way a specialization of the canvas, and it can be used to help an organization realize innovation and achieve its goals. **RQ3** is therefore an attempt to address how the template VPD, can be applied to digitalization of exams at NTNU.

1.5 Report Outline

Chapter 2 – Background Research and Related Work: This chapter consists of an introduction of the current situation at NTNU, including the different processes and solution used for digital exams.

Chapter 3 – User Driven Innovation and Process Improvement: This chapter describes the ways digitalization can improve business processes, and presents proposed business processes and views.

Chapter 4 – Threats of Digital Exams: This chapter discusses some of the new security threats associated with technology and cheating.

Chapter 5 – Countermeasures through Digitalization: In this chapter, we address how to mitigate and counter some of the threats presented in Chapter 4. A risk assessment is included to show how the countermeasures would affect the threats.

Chapter 6 – Requirement Elicitation: In this chapter we will be presented with the value Proposition Design, show how it can be used on customer profiles to demonstrate the different drives..

Chapter 7 – Discussion: Summary of the different chapters and assessment of the previous chapters to create a basis for a conclusion.

Chapter 8 – Conclusion and Further Work: The end of the thesis contains the conclusion of the research questions, and discussion of further work.

This page is intentionally left blank

CHAPTER 2

BACKGROUND RESEARCH AND RELATED WORK

In this chapter, the reader will be presented with the background research. The background research exists of an examination of the current situation of exams and the processes related to the end-of-term assessment, an introduction to academic cheating. Additionally, we will be introduced to a template for value creation, called Value Proposition Design. The chapter is rounded off with related universities and their success.

2.1 EXAMS AT NTNU

In this master thesis, I will propose improvements to the business processes and functions associated with the examination at NTNU. The proposal will consist of views in a 'to-be' situation depicting how the processes can be improved following a digitalization of the examination process. Additionally, I will conduct research of the new security threats that are enabled through a digital environment. Although there have been conducted research pertaining to this specific subject, I will attempt to address how process improvements can produce new countermeasures to the security risks associated with cheating. Before detailing the current examination process, we will look at how exams are conducted at NTNU, both traditionally and digitally.

NTNU is Norway's biggest university with over 32.000 students, hosting approximately 220.000 exams each year [15]. To reiterate, the predominant form of examination at NTNU is written pen and paper exams. The exams are held in supervised examination halls, where the proctors (or invigilators) are responsible for everything happening according to the defined policies and procedures. The traditional pen and paper exams process can be found in 2.1.2, where the reader can follow the exam from planning the exam period, and all the way to the exam being archived after assessing complaints.

NTNU is gradually digitalizing the examination process. This transformation is based on extensive research done by UNINETT and NTNU, as well as different pilot projects conducted at the university. The implementation at the university can be described as an incremental organizational change. Incremental implementation can be competence enhancing if it is associated with a lot of user training; which in terms causes knowledge spread [16]. The goals of the pilot projects are to gain experience and to see how mature NTNU is in terms of infrastructure and readiness of digital exams. Through these projects, the perception of how digital exams can be integrated could change over time, meaning that NTNU has a constructive world view [17]. The incremental implementation of a growing number of digital exams each

year, means that the digital solution and infrastructure associated with the examination process needs to be scalable.

The initiative NTNU Teaching Excellence [18] is responsible for bringing IT into education and provide NTNU with the means for offering education at a high international level. They have been responsible for a project called 'Digital Exam'. The project was started in 2013 and the goal of the project was to conduct small scale digital exams for testing software and investigate if the software fulfils the requirements for a digital examination at the university.

When comparing the digitalization process of the various Norwegian universities, it becomes evident that NTNU is falling short. In Section 2.4, we will take a closer look at some national universities and their approach to digitalizing the examination process.

2.1.1 Safe Exam Browser and Inspera

Before we are introduced to the processes related with the current examination process, we will briefly describe the tools used for handling digital examination at the university. As proposed by UNINETT and preliminary report, the digital exams at NTNU are mainly conducted on student owned equipment, either in the form on home exams or exams held in proctor controlled environments. The software used for the exams in the controlled environment, is called Safe Exam Browser and Inspera Assessment. Safe Exam Browser (SEB) is a "lockdown browser". The main functionality of SEB is that it locks down the computer from running other applications than the browser. This is to prevent the access of on-disk files, web pages, and other aides that are prohibited from usage on the examination. This thesis will not focus on the technical aspects of the current solution,

2.1.2 Examination Process at NTNU

"*NTNU aims to create the basis for the development of knowledge and to create value – economic, cultural and social. We will make the best possible use of our main profile in science and technology, our academic breadth, and our interdisciplinary expertise to tackle the large and complex challenges faced by Norway and the world community*" [19]

The above quote describes the goals of NTNU. The university is one of the cornerstone institutions in the sector of higher education in Norway. Yet, they are behind several other universities in the transition to a digital examination. The definition of digital examination will in the context of this thesis be classified as all the various steps related to examination, not only the actual execution of an exam. This is to avoid confusion.

The goals for an examination has been described by both Hillier [4] and Sindre [20]. A combination of these goals can be described in the following list:

- Teaching and learning
- Validity
- Reliability
- Practicality
- Security
- Production
- Cost

The teaching and learning outcomes are often measured through the students understanding and learning goals. The longevity of traditional exams has meant a tailoring of this form of evaluation to the goals.

The validity is related to the learning goals, and depends on the questions asked [20]. A high validity means that the exam is a good tool for the students to express their knowledge of the subject in accordance with the learning goals.

The practicality of paper was discussed, it is a physical object that is easy to relate and deal with. The current does however fall short in achieving this goal. Imagine the 220.000 exams being conducted at NTNU each year. If we make a rough estimation that each set of exam questions consists of at least 10 sheets of paper, we see how printing could be a demanding task. These ~2 million sheets of paper then need to be organized, transported, and managed by

different stakeholders; creating much room for error. The administrative tasks related to paper uses many resources that could be spent on other tasks. The practicality also falls short when we look at how the submissions are handled, they need to be scanned and copied, stored, and distributed to censors; again, a resource-demanding task.

Production can be found in the process related to students answering an exam. The production is defined as producing answers, and Hillier found that students "*would rather write on computer*" than paper [4]. A result of handwriting suffering a decline in education, and students using word processing software to write, the handwriting gets increasingly unreadable for each passing year. "*Students today can't write by hand anymore, they use PCs in their study*" is one of the drivers behind digitalization as defined by UNINETT [21]. More and more young adults are therefore more comfortable writing on computers, as this is a part of their every-day educational life. The reduced amount of physically producing written text, also results in students suffering from hand cramps when taking exams.

The implication of compromised practicality through extensive administration and management of the physical exams, is that the exam falls short on cost. An example of how much more resources are spent on process steps of traditional exams versus digital exams is presented in Section 3.3.4

End of term examination at NTNU is done both traditionally and digitally. The main form is as mentioned, traditional pen and paper exams, and they will therefore be the focus when we in the succeeding chapters describe the examination process at NTNU. The rationale for doing this is that the small digital fraction of examination we have today, would hypothetically culminate in the process improvements described in later chapters. This means that they are not as mature and complete as the processes presented in that chapter.

The processes affiliated with the traditional pen and paper exam are characterized by a lot of tedious and time-consuming manual labour. The process steps described in the succeeding Section 2.1.2.1 Preparation through 2.1.2.5 Complaints, are all characterized by inconsistencies from department to department. The steps vary in complexity, and throughout the university, a clear standardized workflow is undefined.

The examination process can be broadly divided into five main steps: preparation, execution, censoring, justification and handling complaints. These are steps that are critical to the success of an exam. Next, the reader can find detailed descriptions of the processes and models

associated with examination; depicting the various business and application structures. This includes the business actors, processes, functions, objects/documents, as well as some of the application services used to cater the process steps. The models have been developed using the ArchiMate notation, and the basis and inspiration of the models comes from a set of different sources ([22], [23], [21], [20]).

2.1.2.1 PREPARATION

The first step in the process of conducting an exam is to prepare all the necessary precursory tasks needed to execute an examination at a higher education facility. This step has been aptly named "Preparation", and details how the various actors plan the exam period, create the exams.

This step can again be divided into smaller, more comprehensible steps. These sub-tasks are:

1.1 Plan exam and student activities
1.2 Create exam and choose censor
1.3 Print and distribute exams

The sub-tasks are represented in Figure 1, Figure 2 and Figure 3, as different views of the examination model. The notation is ArchiMate, and each figure contains some elements from the business and application layer. The reason for choosing ArchiMate as a modelling language is the high-level concepts supported in ArchiMate. It can be used by both administration, business, and the technological aspects present in an organization. It focuses on the Business and how it can be mapped and aligned with the IT Strategy. ArchiMate structures its entities according to the TOGAF architecture, which is the preferred architectural approach used by NTNU IT, and interested parties in NTNU IT could therefore benefit from this thesis' use of the language.

The first view shown in this chapter is found in Figure 1. Here we see the process steps related with the student: online registering and withdrawing from an exam, and applying for special accommodation. The process of applying for accommodation is a manual and physical process requiring the student to fill out a form, and send it by mail to the exam office.

The form is received at the exam office, and processed here. The exam office is also responsible for registering the "assessment unit" of an examination in the Felles Studentsystem (FS) and send the information on the exams to the students.

In collaboration with the faculty, the use data for the exam period to plan the examination period, typically in a time planning service, spreadsheet system, or with similar tools. After the period has been planned, the data has to be manually entered into FS.

Plan exam and student activities

Period/prompt	Beginning of semester
Input	Data for exam period
Actors	Exam office, faculty/institute, students
Processes	Create exam plan and information, register assessment unit, register for exam, apply for accommodation
Artefacts	Exam plan
Outcome	Exam registration, candidate list, successful planning of examination period
Tools used	Paper forms, e-mail, time planning system, FS, and Studentweb

TABLE 1: VIEW DESCRIPTION: PREPARATION 1.1

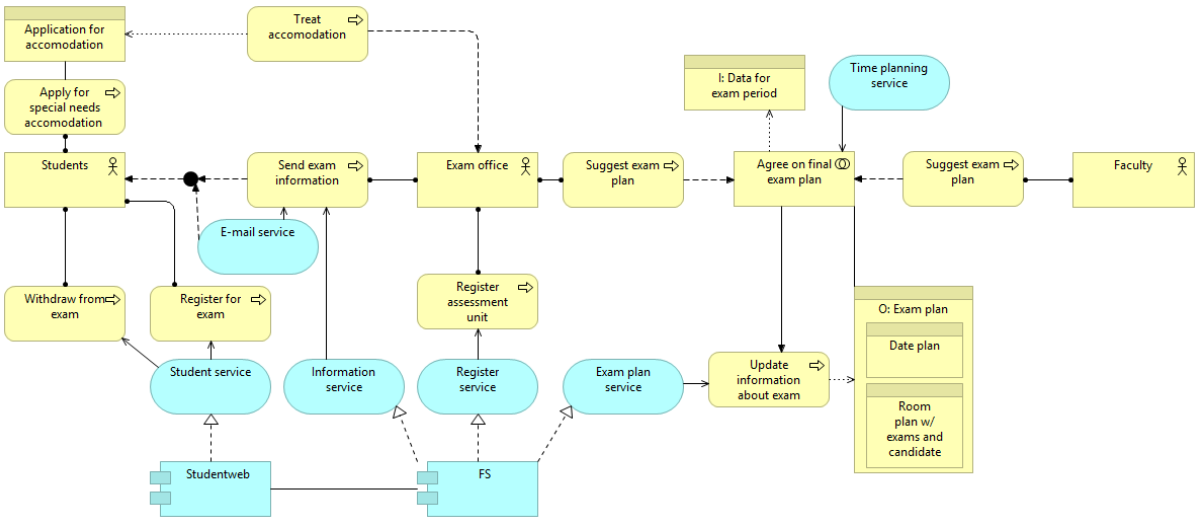


FIGURE 1: PREPARATION: PLAN AND STUDENT ACTIVITIES

When the assessment unit has been registered into FS, the faculty will receive a request for the creation of an exam for that assessment unit. Following this request, a censor is allocated and chosen; and registered in FS by the exam office.

The exam is created typically in a word processing software, i.e. MS Word. Along with the exam, the course coordinator translates the exam, if required, and creates a censor guidance. The exam is then sent to the censor for control and verification. This is a paper process.

Create exam and choose censor

Period/prompt	Request for exam creation
Input	Course description: curriculum, study plan, learning objectives
Actors	Exam office, faculty/course coordinator, censor
Processes	Create exam and censor guidance, allocate and register censor
Artefacts	Exam, censor guidance
Outcome	Physical, signed exam and registration of censor
Tools used	Word processing system, paper, FS

TABLE 2: VIEW DESCRIPTION: PREPARATION 1.2

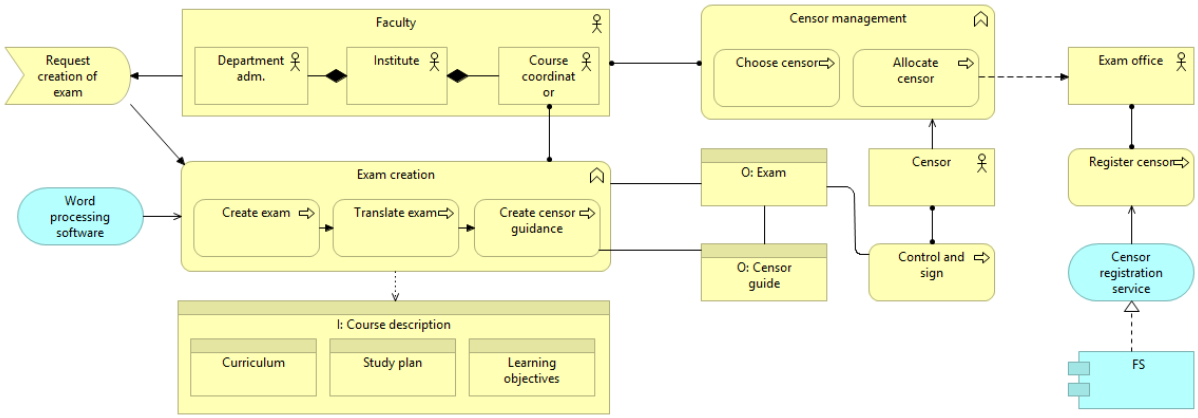


FIGURE 2: PREPARATION: CREATE EXAM AND CHOOSE CENSOR

After the exam has been controlled and signed by the censor, the faculty collects the exam, gathers information regarding the candidates taking the exam and the various language variants the exam should be printed in. This exam packet is then sent to the exam office.

The exam office is then responsible for sending the different exam packets to a printer where the exams are printed out. A transport service picks up the exams from the printer on the examination day; which leads us to the "Execution" step.

Print and distribute exams

Period/prompt	Receive controlled and signed exams
Input	Exams
Actors	Faculty, exam office, printer, transport service
Processes	Collect and get information about exam, print exams, pick up exams
Artefacts	Multilingual copies of exam, printed exam sets, candidate lists
Outcome	Exams printed and start of distribution
Tools used	FS, printer

TABLE 3: VIEW DESCRIPTION: PREPARATION 1.3

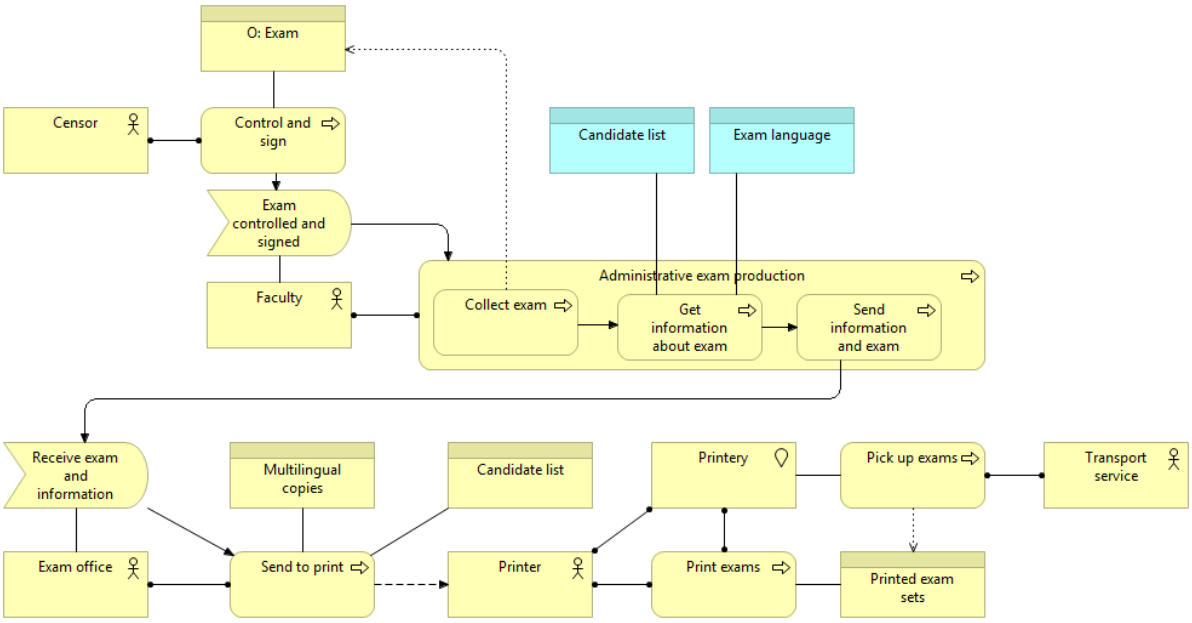


FIGURE 3: PREPARATION: PRINT AND DISTRIBUTE EXAMS

2.1.2.2 EXECUTION

The next step in the overall process is the actual execution of the exam. This is a process done on the various examination dates defined in the exam plan from Figure 1. The process is found in Figure 4, and depicts a view of the examination model. The model only shows elements from the business layer, as this process is permeated by manual labour and physical copies of the business objects found in the process.

The model starts where Figure 3 stops, with the transport service distributing the exams to the examination central at the premise where the exam will be held. After the exams have been delivered to the central, the responsible proctor (invigilator) collects the exams associated with his or her examination room. The exam distribution is then planned (if there are more than one course being assessed in the room), and the exams are distributed to the attending students.

After the students have received the exams, the proctors are tasked with registering the attendance of the students and checking their identification and aides. This is a manual and time-consuming process, where the last student on the row could be sitting and utilizing illegal aides for some time before the student is checked. This means that students are in possession of the exam before having to identify themselves.

During the exam, the students have two main options, answering the questions or withdrawing from the exam. If they experience any of the questions ambiguous or have questions related to the exam, they need to wait for the teacher to enter the premise. If the exam of a single course is being conducted at geographically dispersed locations, this means that a student might have to wait several hours before getting the information they need. Issues with the clarification of issues have been discussed in

When a student is finished with the exam, they are to rip off the copy-page and fill out the information on the exam delivery folder. In exams where the students have to sit the entire duration of the exam, they are given 15 minutes to complete this task. During this 15-minute time slot, they are prohibited from answering any more questions. This can be hard for the proctors to enforce, especially in large examination rooms. Those 15-minutes subjects the students to a great deal of stress after hours of handwriting and hand cramps.

When the student has prepared their delivery folder, the proctors controls the information on the delivery folder, and makes sure that it is accurate. Then the exam is collected and the list of

attendance is updated. The examination process is complete when the exams have been delivered to the central for distribution to the responsible departments.

As previously stated, this process step is characterized by manual labour and large quantities of paper, with no technical support. The proctors are responsible for the legality and proper execution of the examination, and Figure 4 is a view of this process step.

Execution	
Period/prompt	Exam period
Input	Exams and candidate lists
Actors	Transport service, proctors, students, teacher
Processes	Transport exams, pre-exam management, taking exam, delivery
Artefacts	Exam answers
Outcome	Successful execution of exam
Tools used	Paper

TABLE 4: VIEW DESCRIPTION: EXECUTION

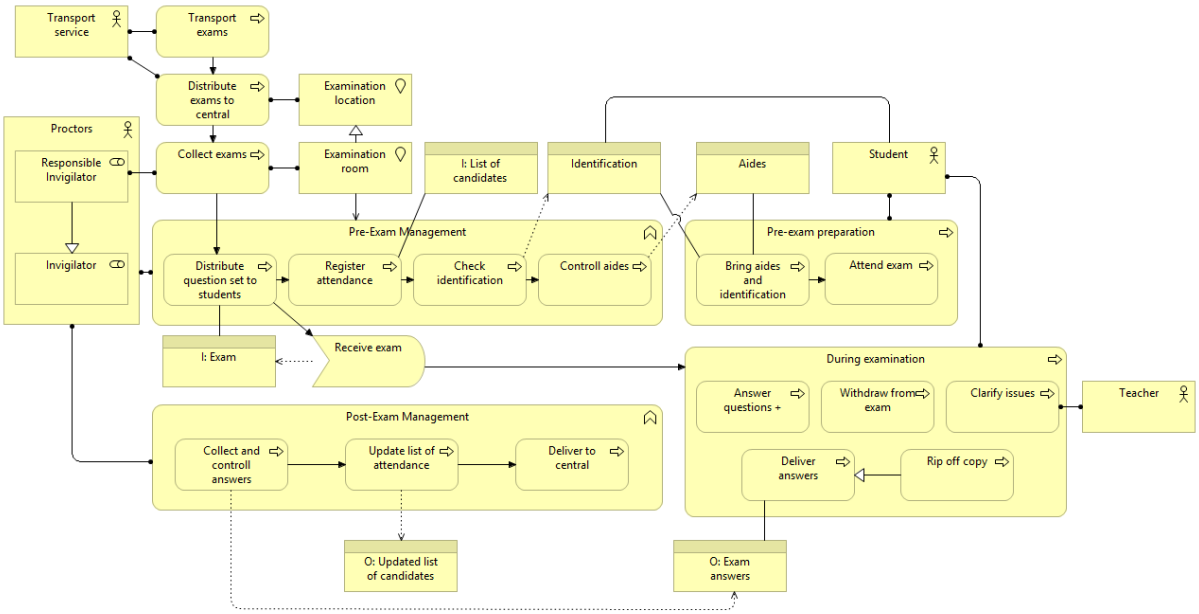


FIGURE 4: EXECUTION VIEW

2.1.2.3 CENSORING

After the exam is done, the deliveries are distributed to the assigned censors from Figure 1. The censors are responsible for grading the exam answers in accordance with the censor guidance. After they have graded the exam using a censoring form scheme, they send it to the responsible institute which then sends it to the exam office. The exam office is responsible for manually putting the grades into FS and publishing the results. After this process is done, they store physical copies of the deliveries.

The next step in the examination process is the censoring of the exams. This step begins when the deliveries have been distributed from the examination central to the department. At the department, the administrator is responsible for distributing the exams to the censor. Depending on the preference of the censor, this is done either digitally or physically. In the censor wants digital copies, the department must scan the deliveries, and send them to the censor by e-mail; accompanied by a digital censor form. If the censor wants physical copies, the exams are copied, and sent by mail to the censor along with a paper form of the censoring.

The censor receives the exams and the deliveries and are now tasked with grading the exams and producing a valid censoring. If applicable, the exam is manually put through a plagiarism checker. The censor fills out the form, either digitally or physically, validates the censoring, creates justification if specified, and sends the form to the responsible institute.

The institute then sends the censoring form to the exam office, where they manually punch in the grades into FS. FS calculates the statistics related to the exam, before the exam office publishes the result; making it available to the student. When the result has been published, the exam office is responsible for archiving the physical versions of the exam deliveries and the questions at a storage according to law. The Norwegian government has mandated that exam questions and censor forms are to be stored indefinitely, while exam deliveries should only be stored for the period they are needed, i.e. until the deadline for justification has passed, as addressed in [24] §3.5.

Figure 5 depicts the sub-process described in the previous paragraphs, and is also used in the "Complaint" sub-process should the student complain and ask for a new grade.

Censoring

Period/prompt	Post examination
Input	Censor forms, exam deliveries
Actors	Department administration, censor, institute, exam office, students
Processes	Distribute answers, censor, publish results
Artefacts	Censor forms, grades
Outcome	Exams censored and grades distributed
Tools used	Physical and digital censor forms, mail/e-mail service, plagiarism checker, FS, Studentweb

TABLE 5: VIEW DESCRIPTION: CENSORING

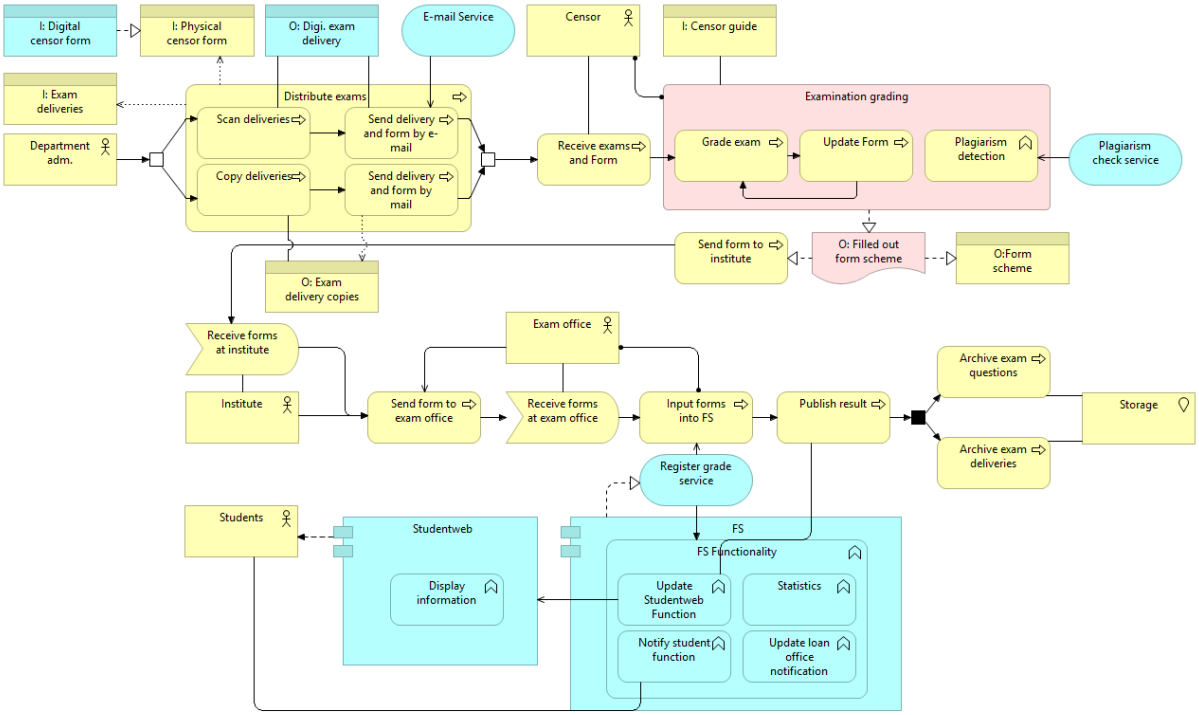


FIGURE 5: CENSOR VIEW

2.1.2.4 JUSTIFICATION

After the student receives the grade, they can request a justification for their grade. This process varies from department to department, but the general process steps will be described in the following chapter.

If the student wish to receive justification, they must find the justification scheme. The justification scheme needs to be filled out and delivered or sent as a physical copy to the faculty. The faculty receives the justification claim, and registers the case in their archive (ePhorte is the system used at NTNU). After the case has been registered, it is sent to the institute related to that exam.

The institute and course responsible are responsible for delivering the justification of the grade to the student. The exam delivery is gathered from the storage, and if it contains justification, the justification form is filled out and sent to the student. If the exam is missing justification, the censor is contacted and the grade is justified. Then the justification form is filled out. The justification form is copied, and sent to the student and the faculty before being updated in the archive.

Figure 6 shows a hypothetical B-student with parts of a motivation view. This is included to show the drivers and goals behind the choice to start a justification process from the student's point of view.

Justification	
Period/prompt	Receive justification
Input	Scheme for justification, exam delivery
Actors	Faculty, admin, course responsible, censor
Processes	Register case, justify grade
Artefacts	Justification form
Outcome	Case registered in archive, student receives justification
Tools used	Archive, paper forms

TABLE 6: VIEW DESCRIPTION: JUSTIFICATION

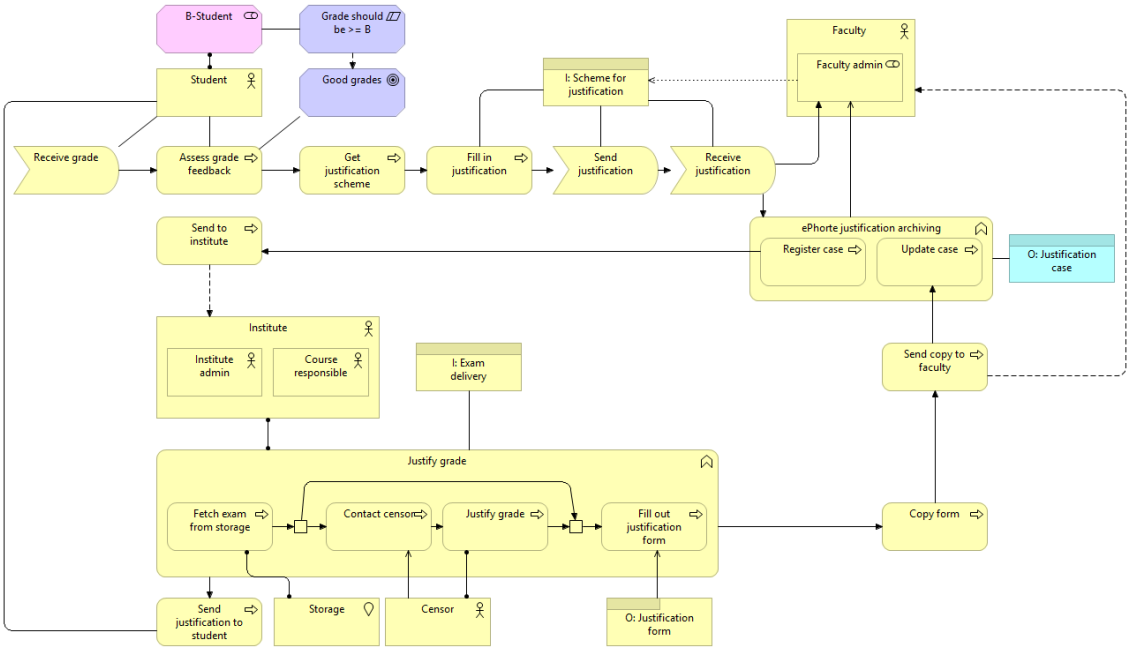


FIGURE 6: JUSTIFICATION VIEW

2.1.2.5 COMPLAINTS

This sub-process can start regardless of the student wanting justification or not. In either case, the student receives the grade or justification and given the motivation, they can request to complain on the grade. This the equivalent of getting another censor to assess their examination delivery.

Similar to the justification process described in the previous chapter, the student has to deliver a physical complaint form to the faculty responsible for their exam. When the faculty receives the complaint claim, they register it in the archive (ePhorte), and begins the censor management processes. In the phase preparation, a complaint censor could also be allocated, but in the view presented in Figure 7, we assume that it has not already been done. When the complaint censor has been allocated, the exam office registers the new censor, and the faculty fetches the exam submission.

This prompts a new censoring process as shown in Figure 5. Here, the complaint censor takes the role of the censor. When the new “Censoring” sub-process has been completed, the student receives the new grade and the faculty updates their archive.

The figure includes parts of the motivation view, as seen in Figure 6, to illustrate that a student needs some sort of motivation to complain on their grade.

Complaint

Period/prompt	Receive justification
Input	Scheme for justification, exam delivery
Actors	Faculty, admin, course responsible, censor
Processes	Register case, justify grade
Artefacts	Justification form
Outcome	Case registered in archive, student receives justification
Tools used	Archive, paper forms

TABLE 7: VIEW DESCRIPTION: COMPLAINT

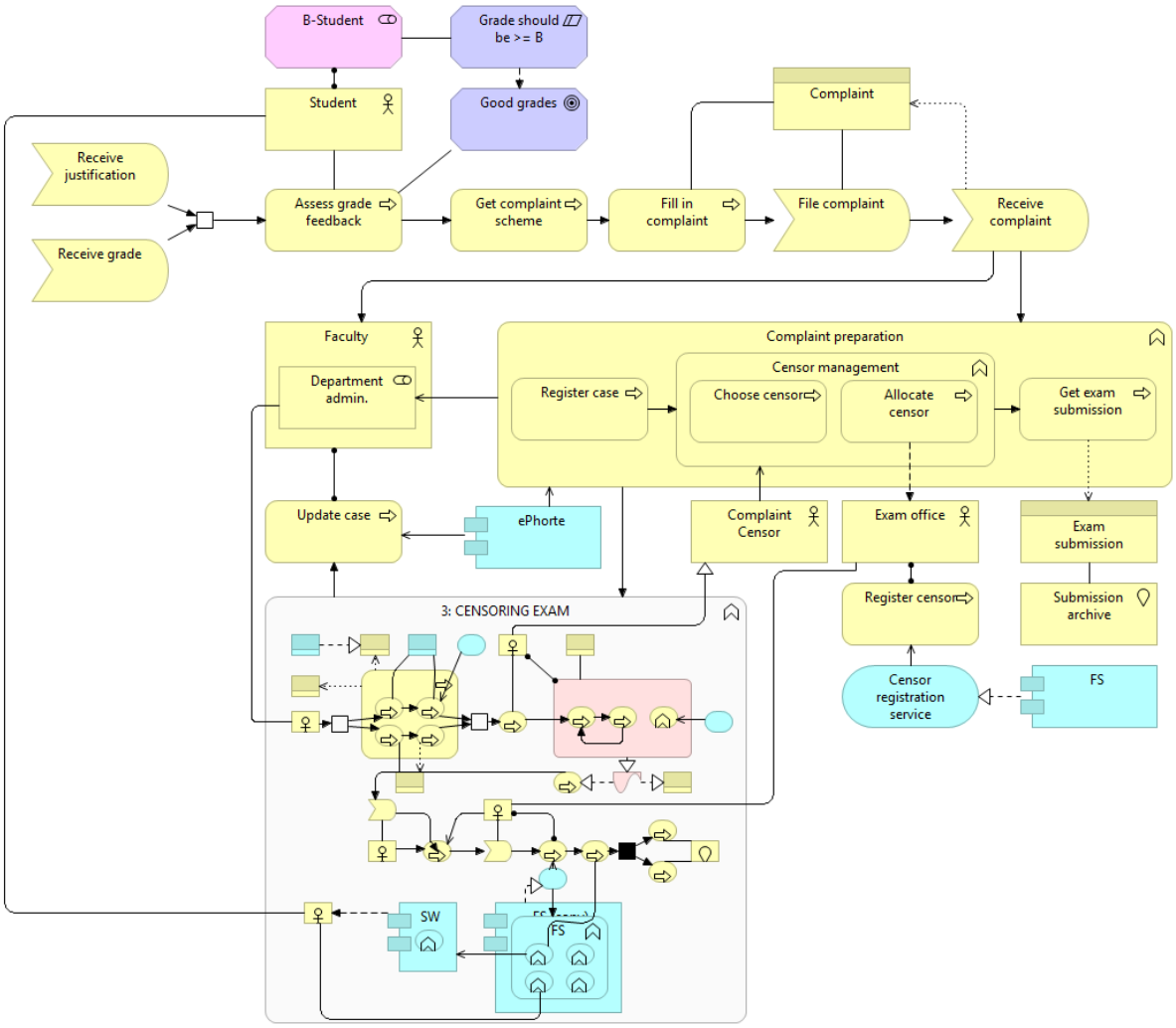


FIGURE 7: COMPLAINT VIEW

Some of the sub-process steps have been omitted and simplified in the views found in the previous chapters. In Table 8, we discuss a few of these steps and the rationale behind the omission or simplification:

Process	**Omitted/simplified**	**Rationale**
Paying proctors	Omitted	Should be in a process called "finalizing exam" which have not been considered
Paying censors	Omitted	Should be in a process called "finalizing exam" which have not been considered
Removing exams from archive	Omitted	This should have been included in "Complaints" but does not necessarily relate to the complaining process and re-censoring. Administrative work related to removing exams are however conducted after the period of justification and complaining has ended.
Creating exams	Simplified	There are many sub-steps to this step, some of them will be included in Figure 13, to show how digitalization can automate the creation.
Censoring exam	Simplified	
During examination	Simplified	Taking toilet breaks and request more paper sheets are not that relevant in the model.

TABLE 8: EXAMPLES OF OMITTED AND SIMPLIFIED PROCESSES

2.2 CHEATING

Cheating is a concept of unwanted behaviour, and exists in many different areas: business, industry, academic. As the scope and motivation of this project is concerned with educational topics, the academic cheating is the focus for this chapter. To understand a cheater, we need to look at the motivation behind the cheating.

The motivation behind learning and gaining academic knowledge is driven by either a specific wish to gain knowledge, or for a learner to demonstrate their competence. These forms of knowledge, named intrinsic and extrinsic motivation [25], have a direct correlation with the motivation for cheating [26]. Students with an extrinsic motivation, wishing to demonstrate their competence, are more likely to cheat than the intrinsic motivated students.

When conducting surveys in cheating behaviours, it might be difficult to get accurate and complete results; as students could fear getting caught. In a survey conducted by Sentio Research for Universitas, 5% of 1001 students admitted to cheating [13]. To demonstrate this probable survey deviation, the survey takers of Michaels and Miethes study reported that 41.9% of their student sample admitted to cheating on exams [27]. In their report, Rettinger and Kramer [28], wanted to investigate the behaviours behind cheating, and how the peer perception and attitude of students can affect cheating behaviours. Their sample showed that ~11% admitted to cheating, 35% had knowledge of other students cheating, and roughly 29% perceived their peers as cheaters. The inconsistencies in the percentage of students admitted to cheating in the different samples, could be a result of cultural diversity; nevertheless, we should assume the number to be higher.

In McCabe and Trevinos 1997 study of 1800 students, they found that the predominant motivation for cheating was peer-related factors [29]. This enforces the extrinsic motivation, where students wish to boast their performance against other peers. Peer perception is therefore important: does an academic honour code exist among the students at universities? They found that these honour codes resulted in lower levels of cheating, as 71% admitted to serious cheating on exams (where no honour code existed) and 54% admitted to cheating where an honour code was present.

They also account for some common methods of cheating:

- Copied answers on exam
- Used unauthorized aides, i.e. illegal notes
- Helped other on exam
- Plagiarism
- Collaboration

As mentioned in Section 1.1, we need to increase the validity and acceptance of new systems. This can be done by creating secure and robust systems. These systems need to address the cheating behaviours found in students. It might not be possible to alter the motivation and number of attempts of cheating, but the system should have strategies to prevent and mitigate the various ways one can exploit the system.

When defining the taxonomy of a secure and robust system, we look at five characteristic areas of the system: privacy, safety, security, dependability, and performance. Each of these characteristics are in some way related to the other characteristics. In this master thesis, the focus will be on the security aspect of a secure and robust system. There is an abundance of various types of security; one might want to support cyber security, computer security, ICT security, data security, or information security, to name a few. These classifications do not necessarily mean the same thing and focuses on different parts of a system, yet they are used interchangeably.

When we talk about security in information systems, one might think it only involves protecting information objects (assets). This is not the case, as we need to look on several aspects of that information: how it is stored, processed, and transferred and distributed. Security is, in ICT, divided into three fundamental attributes: Confidentiality, Integrity, and Availability, more commonly known as CIA. In the beginning of the computer age, security was traditionally associated with confidentiality; and over the years, integrity and availability has become almost just as important. Fahramand, Navathe and Enslow defines confidentiality as the prevention of disclosing information or services to unauthorized entities [30]. In other words, this means to preserve the restrictions on the information access. Integrity is the property of restricting unauthorized altering, manipulation, or deletion of information. Availability is the property of protecting systems from unauthorized disruption. This means that the systems access is reliable and that authorized users can access and use the system.

In addition to these fundamental requirements, it is also common to define three other requirements.

2.3 VALUE PROPOSITION DESIGN

For NTNU to satisfy their goal, it is important to have a strategy that is in line with their ambitions and motivations. A strategy can be defined by the following quote from Kaplan and Norton: "*Strategy is based on a differentiated customer value proposition. Satisfying customers is the source of sustainable value creation*" [31]. Value creation is the task of matching attributes of a service to the needs of a customer, and is used to make an organization attractive to their customers [32].

Fjerdrumsmoen of NTNU Teaching Excellence [2] defines some critical success factors to the project of complete digital assessment:

- Operation and Management
- Process mapping
- Requirement identification and development
- Introduction and implementation
- Anchoring the changes in the departments

These success factors should be part of the strategy, and therefore how they can create value for the organization. The attractiveness of the organization, as seen by the customers, can in the case of NTNU be perceived as the benefits gained from providing an innovative and digital examination service.

To achieve this attractiveness, we need to address how the success factors can be used to drive the digitalization process. As this attractiveness comes in the form of a value proposition, we need to map the user needs to the service.

2.4 INITIATIVES AND OTHER UNIVERSITIES

Work with digitalizing and computerizing the higher stakes exams are being conducted at several universities, both abroad and in Norway. The following section will present universities in various phases of the digital transformation. From the standpoint of NTNU, universities with similar cultural aspects and implemented software will be most relevant. We will therefore focus on Norwegian universities.

In the higher education landscape of Norway, we have an important actor: UNINETT. UNINETT is a government owned company in charge of developing the national education network. The goal of UNINETT is:

"Students and employees of the Norwegian higher education sector should have access to a set of ICT-services and infrastructure that enables modern education, research, and dissemination on a high international level". [33]

Through their initiative called eCampus, they aim to provide ICT services that enables digital assessment. The focus of this initiative was to find a digital tool that best suited their requirements for a digital examination at the Norwegian universities. The resulting suggestion of tool was Inspera Assessment. It is evident that the Norwegian universities has reaped the benefits of using this tool as the use of the tool tripled from the spring of 2015 to the spring of 2016., from 25.000 to 75.000 examinations [34]. This rapid growth shows that universities are eager to transform their examinations.

The university that is in the forefront of digitalizing the examination process in Norway, is the University of Agder. Like UiO, they have also focused on providing the infrastructure necessary in order to conduct large quantities of examinations. This is done in their multipurpose training facility, Spicheren. This location draws large resemblances to SiT Dragvoll found close to the NTNU campus called Dragvoll. At UiA you can get the exam on both digital and physical format. This does not necessarily be synonymous with process improvement, as the processes associated with printing, copying, and distributing the physical paper copies are still present.

The University of Oslo (abbreviated UiO), is Norway's second biggest university in terms of size [35]. Founded in 1811, the university is also one of the oldest institutions in educational Norway. Approximately 26.800 students are enrolled at the university and 85.700 exams are conducted on a yearly basis. The goal of the university in regards to examination is to make it paperless for students, administration, course responsible and the censors. The university is also part of the initiative UNINETT, although a bit further in the digital transition than NTNU. In 2017 the final evaluation was divided into 53% digital exams, 30% hand-ins, 13% pen and paper exams and 4% other forms of valuation [36].

FIGURE 8: SILURVEIEN 2 - PHOTO: ALEXANDER LORENTZEN [37]

One of their critical keys to success is called Silurveien 2. This is a designated building/space specifically designed with infrastructure to support digital examinations, see Figure 8. In the spring semester of 2017, almost 74% of all exams where conducted at this facility [38]. One of the challenges that they have encountered with the digitalization is that the form of evaluation must be changed in order to cater to the new format, and the limitations of existing solutions.

The Norwegian Business School is outside the initiative eCampus, and has rather developed their own system called DigiEx [39]. They took a different approach than the universities associated with eCampus, focusing on automating and reengineering of the processes associated with the administrative aspects of digital assessment. They have stated that a success criteria is to set realistic sub-goals and learn from the experiences gained through incremental implementation.

The experience NTNU can draw from the other, similar universities are related to the limitations and challenges they have faced with digitalizing. In order to eliminate the need for supporting paper submissions to the exam (i.e. models and charts), the software should support third-party applications. At universities, some of the most important objects of evaluation and assessment are the "big" exams, for instance bachelor and master thesis. Censoring these big exams should also be supported in the system. As we have seen, justification is handled differently in the different faculties at NTNU, and it is representative for the other universities as well. This process step in the digital examination process will be addressed in Section 3.3.4.

Universities are diverse organizations, often geographically dispersed and with different faculties having different types of administrations (centralized/decentralized). As discussed in my project thesis [40], organizational transformation can lead to the destruction or creation of competence. By improving the processes in a way that retains their goal and motivation, NTNU can hopefully achieve a successful incremental implementation that increases the spread of

knowledge. In the next chapter, we will see how the digitalization can improve the processes and cater to different needs.

2.5 SUMMARY

This chapter described the exams at NTNU. Through the background research, it is evident that the examination process at NTNU needs to be focused on. Many of the processes affiliated with the examination process is characterized by large quantities of administrative tasks demanding many resources and man-hours. The process steps have been shown to be tedious and in need of reengineering.

When NTNU completely shifts to a digital solution, they want to maintain their academic integrity. An example of a threat that discriminates the integrity is cheating, and more specifically, academic cheating. It is therefore paramount to address how a system can support different safeguards to avoid this unwanted behaviour.

Maintaining the integrity and core-activities found in the organization, is a clear strategic objective. Value Proposition Design is a proved and recommended method for addressing these objectives.

This page is intentionally left blank

CHAPTER 3

PROCESS IMPROVEMENT

The purpose of this chapter is to address the importance of process improvements. When the importance has been described, we are presented with the motivation behind digital examination. Based on the motivation, and the congested and ineffective processes described in Section 2.1.2, an example of improved processes is presented. These processes will be used to show how digitalization of exams can support process improvement, by defining the benefits realized in a digital solution.

3.1 Process Improvements

'What is process improvement?' one might ask. Zahran defines process improvement as the task of getting a continuous improvement of a process [41]. It involves assessing the various processes in a business or organization, and act upon that assessment if the processes are redundant or in need of change. A way to assess the processes are to look at the motivation and goals behind them: Do the processes fulfil the goals in a satisfactory manner? Appian defines process improvement as *"... the proactive task of identifying, analysing and improving upon existing processes within an organization for optimization and to meet new quotas or standards of quality*" [42].

Zahran describes how Software Process Improvement can increase the success of an organization, but in order to achieve that improvement, the processes related to organization, management, engineering, business, and support are needed to be present and improved as well. This description would implicate that some of the benefits realized through software process improvement, also apply to the surrounding processes. He points out different needs for realizing the benefit associated with process improvement:

- Align process improvement with business needs and stakeholder satisfaction
- Incremental approach to implementation
- Focused investments
- Training
- Enforcing the process

Sandkuhl et. al states that a typical business challenge is to improve business processes [43]. They include a description of what an enterprise model supporting process improvement should contain. From the Table 9, we see that the typical outcome is strategic objectives and alignment with the IT strategy. As discussed previously, we want the strategy to be explicitly defined as to how an organization can retain their core values and activities, and an enterprise model can

therefore be used to illustrate this point. This is as described in Section 2.1.2, one of the rationales for choosing ArchiMate.

Enterprise model for process improvement	
Purpose	Improving business processes
Input required	Processes to be improved including the relevant actor dependencies, such as the process owner
Who should be involved	Management level for defining strategic objectives; process owner and involved staff for designing future processes; operations manager and technical support for process implementation
Typical outcome	Strategic objectives guiding process improvement; future processes with roles, resources, and supporting IT; action plan for implementing the change process
Critical quality issues	Fulfilment of strategic objectives; feasibility of future processes in practice; acceptance by staff involved; integration with other processes and systems in the organization
Tool support	Modelling of processes at several levels of abstraction, using the process decomposition principle.

TABLE 9: ENTERPRISE MODELS FOR PROCESS IMPROVEMENT [43] PAGE 15

To briefly summarize the importance of process improvements, we can assert that process improvements increases the efficiency of an organization, manages adjustments with regards to the strategy and potential new services. It decreases cost and use of resources, while still protecting the core activities and goals of the organization. Improving the processes does not on its own address all these points, but when we look at the strategic goals and structures within the organization; we can achieve what we want.

3.2 MOTIVATION

We have seen how process improvements can motivate the strategic objectives and increase acceptance of the stakeholders. Process improvements simplify and can show the integration of processes related to new systems. Through process improvements, we want to maintain the core activities and refine them in a way to i.e. increase efficiency and productivity, and decrease cost and use of resources.

The motivation for the digitalization of exams have been discussed in Section 1.1 and 2.1.2. UNINETT describes the drivers behind digital assessment as "*working smarter, moving from*

paper based assessment procedures to digital procedures, reducing time and energy spent, and improving the quality of the old written assessments procedure" [21].

3.3 IMPROVED EXAMINATION PROCESS

The main goal of the examination process was found in the previous sub-chapter. The purpose of this chapter is to see how we can tie the motivation to the improved and proposed models for the organization. There are many ways one might try to achieve these goals, and the improved processes will address these. NTNU is a large organization, with many geographically dispersed departments. Throughout these departments, the examination process has been characterized by many unnecessary manual administrative tasks and man-hours spent printing, scanning, and copying various forms of paper; either exam questions, justification forms, exam deliveries, candidate lists, complaint forms, censor schemes, and the list goes on. All the copies of the different papers also must be stored physically as mandated by the Norwegian government.

There are very few steps which are truly automated, presenting the opportunity for errors caused by humans. As we will see in Section 4.1, humans are the main source of errors and threats to a system. The flow of communication between various departments and stakeholders are also lacking, or surprisingly low. Take for instance the process of censoring, where the filled-out censor form must go through the faculty on its way to the exam office before it is manually punched into the system.

How can digitalization help improve the business processes in this organization? The reader will find the views presented in the succeeding chapters to be influenced more by application components than the ones in the current situation. The application components aim to show many of the steps in the sub-processes have been automated to reduce the human errors and tedious amount of manual labour. As many of the steps have been automated and digitalized, we also eliminate the need for all the administrative work related to printing, copying, scanning, and storing physical copies of all the paper that was once part of the process. The views are used to show how the processes integrates with different systems in the organization, creating a digital ecosystem for the university.

Before presenting the improved processes and their correlating technical components, there are some assumptions to be made about the system and how it works. The cost of developing this system is not taken into account, as we need to change existing systems, and adapt them to the example presented. The increase of functionality creates a need for resources spent on

developing it. This has been taken into consideration, but it is beyond the scope of this thesis to estimate the real cost of such an implementation and therefore not discussed further in this thesis.

As a precursor, we assume that the users are logged in. The different users have different permissions and restrictions in the system, and a simple view of how the log-in can be found in Figure 9. The only time when the log-in process is different is during the execution of the exam. This will be discussed in Section 3.3.2.

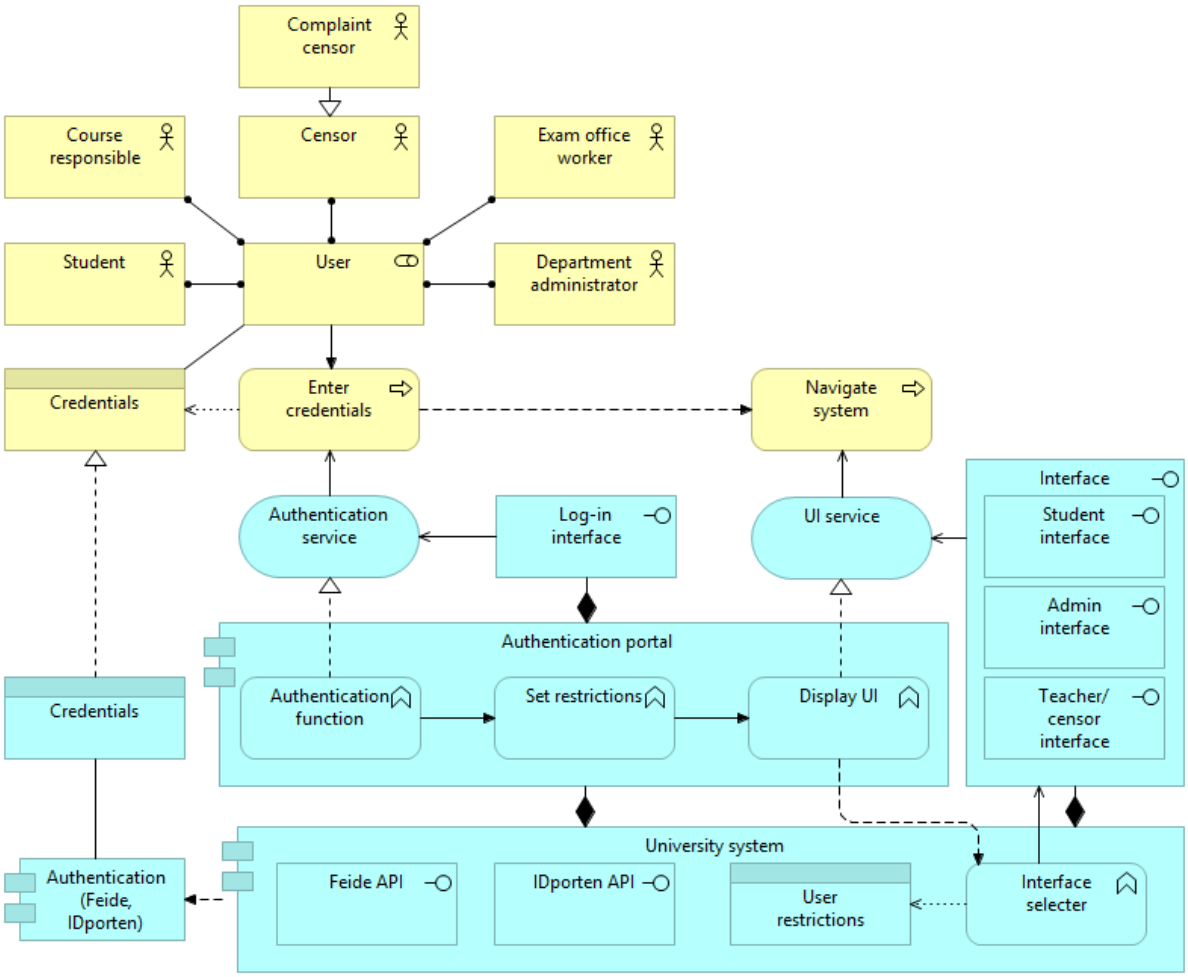


FIGURE 9: ASSUMPTION - LOG IN

The system associated with the presented improved processes are supported not necessarily by the current solution from in Section 2.1.2. The university system we see in the various views is a hypothetical digital ecosystem. A rough example of some of the components can be seen in Figure 10. It does not show all the necessary components needed to make it work. Additionally, it creates a new position for the IT managers and departments. Throughout every process step

they need to be present to provide support and monitor the system. During execution of examination, they might be tasked with monitoring the network to discover any forms of cheating.

In the figure, we see a shared university portal. This could bring several universities together creating a common portal for registering exam questions and tasks. NTNU could then become part of a bigger ecosystem, where exam questions go through extensive quality assurance and control. How this can support process improvement is discussed in Section 5.2.

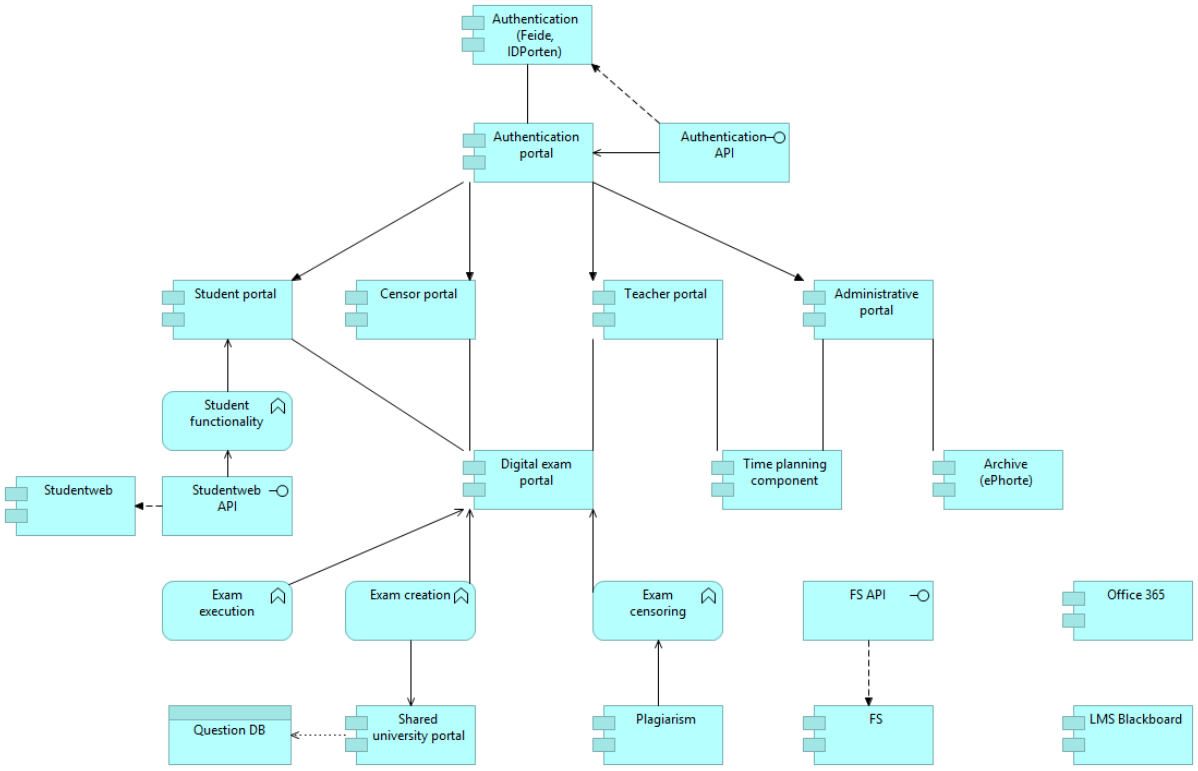


FIGURE 10: EXCERPT OF POTENTIAL COMPONENTS OF A DIGITAL ECOSYSTEM

3.3.1 PREPARATION

We saw in Section 2.1.2.1, that there are many steps to the sub-process "Preparation". To increase the readability and comprehensibility of the views related to this sub-process, we have split the preparation in two parts, correlating with the two first steps found in the current situation, Figure 1 and Figure 2.

The activities for the student have not changed a lot. Instead of registering and withdrawing from exams on a separate Studentweb portal, they can now do it in their student portal. The student portal is part of the university system, and the course management is realized through a Studentweb API. Studentweb is a national Norwegian service for student management, and should not be excluded from the university's digital ecosystem. This is to still pertain the flow of information between different universities, should the student wish to change university. By making this functionality available in the university system, we ensure that the student only has to deal and relate to one system. This will be helpful to exchange students and new students. In relation to the student stakeholder in the system, they can now apply for accommodation through the student portal. This removes the need for the student to print out, fill in, and mail the application, making it more streamlined. The student portal will allow the student to upload necessary documentation to account for their need.

The exam office is still responsible for registering the assessment unit and assess the application for accommodation. This is done in the university system. Just like Studentweb, Felles studentsystem (FS) is also included in the digital ecosystem. FS is an administrative system for universities and higher education and is used by 36 institutions in Norway [44]. We simply move the need to use FS directly, and course management can now be done in the universities ecosystem through APIs.

One of the main tasks the exam office was responsible for in this phase was to plan the examination period, sitting down with the various members of faculty to account for their dependencies and then allocating different exams to free locations after the plan was completed. Again, a manual task where the plan was compiled using different systems: spreadsheets, time planning services, paper forms. As we can see in Figure 1, the exam office now triggers a prompt for the faculties to specify date dependencies related to their courses. After all the faculties have input their dependencies into the system, a time planning component is responsible for creating the exam plan. It fetches the constraints: available rooms and their infrastructure, course and dependencies, number of candidates and students in need of

accommodation. An exam planning algorithm uses the course and date dependencies to first plan the dates of the exam, information that is displayed in the system for the users to see. When the deadline for registering for a course has passed, a room planning algorithm steps in, allocating the candidates and exams to rooms. This information is automatically displayed 3 days before the exam, like in the current system.

Table 10 can be used to summarize the view found in Figure 11, and shows how the processes have been automated and how the technical components used in this step are integrated and used.

Plan exam and student activities

Period/prompt	Beginning of Semester
Input	-
Actors	Exam Office, Faculty, Students
Changed processes	Request dependencies, apply for accommodation, create plan (automatic)
Artefacts	Exam plan
Outcome	Automatically created exam plan based on different constraints and dependencies
Tools used	University system, time planning component, portals

TABLE 10: VIEW DESCRIPTION: PREPARATION 1.1 IMPROVED

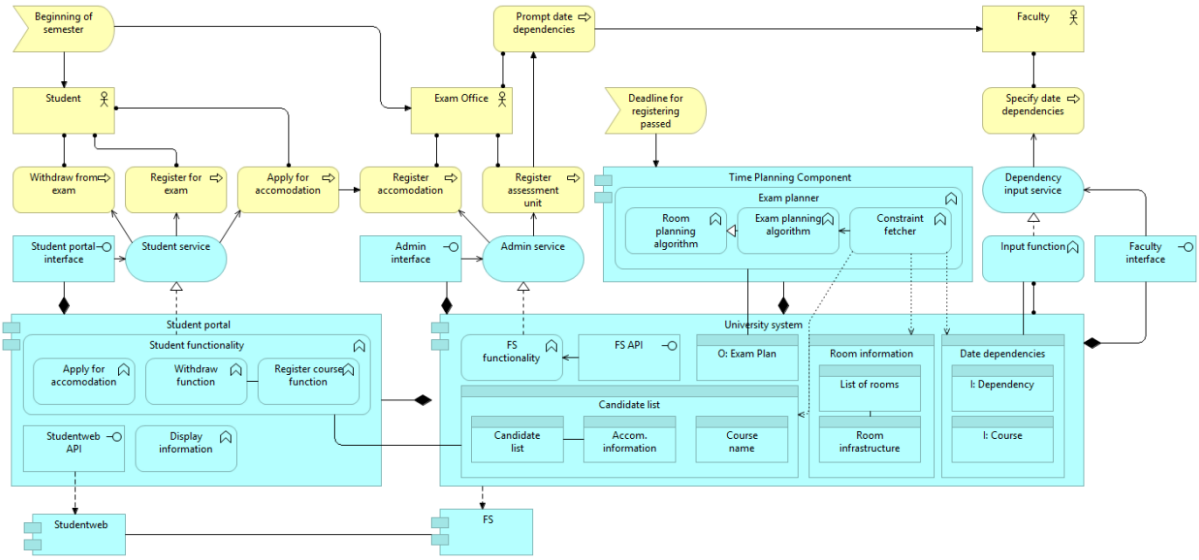


FIGURE 11: IMPROVED PREPARATION: PLAN AND STUDENT VIEW

Previously, the faculty receives a request prompting the creation of an exam. The exam creation is typically done in a word processing software, where the course coordinator can use the course description, and an existing question bank to create the exam. There are many sub-steps in this creation step, but they have been omitted in Figure 2. When the exam is complete, the censor has to control and sign the exam.

In the proposed solution, when the exam plan has been created and an assessment unit has been registered, the system sends a notification to the faculty. This notification is a request prompting the creation of an exam. The course coordinator can then log in to the system and chose the course to make the exam for. This could be chosen from a list of the available courses that the coordinator is responsible for. When the course has been chosen, the system automatically fills out the information, i.e., exam date, exam responsible etc.

A feature in the proposed system would suggest questions based on different tags and descriptions in the course information. These questions could be from a database shared by multiple universities cooperating. The system would guide the user through the various steps needed to create an exam.

When the exam has been created, a translating component could be used to translate the exam automatically. Following the translation, the user is tasked to assess and approve the translation. In the process, the user sets the restrictions on what aides the students can use when taking the exam. Through natural language processing, the system could also contribute to creating a censor guidance. After all of the processes in this work package are done, the exam is stored and the status is set to restricted and deactivated. Through a collaborative service, the censor and faculty can now quality assure the exam digitally. This collaborative service means that they can complete the task from separate locations, making it more dynamic.

Another task the faculty is responsible in this step is the censor management. In this task, we enforce the selection of a complaint censor, in addition to the regular censor. If all of the censors are allocated in this step, we improve a later sub-process, “Complaint”. The system could, as with the exam questions, suggest censors based on specified prerequisites, i.e. field of expertise, availability, knowledge of topic, previous experience with censoring this course, et cetera.

The digitalization of this step makes it easier to verify and quality assure the exam, as well as the ease of creating an exam. If we also include a shared database of exam questions and

answers, we can increase the flow of knowledge between various institutions and ensure that the teaching and learning outcome is on par with other universities.

Create exam and choose censor

Period/prompt	Request for exam creation
Input	Request
Actors	Course coordinator, censor
Changed Processes	Create exam, censor management
Artefacts	Exam, censor guide
Outcome	Exam created through suggestions, databanks, translation tools
Tools used	Create exam portal, shared university portal

TABLE 11 VIEW DESCRIPTION: PREPARATION 1.2 IMPROVED

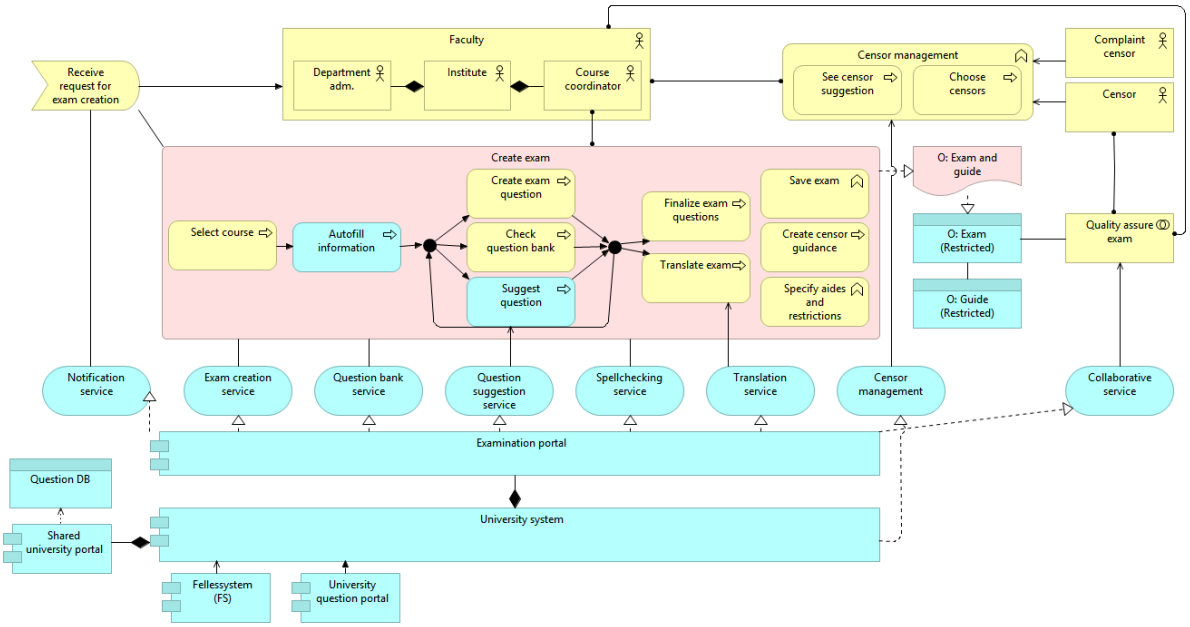


FIGURE 12: IMPROVED PREPARATION: CREATE EXAM AND CENSOR VIEW

The exam is now fully digital. Thus, the step of the sub-process "Preparation" described in Section 2.1.2.1, as the printing and distribution of the exam have now been eliminated. This saves costs related to printing and transporting, as well as removes human errors associated with printing. The distribution of the exam is now done automatically when the exam is due to start, or by activating it in the system by a technical administrator in special cases.

3.3.2 EXECUTION

As we saw in chapter 2, this entire process step is executed with manual labour and a vast number of physical objects. The exams need to be distributed to the correct location and correct

room. When they have been picked up by the chief proctor, it gets distributed to the attending students before checking their credentials. This means that the student is in possession of the exam before having to identify themselves.

With the proposed model, we see a few changes. The previous task of distributing exams from location to room to correct students is now automatic, and prompted when the specified exam should start. In special cases, a technical administrator can activate the exam in the system. Students can only get access to the exam by providing correct credentials and a key only available at the examination location. By logging into the system with their credentials, they validate their authenticity and identification. As a safeguard, the proctors are still to check the provided identification. The system can set restraints on what digital aides the student can use, but the physical aides still needs to be approved by the proctors.

In the case of students being unsure about the formulation of certain questions, they no longer have to wait for the teacher to arrive at the location. The proposed system allows for anonymous chat with an online proctor who filters and monitors the questions to a course responsible. If the question is of value to the entire group taking the exam, they get a notification with the information. Additionally, if the exam responsible have found an error in their exam, they can now transmit this information instantaneously to the students instead of travelling to geographically dispersed locations to bring the students this information.

When the students are content with their submission, they simply press a button in the system to deliver. After delivery, they present the delivery receipt screen to the proctors and the examination is done. To further ensure the authenticity of the student taking the exam, one could include a delivery code which the proctors are in possession off that the student must input before delivering.

When the exam reaches the end of its allotted time, it gets locked and deactivated. The exams are now stored in the cloud, and will be available for the censor. By having instant online versions of the exam, we remove the process of collecting, sorting, and transporting the exams after completion.

Execution

Period/prompt	Exam period
Input	Credentials
Actors	Students, proctors
Processes	Digital exam submission
Artefacts	Digital receipt
Outcome	Successful execution of exam
Tools used	Digital exam portal

TABLE 12: VIEW DESCRIPTION: EXECUTION IMPROVED

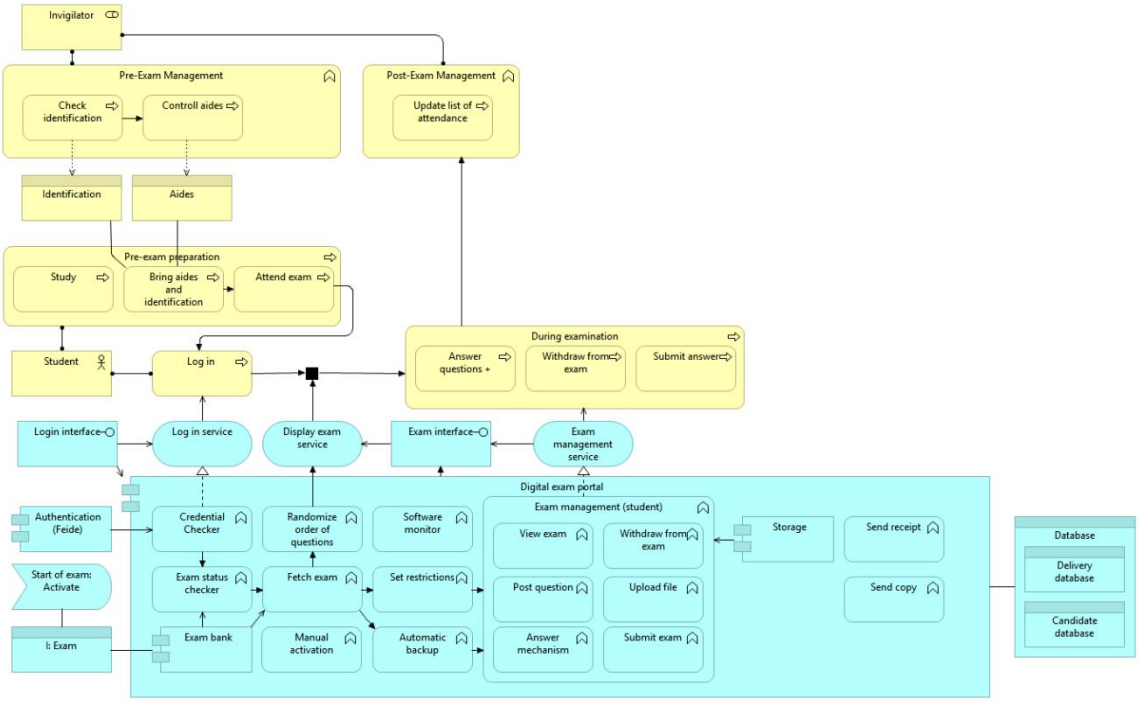


FIGURE 13: IMPROVED EXECUTION VIEW

3.3.3 CENSORING

The current censoring process consists of many steps before the actual censoring begins. The exam submissions are scanned or copied manually. This is a task that uses many resources and man-hours, in addition to the tediousness of the manual labour. After the submissions have been copied or scanned, they are sent by either e-mail or regular mail to the assigned censor. This means that it takes some time after the completion of the exam until the censor gets a hand on their copy. When the exams have been graded, (usually done in a digital spreadsheet), a physical copy is sent to the institute. The institute then verifies the censoring before sending the censor scheme to the exam office. At the exam office, they manually punch in the grades into FS, before physically archiving the grades and exam submissions.

In the proposed model of the new process, the censor receives the exams immediately following the end of the exam. This allows the time-consuming distribution of exam submissions to the censor, to be omitted; freeing up resources and the department administration. By automating this distribution process, we already see the censoring process improve.

Once the censoring is complete, it gets stored and sent to the institute and exam office. They verify and accept the censoring, prompting it to be automatically uploaded to FS. Assuming the censor added justification in the digital censor scheme, the two actors in this step can choose to include it in the information sent to the student. By including this functionality, the entire step "Justification" in the examination process can be excluded and thus simplifying the process further. Removing the need to manually punch in the grades in FS and the need for a physical storage, the process becomes more streamlined and economic.

Censor	
Period/prompt	Immediately after exam
Input	Exams
Actors	Censor, Institute, Exam office
Processes	Examination grading
Artefacts	Censor forms, justification
Outcome	Exams censored along with justification
Tools used	Censor portal

TABLE 13: VIEW DESCRIPTION: CENSORING IMPROVED

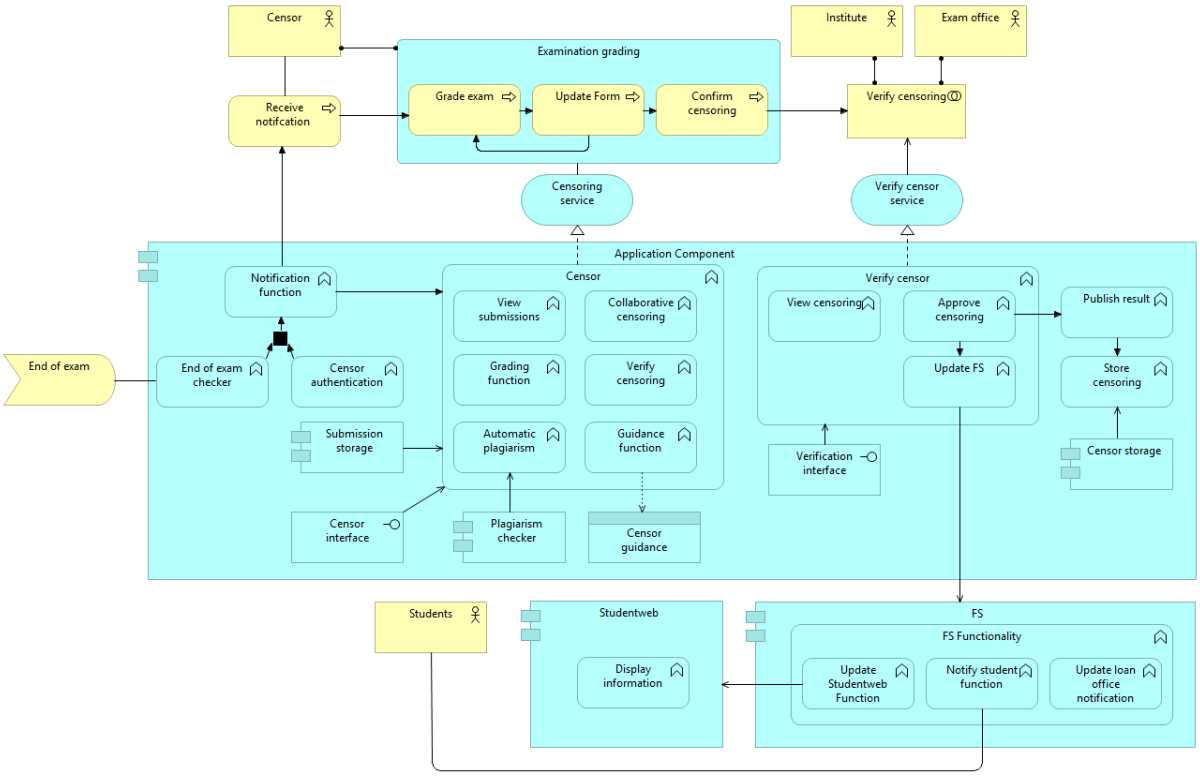


FIGURE 14: IMPROVED CENSORING

3.3.4 JUSTIFICATION

It is already clear that digitalizing this process step will improve the process. The Faculty of Information Technology and Electrical Engineering (formerly known as IME) have had a web-based system for handling justification. At other faculties, this process starts with students printing out and filling out justification forms, which then has to be handled by the respective faculties. After the form is delivered, many administrative processes have to be started, requiring many unnecessary man-hours and resources. The web-based system at IME lead to them using approximately 50% less resources on administrative processes than the other respective faculties at the university [22].

In the current solution, the different faculties handle justification in their own manner. Each process has some deviation to the model shown in Figure 6. If the university makes it a requirement for the censors to fill out the justification for each answer in the examination submission, this step can be merged with the previous step in the process, Censoring. By including this as a step in that sub-process, the information related to the censor and grade becomes more wholesome and complete. Automating the distribution of justification along with the grade is a huge benefit and major improvement to the process.

If this is to be a requirement in the future processes, we see a great improvement in the processes as we manage to eliminate an entire sub-process; which in terms, frees up a lot of resources associated with this step. There could, however, be cases where the responsible stakeholders want to withhold the justification; and only giving it to students who asks for it. We could still force the requirement that each censoring should include a hidden justification, only displaying it after a student request.

The inclusion of justification with the grade will greatly benefit the stakeholders in that sub-process. A rough estimation done by Fundator AS shows that including the justification instantly could save up to 4.850 man-hours (or roughly 2.5 FTEs) on a yearly basis [23].

3.3.5 COMPLAINTS

When the student received either the grade or the justification, the student could prompt a complaining process. This could be motivated by their goals and drivers. If they are not content with the result, they can file a complaint. In the current situation, the process of filing a complaint requires the student to find the form online, print it out, fill it out, and then either send it by mail or delivering it to the faculty. Again, a manual process with physical objects. The faculty receives the complaint and has to register the case in the archive system (ePhorte). Following the registration of the case, they have to allocate a new complaint censor, or contact a complaint censor if they already exist in the system. The exam is then fetched and distributed to the complaint censor. The rest of the sub-process complaints continues with the sub-process "Censoring".

The digitalization of this sub-process aims to automate many of the steps and eliminate the need for paper forms. When the student receives their grade, they can now file a complaint by simply pressing a button in their student portal. If we follow the requirement from the improved preparation sub-process, a complaint censor is already allocated. If we already have a complaint censor, we can eliminate many steps in this sub-process: When the student files the complaint, a complaint censor is notified. Upon receiving the notification, the system sends the files associated with that student's submission: the exam questions, the submission, the censor guidance. The censor form and grade should not be included as this can create bias towards the complaint censor's decision. The files are displayed in a censor interface, and the censoring can begin. This process mirrors that described in Section 3.3.3, and the improvements described in the censoring process are therefore also applicable here.

This view is identical to the improved censoring view. The only difference is that the prompt for starting the process is a student filing the complaint in the system, and not the end of the exam.

3.4 BENEFITS

After discussing the importance of process improvement, the reader was presented with the motivation behind digitalizing the processes, before an overview of a possible 'to-be' solution was presented. In the current chapter, we will discuss some of the benefits realized through the new digital processes.

We have seen how the goals of NTNU is to create different forms of value for both the organization itself, and the surrounding world. Unfortunately, many resources are spent unnecessarily on the current examination process. Through cutting resources and man-hours needed for the examination process, we free up a lot of these resources which can be spent on other value creating activities.

The goals of the examination presented previously, can be classified as the strategic objectives of the organization, in regards to examination. As we saw in Table 9, the typical output of process improvement is related to the strategic objectives, and we will now examine how they correlate.

Teaching and learning outcomes of the examination is related to what the student can actually learn in during the course. This bullet point does not specifically have something to do with the examination, but if a digital examination raises the validity, i.e. how valid an exam is related to the learning objectives [20], the students will have a better opportunity to express their knowledge.

Through digital examinations, we might have to rethink the way we evaluate students. This could in terms implicate that a new form of evaluation is required to properly assess the submissions in digital exams. With infrastructure and the spatial issues surrounding digital examinations described in, we could see an increase in home-exams, i.e. more open-book exams. This would imply that censoring takes longer time as students can write longer answers, and they might not properly translate that knowledge or obtain the knowledge presented as they can use aides which are not common on traditional pen and paper exams.

One of the big set-backs with traditional exams are the practicality, especially with regards to handling the paper. Through digitalization, we simplify and remove the processes related to distribution, copying, printing, scanning, archiving, as this can be done in a digital environment. This is a great improvement of the processes, and as described in Section 3.3.4, about justification, it frees up a lot of administrative resources. Digitalizing the examination process also reduces the need for physical meetings when something has to be agreed upon, whether it is the examination plan, during the examination creation or censor control. Should the course responsible suffer illness on the day of the exam where it is necessary for him or her to physically show up, they can now answer and clarify any issues the exam attendees might have through the digital environment. Hence, simplifying and improving these processes.

When we talk about validity, we can also look on the validity of the information the students receive during an exam. As Sindre discussed, in small courses where the course responsible knows the entire class, they might be biased when giving out information and clarifying issues [20]. If we take this process online, we make sure that every student is completely anonymous when asking questions, ensuring the privacy of the student. The response from the teacher is then, presumably stripped of bias; granting a more overall valid response.

In Section 5.2, we will discuss how security is enforced through digitalizing the processes, and how this can improve the processes with regards to cheating.

We have seen how process improvements can motivate the strategic objectives and increase acceptance of the stakeholders. Process improvements simplify and can show the integration of processes related to new systems. Through process improvements, we want to maintain the core activities and refine them in a way to i.e. increase efficiency and productivity, and decrease cost and use of resources.

3.5 SUMMARY

In this chapter, we have laid the foundation for the first research question: How can digitalization support process improvement. The main elements to draw from this chapter is how process improvement can maintain and refine the core activities without them loosing purpose. Through automation, simplification, and rethinking of the current process, we have seen how digitalization of the process can lead to improvement, not only at the process core, but the organization in its entirety. Digitalization can in terms, described in this chapter, help the organization reach its strategic goals.

This page is intentionally left blank

CHAPTER 4

THREATS OF DIGITAL EXAMS

We have now seen how process improvement is important when digitalization is present in organizational transformation. When we transform manual and physical processes to digital processes, there are many new aspects we need to account for. Digitalization implies the implementation of a digital solution; and with digital solutions comes new information objects. These information objects, or assets, are things we need to protect. This chapter introduces threats, and aims to show how general threats can cause unwanted incidents using vulnerabilities in a system. After a short generalization, vulnerabilities of a digital examination are presented, with a focus on the examination environment, sets of questions associated with the exam, and the exam submissions. The shift to a digital process motivates an arrival of new threats, and these security threats are therefore presented.

4.1 Threats & Threat Sources

The reader was presented with the fault-error-failure pathology, and how it becomes a threat-vulnerability-incident when we have threats imposed by human actors. The human actors can be classified as threat sources/agents. With information systems "*a threat is manifested by a threat agent/source using a specific penetration technique to produce an undesired effect on the network*" [30]. In the threat-vulnerability-incident pathology described in [14], a threat source is the source of an unwanted incident. The pathology is part of a bigger ontology as defined by Shahmehri, Herzog and Duma. [45]

There are different ways to classify threats, but the classification we will use in this thesis is: intentional, unintentional, and random threats.

A random threat is not typically associated with a direct human involvement and might stem from technical software or hardware faults, as well as forces of nature. The technical failures might be caused by humans not properly updating software, using incompatible software components, or hard drives that stop working. Unintentional threats come in the form of humans making mistakes; i.e. due to outdated software, weak security procedures, wrong transmission of information, entering incorrect data. When we talk about security, humans are often called the weakest link, and an investigation from a committee appointed by Royal Decree [46], states that human mistakes, or unintentional threats, are one of the most important causes of incidents. An intentional threat is an attack aimed at creating an undesirable incident, and could come from both authorized and unauthorized users of the system; i.e. software attacks, theft, corporate espionage and sabotage, information extortion.

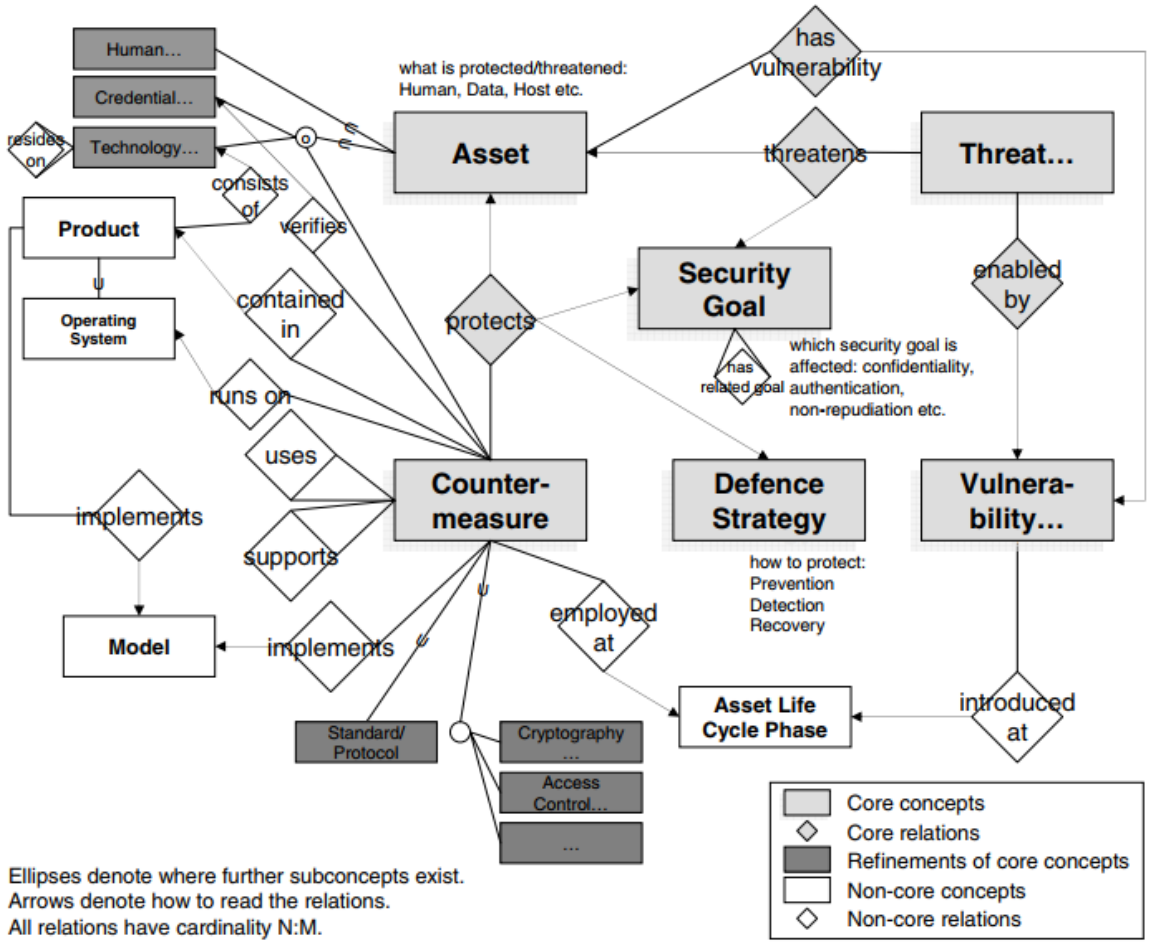


FIGURE 15: SECURITY ONTHOLOGY [45](PAGE 4)

With the addition of humans, we will now look on different ways they pose as a threat source. A threat source is the source of an unwanted incident. Depending on the motivation, resources and knowledge, we divide threat sources from intentional threats into “script kiddies”/social hackers, sophisticated attackers, hacktivists, economically driven criminals, cyberterrorists, and competing businesses. For the case presented in this thesis, we will focus on script kiddies and economically driven criminals.

A script kiddie is characterized by an individual looking for a challenge, using pre-existing tools to hack the system. They are often unaware of the consequences of their actions.

Economically driven criminals, or hackers, might in this case be someone who sells software and solutions in order to hack the examination system to give their users an unfair advantage.

When we talk about the threat-vulnerability-incident pathology, we define vulnerabilities as the weaknesses that allows a threat to cause an incident. A vulnerability is either known or unknown, and outdated software is the easiest vulnerability to exploit.

The three fundamental security attributes presented in Section 2.2, are important to mitigate the different types of threats a system might encounter. Additionally, we also have three other security attributes that mitigate threats:

- Authenticity: Is concerned with the trust and confidence of the validity of either a data object or user, i.e. is the exam submission from the authentic user?
- Accountability: this security requirement mandates that the actions are uniquely traced to the actor.
- Non-repudiation: Prevents the users to deny a transmission. It can also prevent a digital action to be denied after it is executed.

To summarize, we have been presented with threats and threat sources in a general ICT system and how they relate to each other. In the succeeding chapter, we will specify digital threats related to higher education, and more specifically, related to digital exams. We have been presented with more security requirements and in Section 4.3 we will discuss how a cheater might compromise these security requirements, and address how it can be mitigated in Section 5.1 through 5.4.

4.2 Vulnerabilities and Incidents of Digital Exams

We consider vulnerabilities to be known and unknown with regards to ICT. A vulnerability is perceived as something that compromises the security requirements of the system. In digitalization of the examination process, new threats arise. With the shift to digital exams, we want to maintain the quality that every student is presented with equal rights as to what they can do and what they have access to when taking the exam. Any unwanted behaviour, cheating, would be a compromise on the security requirements. The examination environment should not be able to grant users unfair advantages over other users. This would damage the integrity of both the software and reputation of the university. Giustolisi, Lenzini and Giampaolo states that "*whatever the framework and the way of marking tests, e-exams fail their mission unless designed to be robust to frauds*" [47]. They further state that there are several stakeholders who could profit from cheating; the examination attendees aiming to get an unfair advantage, and the administration that could manipulate scores to gain governmental funds [48].

For the sake of this thesis, the vulnerable assets in the examination process are defined as the exam questions, the examination environment, and the exam submissions. These are the assets that we want to protect.

Hovde and Owe proposes number of ways to conduct a digital exam [23]. Each of these alternatives present different vulnerabilities. NTNU have chosen to conduct digital exams using so-called BYOD exams, where the technical equipment used to conduct the exam are the student owned computers. This alternative increases the potential vulnerabilities in contrast to exams conducted on university owned equipment. With the university's own computers, they would have a greater opportunity to monitor and account for the software installed on these computers. It would limit the possibility of tampering of the machines.

A strength the pen and paper exam possess is the longevity in which it has existed. Over the course of its existence, awareness strategies and procedures have been developed and improved to prevent and detect cheating. In the digital shift, the market is still somewhat immature, and the same strategies and procedures might not be applicable to the digital exam counterpart. This weakness is something that must be addressed.

4.3 Digital threats in higher education

The reader was presented with characteristics of cheating behaviour and examples of how cheating can be executed on a normal pen and paper exam. We will now discuss some of the new cheating approaches that have been enabled through a more digital and computerized daily life.

The gradually increase in new gadgets have also led to people finding new ways to exploit them for their own benefit. This unwanted behaviour has also transmitted into higher education and end-of-term examinations. Levy and Ramim presents plagiarism, using devices such as PDAs, calculators and mobile phones, e-collaboration through instant messaging and forums, and deceiving by using another person's log-in credentials as new digital ways to cheat. [49]

In research conducted by Hillier [4], he saw a rising concern amongst the students: how can you prevent someone from looking at the answers on your screen and how do you address the issue of students hacking into the assessment or examination platform? The concerns are legitimate, and an example of the latter can be found in the several articles written by university papers ([50], [51], [52]). The articles details security breaches in the examination platform SEB, which is used at many Norwegian universities. Over the recent years, an increase in

research and news articles related to cheating in e-exams have emerged. This is not synonymous with the non-existence of cheating in traditional exams, and as put by Øyvind Hauge, the project manager for IT Strategy at NTNU: "*It's unfortunately also possible to cheat on pen and paper exams, but digital exams get more attention*" [50].

Before presenting the new threats related to digital exams, we will examine the threat sources. An obvious threat source is the student taking the exam. The reasons for cheating can range from a student prioritizing another subject and choosing to take the easy way out, or a notorious cheater who would go to extremes to get an unfair advantage in the competitive everyday life. In the case of using known vulnerabilities, like the one described in the article in Khronos [51], they could gain access to unauthorized aides within two minutes. The security breaches found in the examination environment could also be used by black-hat hackers to create software which they could sell to students that wishes to cheat. This means that the threat sources can be classified as either script kiddies or economically driven criminals.

Since vulnerabilities enables threats to manifest, we will now look at the vulnerable assets and how they can be manipulated by threat sources. The assets described in the previous chapter can be found in different steps throughout the examination process.

The first asset is the exam questions, an asset we encounter in the preparation and execution steps. A weakness of the system where the exam questions are created are the users with administrative rights. One must assume and trust that they are honest. This administrative party is the one that facilitates the access to the data object. Through a series of unintentional events, the administrative user might grant a student full disclosure of the questions and the censor guidance associated with the exam. This could be caused by the user entering incorrect data into the system or through not following proper security policies specified in the organization.

It should now be clear to the reader that due to cost, scalability and something else, that BYOD are the way digital exams are conducted, and planned to be conducted at NTNU. This implicates that the examination environment is located on the student-owned equipment.

Several researchers have conducted work into the use of BYOD exams to expose weaknesses. This work has also resulted in different mitigation strategies, but Phillip Dawson argues that they can never "*completely protect the integrity of BYOD e-exams*" [53]. This statement can intuitively be interpreted as a complete dissuasion from using student owned equipment.

The asset should only exist during the period the student is permitted to take the exam. Should a breach in this availability requirement present itself, the student might be able to alter their answers after the completed exam, which is a breach in the integrity of the exam submission asset.

In his paper [53], Dawson present five ways to hack, and cheat using the examination environment, classified as theoretical and confirmed attacks. The exploits presented are:

- Copying contents of USB to hard disk
- Virtual machine
- USB keyboard hacks
- Modifying software
- Cold boot attacks

He debates that each of these exploits require no skills of the student using the environment to execute; but some of them requires some skills to develop. All the five threats can be classified as intentional threats caused by humans, and they all breach the integrity of the examination environment, either by circumventing restrictions. Modifying the software and using virtual machines means that the student could be able to access aides that are restricted and communicate with other students taking the exam, or other people outside of the environment.

The last asset is the exam submission, found in the censoring and complaint steps. Miguel, Caballé, Xhafa and Pricto describes integrity, authenticity, confidentiality, and non-repudiation as important requirements of the exam submission [54]. The integrity is related to the prevention of manipulation of the submission after it has been delivered. Authentication of the asset mean that the censor can be sure that the submission is related to the correct student, and if a student can access their submission after completion, this breaches the confidentiality of the exam. A student should not be able to falsely deny their participation in the digital exam, as enforced by non-repudiation.

On the next page, a few threats related to the different assets can be found. Along with the threats, we will see whether they can be classified as cheating, and the nature of the threat. To further stress what have been said before, this is not a complete picture of the security threats associated with digital examination.

Threat	Cheating	Nature of threat with examples
Exam questions		
Giving access to unauthorized users	If intentionally	Unintentional: Wrong input or configuration of access controls. Intentional: Give students access
Questions are lost due to attack on databases	If student is behind the attack	Intentional
Disclosure of questions to student before taking exam	If intentional	Unintentional: Weak security policies Intentional: Given access
Exam environment		
Impersonation and deception	Yes	Intentional: Logging in with false credentials, using Virtual machines or modified software
Circumventing restrictions	Yes	Unintentional: Not updated software Intentional: Using Virtual Machines
Inject text from USB-device	Yes	Intentional: Attack on the system
Modifying software to open the lockdown	Yes	Intentional: Modifying software is definitively an intentional attack
System is available before the exam	If intentional	
Exam submission		
Unauthorized access to the submission	If misuse and awareness	Random: Faults embedded in software Unintentional: incorrect configuration Intentional: Software attacks
Manipulation of delivered exam	Yes	Intentional: Non-repudiation is a breach of the system
Submission is associated with wrong submitter	If intentional	
Student successfully denies ties to submission	Yes, falsely denying attendance	

TABLE 14: EXAMPLES OF THREATS RELATED TO ASSETS

In correlation to the examples of cheating presented by NTNU, we can assess that BYOD exams enables the copying of the answer from the internet, answer is prepared by another person, and enabling the use of illegal aides during an exam. This chapter proves that the cheating picture associated with digital exams is complex, and does not present all the possibilities of digital cheating.

4.4 SUMMARY

It can unmistakable be argued that with technical solutions, new security threats arise: as there will always be vulnerabilities that can be exploited. We have previously accounted for the motivation of cheating, and it will undoubtedly still exist, even the new environment. There are new vulnerabilities that can facilitate cheating, and these new security threats needs to be addressed.

This page is intentionally left blank

CHAPTER 5

COUNTERMEASURES THROUGH DIGITALIZATION

Up until this point, we have seen how digitalization of the examination process brings benefits through process improvement. But, with new technology comes challenges. This thesis concentrates on the challenge academic cheating. Pertaining to cheating, we have seen how a digital system presents new security threats that does not exist in the current situation. As cheating causes deterioration of the integrity of assets related to the exam, we need protect these assets. The chapter begins with an introduction to a set of safeguards used to protect assets. These safeguards, or countermeasures, can be described as security controls. The aim of this chapter is to analyse whether process improvement can support countermeasures to the vulnerabilities and threats defined in the preceding chapter.

When the countermeasures have been presented, the reader will find a risk assessment. This risk assessment tries to address some unwanted incidents related to the digital examination, and suggests what countermeasures and strategies the university could deploy. Then we present two risk matrices to visually show how the countermeasures affect the consequence and likelihood of a risk.

5.1 COUNTERMEASURES

Countermeasures are measures to be implemented in order to secure the specified non-functional requirements of a system. The countermeasures depend on the consequences and possibilities that incidents and failures occur. When choosing countermeasures, it is typical to look on a trade-off between cost of the system, the cost of incidents and the cost of implementing the countermeasures. In Figure 15 we see a visual representation of the security ontology described by Shahmehri, Herzog and Duma [45], which can be used to ascertain that a countermeasure protects an asset and a security requirement through defence strategies.

The ontology also defines a classification of countermeasures by showing various sub-concepts of countermeasures and their specializations. The classification can be found in Figure 16 on the next page. Their ontology comprises of 133 different countermeasures, and this chapter will look at some of these countermeasures and see how they can be implemented by digitalizing the processes of an examination.

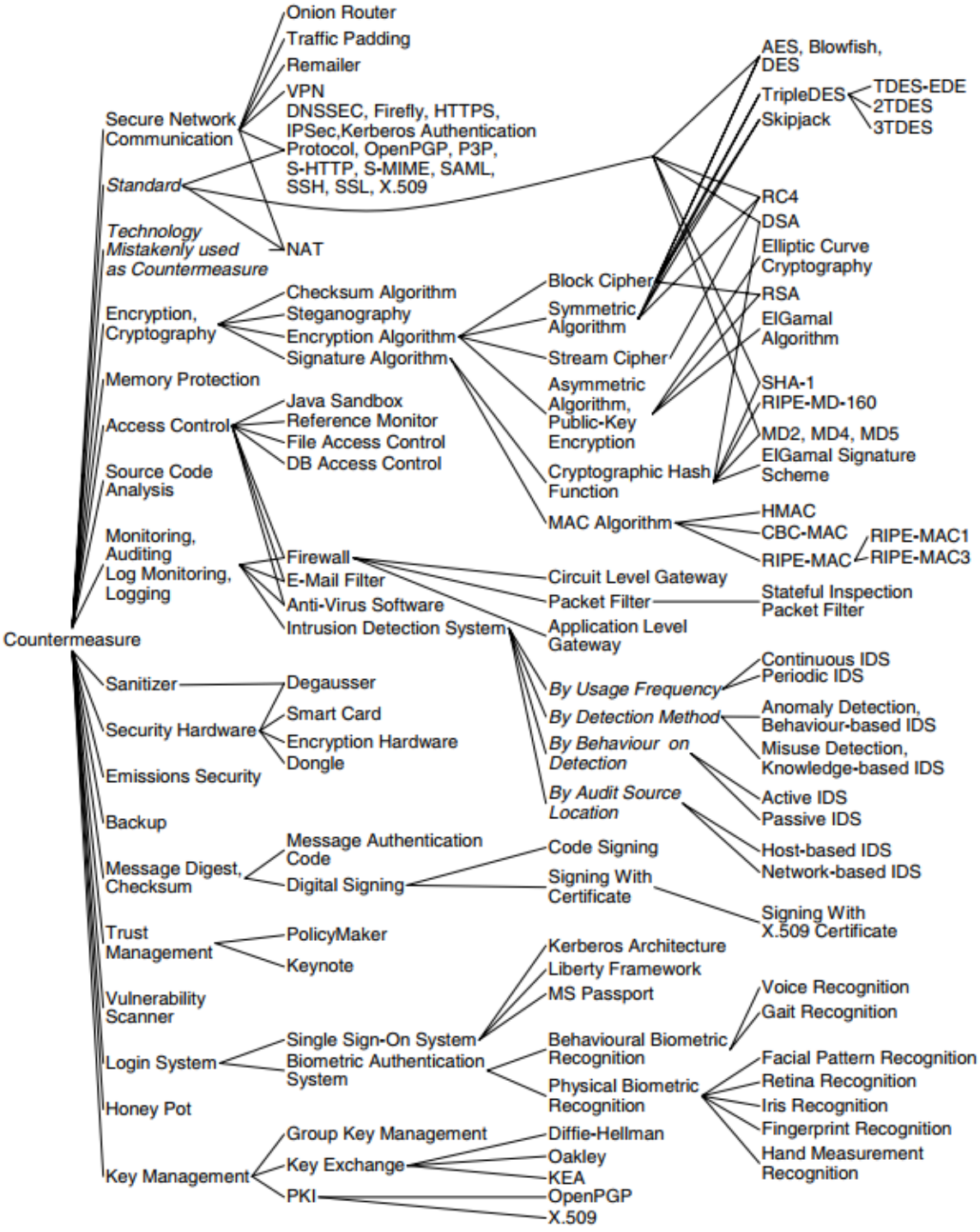


FIGURE 16: COUNTERMEASURE CLASSIFICATION [45] PAGE 7

5.1.1 SECURITY CONTROLS

With regards to security, we use security controls as countermeasures. These countermeasures are used to avoid, detect, mitigate, or minimize the potential risk to the assets of the system. Northcutt classifies the security controls into two categories [55]: when they are used, and the terms of their nature. Table 15: Security Controls – Temporal and Table 16 shows the classification of the security controls. The security controls are designed to ensure that a user is who he claims to be, that the integrity of the information is upheld, and that the information needed is available.

Security controls: When they are used

Preventive (before)	Prevent the incident from occurring
Detective (during)	Identify and classify incident when its occurring
Corrective (after)	Limit damage caused by incident

TABLE 15: SECURITY CONTROLS – TEMPORAL

Security controls: Terms of nature

	Administrative	Technical	Physical
EXAMPLES	Security awareness training, incident response systems	Anti-virus software, Firewalls, authentication mechanisms	Locked doors, surveillance cameras

TABLE 16: SECURITY CONTROLS - NATURE

5.2 COUNTERMEASURES THROUGH PROCESS IMPROVEMENT

Before looking at the countermeasures to new security threats, it would be fair to discuss how a digital exam can tackle some of the current forms of cheating one might find at a university.

In large examination halls, students taking the same course are more than often situated close to another student taking the same exam. This would mean that the ease of which one can glance over to the neighbouring table to scout for answers is relatively high. Especially pertaining to

multiple choice examinations where the answer sheet is less complex than a full-page of text. This can be addressed in the current situation by printing out multiple permutations of the answer sheets and questions, but would increase the administrative costs related to printing and transporting. One might also scramble several courses in the same room, but this would put a strain on the proctors when handing out questions, and collecting and sorting the submissions. The course responsible would also have to use more time finding his student amidst the crowd. As proposed in the view found in Figure 13, we see that the process of distributing the exams to the students contains a randomize function. This function will scramble the order of the answers and in the case of multiple choice, the order of options; and is included as a countermeasure to students with a longing look.

Digital exams are synonymous with online delivery, and exams at a location supporting network access, would mean that students could be dispersed throughout several rooms as long as they are connected. This change in the process of taking an exam would make it more flexible.

It could also be easy for a person to impersonate the student taking the exam, as long as they have a certain resemblance. The only way to tackle this is through picture-IDs that the proctors would assess. Digitalizing the process of identification implements the use of technical security protocols, as well as still maintaining the physical security protocol of picture-IDs.

If the technical security protocols only contain a user name and password, it might still not be a good enough countermeasure to impersonation. A student willing to give away their picture-ID is almost certain to also willingly sharing their security credentials. In order to ascertain proper individual identities one could resort to biometrics. Biometrics is a recognition system that matches a physical property to stored date [56]. Levy and Ramin proposes that biometrics might be a solution to properly authenticating a student.

In the digital process, users get access to the exam using a key given to them at the examination location. This key is part of the access control granting the student on premise the ability to execute the exam in the examination environment. As proposed in the detail of the improved process, the proctors could be in possession of a different delivery code which the student should input. If we enforce the students to input this key with an onlooking proctor, we include the administrative security protocol of the ‘four-eye principle’: two individuals approve the action before it is taken.

In the master thesis written by Søgaard we see how altering the source code of the examination environment can be used to hack the software, giving the user unfair advantages [57]. Given the countermeasure classification shown in Figure 16, we could implement Source Code analysis, meaning that the environment cannot be run if there has been tampering with the software. This ensures that every student is in possession of equal possibilities.

A strength the pen and paper exam possess is the longevity in which it has existed. Over the course of its existence, awareness strategies and procedures have been developed and improved to prevent and detect cheating. In the digital shift, the market is still somewhat immature, and the same strategies and procedures might not be applicable to the digital exam counterpart. This weakness is something that must be addressed.

Additionally, the proctors we find at most of the exams conducted at NTNU, are senior citizens. a group of the population that might not be the most tech savvy. Phang et. al summarizes this "*The elderly population being less familiar with IT implies that issues pertaining to their acceptance of information systems (IS) deserve special attention*" [58]. They might not be able to distinguish proper and improper use of the system. If we include education through security awareness training, we can improve the perceived acceptance of the system.

5.3 Risk Assessment

In the following chapter, the reader will be introduced to some unwanted incidents, and the assessment of the risks they impose.

For unacceptable risks, in this case cheating, we want to select countermeasures that either reduce the possibility or consequence of the risk. This can be achieved through four main strategies: avoid, reduce, transfer, and accept.

- Avoiding a risk would mean to choose a different approach than the one used, or to avoid the activity. The strategy of avoiding is usually perceived as a last resort.
- Reducing a risk is the most common strategy. It ensures that the activity is still doable, by having measures to reduce the negative outcome of the risk.
- Transferring the risk is to let another party handle a task that is deemed too risky for the organization. An example of transferring risks is hired protection at big social events.
- Acceptance of the risk is the strategy chosen for risks that have small negative outcomes and possibilities.

Risk assessment and risk matrix are used to maintain trust in the system, maintain the quality of service, protect the employees, and to spread competence while addressing risks.

 # Unwanted Incident 1

Threat source	Exam attendees
Incident	Students can look at the screens of other students for the answer to questions they are unsure about.
Probability	Likely
Consequence	Major, Worst case, you get an unfair advantage and get expelled.
Strategy	Avoid
Countermeasure	Randomize question order and scramble options functionality in the system, disperse the courses throughout the location

TABLE 17: UNWANTED INCIDENT #1

 # Unwanted Incident 2

Threat source	"Script kiddie"
Incident	Student gets access to aides that aren't approved. This could be instant messaging, internet, files on device
Probability	Unlikely
Consequence	Critical
Strategy	Avoid
Countermeasure	Online invigilation through monitoring

TABLE 18: UNWANTED INCIDENT #2

 # Unwanted Incident 3

Threat source	Student who bought illegal software
Incident	Student has a modified version of the software, granting permission to access illegal aides
Probability	Certain, if software is easily accessible
Consequence	Major, Worst case, you get an unfair advantage and get expelled.
Strategy	Reduce risk
Countermeasure	Source code analysis and monitoring, if the students know that they are being monitored, the probability of them using it is lowered

TABLE 19: UNWANTED INCIDENT #3

There are as described in the previous chapter, many more security threats and potential unwanted incidents. In this chapter, we have included three examples, just to give the reader a taste of how it can be used in a risk matrix to assess the impact of the countermeasures.

5.4 Risk Matrix

Based on the risk assessment described in the previous section, we can produce the risk matrix found in Table 20. This risk matrix represents the unwanted incidents as indicated by their consequence and probability.

CONSEQUENCE	4. Critical		U2		
	3. Major			U1	U3
	2. Moderate				
	1. Insignificant				
		1. Rare	2. Unlikely	3. Likely	4. Certain
	PROBABILITY				

TABLE 20: RISK MATRIX PRE-COUNTERMEASURE

In Section 5.1.1 and 5.2, we discuss probable security mechanisms and countermeasures to lower either the consequence or probability of the risk of the unwanted incident. Table 21 shows how the risks are affected

CONSEQUENCE	4. Critical				
	3. Major	U1	U2		
	2. Moderate	U3			
	1. Insignificant				
		1. Rare	2. Unlikely	3. Likely	4. Certain
	PROBABILITY				

TABLE 21: RISK MATRIX POST-COUNTERMEASURE

5.5 Summary

It is apparent that we need to address the new security threats that emerges in technical solutions and processes. After reading this chapter, the reader should have a clearer picture as to how process improvement reduce the likelihood or consequence of a risk through countermeasure support.

This page is intentionally left blank

CHAPTER 6

VALUE CREATION

6.1 Strategy and Value creation

To meet the NTNU digitalization strategy objective is not a matter of re-engineering candidate business processes by replacing all or part of them through digitalization only. Over and again news media have reported failed implementation of IT based enterprise systems in the public as well as the private sector. To pave the way for a successful digitalization and the accompanying technology uptake it is paramount that the actors and stakeholders impacted by such a transition are engaged in and actively participates in the change process. If actors and stakeholders experience no added value in the process the digitalization will fail dramatically. Thus, the enterprise modelling methodology does not guarantee any stakeholder engagement nor focuses on the value added for the actors as such and therefore this calls for formal methodology that supports value creation in close cooperation with actors and stakeholders. This chapter introduces Value Proposition Design as a candidate methodology for driving the digitalization of examination processes.

6.2 Initial Application of Value Proposition Design

The key principle of Value Proposition Design is about applying tools and processes to the search for value propositions that meet the strategy objectives with the focus on what the customers (in this case NTNU stakeholders and actors) want and then keeping them aligned what they want post search. Value Proposition Design shows how to use a template (Value Proposition Canvas) to design and test value propositions in an iterative search for customers want, thus turning knowledge into action.

The purpose of Value Proposition Design [59] is to help the users of the template to create products and services the customer wants. This can in terms be used to turn an idea into reality. As described in Section 2.3, VPD looks at customer profile and the value proposition associated with that profile.

Customer profiling consists of the customer jobs, and pains and gains associated with the customer jobs. The value proposition consists of which features and services can be used to get the jobs done, and the pain relievers and gain creators.

The elements of the template can be found in Table 22. I will attempt to assess whether the design can be used in the case of NTNU. In order to assess this, we need to look at the elements of the template, and see how they can be translated to fit NTNUs digitalization process. From

the table, we can therefore conclude that three main things to address for NTNUs users and stakeholders are (Customer profiling):

1. Jobs done
2. Pains
3. Gains

Pains	Undesired outcomes, problems, characteristics Obstacles Risks (undesired potential outcomes)
Gains	Required gains Expected gains Desired gains / Unexpected gains
Features	Physical/tangible Intangible Digital Financial
Pain relievers	Improve mood Produce resource savings Fix underperforming solutions End difficulties and challenges Eliminate risks Eradicate errors made by users
Gain creators	Create savings that please customers Produce expected outcomes Outperform current VP Create positive social consequences Fulfil desire, do something specific Match customers' criteria Help adoption (lower cost, fewer investments, lower risk, better quality, improved performance)

TABLE 22: ELEMENTS OF VPD (COURTESY OF [59])

Three main things to address for the digitalization of exam (Value proposition)

1. Features, products and services
2. Pain relievers
3. Gain creators

6.3 VPD AND EXAMINATION PROCESS

Customers are the actors and stakeholders of the processes affected through digitalization. The customers can therefore be siphoned from the views presented in Chapter 2.

- Students
- Course responsible
- Faculty
- Censors
- Exam office
- Proctors

Additionally, we want to create a digital solution that handles the examination process. In this digital solution, as proposed in Section 3.3, we also have the actors named 'technical staff'. Each of these customers would want and need different services, and therefore, different Templates. An example of a customer profile for Students is shown below.

Students		
Customer profile		
Jobs done	Pains	Gains
-Register & withdraw from exam -Apply for special accommodation -Take exam -Register claims for justification and complaints	-Physical objects printed, signed and mailed. -Reduced motor skills -Slow output of knowledge -Fear of cheating -Tedious processes	No more paper and pencil Improved writing speed Known platform Ease of use Easy access to exam and exam info pre-and post-exam as well

	Value proposition	
Features, services	Pain relievers	Gain creators
-Application service -Examination service -Claims service	-Form functionality -Exams typed on keyboard	Dedicated feature set for student Collaboration systems Information search and retrieval Examination service access

TABLE 23: VPD EXAMPLE FOR CUSTOMER PROFILE: STUDENT

With VPD we can find the best fit between the processes and methods. The toolbox approach supported by VPD means that we can test business hypothesis and summarize the lessons learned on progress boards. This can in terms be used as a tool in turning knowledge into action, which is the weakest step in the change processes.

6.4 SUMMARY

It is evident that the enterprise modelling principles presented with the process improvements are supported by the digitalization of exams. However, it does not guarantee the acceptance of any stakeholder engagement nor focuses on the value added for the actors as such and therefore this calls for formal methodology that supports value creation in close cooperation with actors and stakeholders. Through examples and assumptions, it is clear that Value Proposition Design can be used to drive the digitalization, focusing on points that are not addressed by process improvement.

This page is intentionally left blank

CHAPTER 7

DISCUSSION

In this chapter, we will evaluate the results of the investigation and research. For each part of the thesis, we will discuss the expectations and reasons for the results we got. Then we will look on the limitations on the research and suggest further work to be done.

7.1 Process Improvements through Digitalization

The first question postulated was with regards to process improvements, and how it can be supported through digitalization of exams. The method used to asses this question was to first do a mapping of the current situation and processes. The models created from the foundation literature did not include the processes related to digital exams we have today. The rationale for this was that the university has not come far enough in the process to show the maturity of that process. This is therefore a limitation in the research, as we only assess the current traditional pen and paper exam.

It did, however become evident that there were a lot of issues with the current practice. Whenever a student had to file a claim for either special needs, justification, or complaints, they had to find the form online, print it out, fill it out, before finally delivering it to the correct department. One would think that this was the end of that process, but no. When the claim was received at the proper department, they had to send it to the correct stakeholders.

Similarly, the processes related to creating the examination plan was cumbersome where both the faculty and exam office created their separate plans, before sorting out differences and finally agreeing on a plan. This was first done in a worksheet or time planning software, before printed out and manually put into FS. Then, when every student has registered or withdrawn from the exam and the deadline for registration passed, they had to include room reservations in the plan; manually accounting for special needs and other cases.

The creation of the exam also exists of a few backwards steps. When the exam is created, in word processing software, it is taken to the censor for approval. When it is approved, the exam is sent to the department, who collects the necessary information associated with the exam. Then it is sent to the exam office who is responsible for sending it to the printer. The printers are responsible for quality assuring all of the 220.000 exams being printed out. Exams are transported to the exams through a transportation service.

These are some examples of all of the manual and resource-consuming tasks in the examination workflow, meant to reiterate that the processes are backwards and ineffective. The researcher

was not aware of all the extra steps needed in the current situation, with the physical objects having to interact with so many different employees throughout its lifetime.

Based on characteristics of process improvement, the researcher attempted to model a hypothetical 'to-be' situation. The benefits realized by the process improvements of a digital exam have been summarized in Section 3.4. Through automation and process simplification, there are several benefits supported by the proposed 'to-be' processes:

- Manual labour, paper
- Reduce errors (eliminate steps)
- Quality assurance
- Better flow of communication between departments
- Alignment of strategic goals with IT Strategy

The processes have, as discussed, not been modelled with the classic BPMN notation, but rather in ArchiMate views consisting of business and technical aspects of the organization. The rationale behind this choice was for the reader to see how the technical aspect improves automatic processes and simplifies many of the administrative tasks.

By eliminating and improving the administrative tasks, we get a surplus of resources and man-hours that can be used on value creating work. The consequences of these different improvements are that there are huge gains to get from digitalization of the examination.

For further research, it would be beneficial to create several models and views throughout the digitalization, using multiple 'to-be' situations. By doing this, we can better guide the process as a whole, showing the critical points at each step; and the benefits gained from altering the process steps.

7.2 Security Threats

For the second question, we wanted to examine some current known security threats. Before being able to assess the security threats, we had to be introduced to secure and robust systems and some qualities associated with such systems. Through this introduction, we discovered threats, and how humans are the weakest link in information systems. The humans pose as threats that knowingly or unbeknownst causes an unwanted incident through a vulnerability in the system.

When we go from a paper system to a digital system, there are new threats to account for, and in this part, we saw different ways a threat could exploit a vulnerability. Having taken courses in security earlier, the researcher was aware of the vastness of threats that exists in information systems. The challenge was to map them to the unwanted behaviour associated with cheating.

The researcher, being a student and peer, was aware of cheating in tertiary education; but not to the extent presented in some of the documents found in the investigation. The consequences of this is that we need to make sure that the threats associated with cheating are mitigated and address in a proper manner.

The research does however, contain limitations. In order to properly address the threats associated with cheating, especially at NTNU, research into student behaviour at this university would preferably be conducted. For further work, extensive research into the new security threats is advised.

7.3 COUNTERMEASURES

The second part of the second research question was concerned with how to address the new security threats discovered in part one of that research. These countermeasures were meant to be countermeasures associated with digitalization of the processes and improved processes. The systems for digital assessment are still immature, and the market is fresh. The security threats that have been found in previous research has already been attempted to mitigate through technical solutions. Because of the immaturity of the subject, finding countermeasures will be influenced by guesswork and informed assumptions.

When we digitalize a process, it is imperative that we provide the necessary support needed to properly internalize it. The longevity of the traditional pen and paper exams are a great strength, as it has meant that the procedures and policies surrounding security have been well established. When we try to internalize the new process, we need to support the training of the stakeholders associated with the reengineered process. Only through proper training, and helping the users accept the changes can we decrease the possibilities for human errors in using the system. The digital solution provides simplification and automation to remove security threats (that permeates the current situation) associated with human errors. Computerization of the processes and examination environment mean that we also get some new safeguards in addressing cheating.

Through monitoring network traffic, it is possible to determine whether a student communicates with outsiders, or uses aides on the internet. With source code analysis implemented in the system, the process of starting an exam limits students that have modified the software from accessing the exam. In digitalizing the process, we might also introduce new elements to the step of authentication when taking an exam. As discussed, a result of new security requirements might mean the introduction of biometrics, the identification through physical features. Should biometrics be an integral part of the digital examination process, the university must, as specified by the Data Protection Authority (Datatilsynet) regulate and implement it according to the Personal Data Act §12 as mandated by the Norwegian government. [60]

For further research, it is advised that a team of enterprise architects assess and observe users interacting and doing work in the digital solution.

7.4 Value Creation

In the motivation and background research, we debated the importance of an organizations' strategy and motivation. We saw how the strategy is a tool for creating value for an organization and its customers. The customers where in the case of NTNU, the stakeholders associated with the examination process. The Value Proposition Design, as proposed by Osterwalder, is a proven tool for testing out hypotheses concerned with what can create value in an organization.

It is a powerful tool for creating acceptance throughout and organization. We have debated how the stakeholders needs to relate to new and possibly depleted tasks. VPD can in that case be used to create acceptance to the changed working environment of the individual stakeholder.

The research showed that it can through acceptance and alignment of goals be used to drive digitalization of the processes. If we manage to follow up on the strategic objectives, we create efficiency, maintain the core activities, and free up new resources for new value creating work processes.

The limitations of the research associated with this research question comes from an exclusion of actually implementing it and trying it out in the organization. This is an unfortunate consequence of the researcher being on sick leave throughout the semester.

This page is intentionally left blank

CHAPTER 8

CONCLUSION AND FURTHER WORK

8.1 CONCLUSION

The thesis describes the current processes, and the bottle-necks and ineffective steps related to these processes. The current examination process of traditional pen and paper exams are characterized by a lot of manual labour and processing of physical objects. Humans being the weakest link in information systems, would also implicate that many of the tasks are subject to errors caused by humans. The cost, both economically and resource-wise, is very significant due to the unnecessary administrative tasks.

It became clear through the background research that the examination process at NTNU needs to be addressed. The processes proved to be cumbersome, ineffective and characterized by resource-demanding tasks. We saw how the current process matched the motivations and goals of an exam, and it became evident that they needed improvement.

It is stipulated that a way to tackle process improvement, is through digitalization of the examination process. When we go through the organizational transformation of digitalizing processes, we need a final digital solution to rely on. A digital system, or solution, would need to satisfy the motivations and goals of an exam while maintaining academic integrity. With digital solutions, we also get new ways to exploit the vulnerabilities of a system. These new exploits can be used to get an unfair advantage when taking an exam. As the new security threats manifests themselves, it is paramount that the organization have addressed how the system can support different countermeasures to the cheater's behaviour.

To reiterate, maintaining the integrity and core-activities found in the organization, is a clear strategic objective. Value Proposition Design is a proved and recommended method for addressing these objectives.

Bearing this in mind, we will now conclude the thesis and answer the research questions proposed in Section 1.1.

RQ1: How can digitalization of exams support user driven innovation and process improvement?

We have seen how the current examination process is characterized by unnecessary use of resources and a lot of time-consuming and tedious tasks. It is evident that digitalization support the automation, simplification, and rethinking of the current processes, while still maintaining new and refined core activities and goals. The implication is that digitalization of the examination can support process improvement, not only in the scope of processes, but the

university as a whole. New resources are freed up to work with new ways of creating value for the organization.

RQ2.1: What new security threats related to cheating arises when changing/digitalizing the processes of examination?

When we introduce a digital platform for handling every aspect of an examination, we also introduce new threats. A digital system faces different threats than a paper system. Due to differences in learning motivation established in school kids from a young age, we can never be sure that cheating can be exterminated. With the undoubtedly presence of cheating, we have found vulnerabilities in a digital solution and presented some new security threats.

So, we have new security threats enabled by the system, now we need to address them. There is always a correlation between threats and countermeasures, and the next research question will demonstrate ways of mitigation the threats.

RQ2.2: What new security measures can be supported through digitalizing the processes?

It is apparent that we need to address the new security threats that emerges in technical solutions and processes. The reader has been presented with a variety of countermeasures we might wish to include in a digital system. More specifically, the reader has been introduced to some strategies and safeguards which can in fact be used to uphold the security requirements associated with a secure and robust system.

It is evidential that digitalization can support new security measures, and how the processes can reduce the likelihood and consequence of a risk through safeguard support.

RQ3: Is it possible to use aspects of Value Proposition Design to drive the digitalization of examination processes?

To reiterate, we will again present the summary from the chapter concerned with value creation:

It is evident that the enterprise modelling principles presented with the process improvements are supported by the digitalization of exams. However, it does not guarantee the acceptance of any stakeholder engagement nor focuses on the value added for the actors as such and therefore this calls for formal methodology that supports value creation in close cooperation with actors and stakeholders. Through examples and assumptions, it is clear that Value Proposition Design

can be used to drive the digitalization, focusing on points that are not addressed by process improvement.

8.2 Further Work

Sedara talks about anticipated performance of enterprise systems (ES) and reasons why organizations fail to realize the benefits [61]. In order to ensure that digitalization of the examination process leads to process improvements, these points of failures are important for NTNU in working with implementing a digital solution:

- Concentrated only on the technical aspects, ignoring the business aspects
- Poor project scope definition
- Weaknesses in the ES design approach
- Current state of ES life cycle

When trying to realize the benefit one can reap from process improvements, it is crucial that the university not only focuses on the technical solution, but also the organizational transformation it brings. Through simplifying and changing the processes, a few business actors might need to restructure their work, lose current responsibilities, and be assigned to new tasks. This transformation of everyday organization needs to be accounted for, and taken into consideration when each incremental step is taken.

Where there is technology, there are also someone trying to exploit it in different ways. A system can never possess safeguards against every imaginable threat, as the threat picture is a never-ending evolving environment. The digital solution should however, consist of a composition of known safeguards against various types of hacking, and security measures and procedures against a breach of the security requirements. When new forms of cheating and circumventing the system are discovered, safeguards needs to be developed and integrated into the system. Until then, the university should put trust in their students' honesty and keep up with the behavioural trust management and policies they currently have.

This page is intentionally left blank

BIBLIOGRAPHY

[1] R. Eno, “The Culture of the Tang Dynasty - Indiana University,” Spring 2008. [Online]. Available: http://www.indiana.edu/~e232/13-Tang.pdf. [Accessed 04 12 2016].

[2] A. Fjerdrumsmoen, “Digital Eksamen,” 14 04 2016. [Online]. Available: https://www.ntnu.no/wiki/display/ppfntnuit/-Digital+eksamen. [Accessed 25 11 2016].

[3] M. Hillier and A. Fluck, “Arguing for e-exams in high stakes examinations,” in *Electric Dreams - 30th ascilite Conference*, Sydney, 2013.

[4] M. Hillier, “The very idea of e-Exams: student (pre)conceptions,” in *Australasian Society for Computers in Learning in Tertiary Eductaion Conference*, Dunedin, 2014.

[5] V. Connelly, J. E. Dockrell and J. Barnett, “The slow handwriting of undergraduate students constrains overall performance in exam essays,” *Educational Psychology - An International Journal of Experimental Educational Psychology*, no. 25, pp. 99-107, 2005.

[6] M. Connor, “Handwriting performance and GCSE concessions,” *Handwriting Review 9*, pp. 7-21, 1995.

[7] P. Parr, N. Levi and K. Jacka, “Unspeeded Examinations: An Equitable and Practical Method of Assessment,” in *Equity and Access Conference*, Melbourne, 1995.

[8] S. Sülzenbrück, M. Hegele, G. Rinkenauer and H. Heuer, “The death of handwriting: secondary effects of frequent computer use on basic motor skills,” *Journal of Motor Behavior*, no. 3, pp. 247-251, 2011.

[9] M. A. Steiner, “Cheating in School,” *The School Review*, no. 7, pp. 535-549, September 1932.

[10] T. Kvenild, “Cheating on exams,” NTNU, 9 December 2015. [Online]. Available: https://innsida.ntnu.no/wiki/-/wiki/English/Cheating+on+exams. [Accessed 29 June 2017].

[11] Kunnskapsdepartementet, *Lov om universiteter og høyskoler*, 2005.

[12] S. S. Otterlei, “Flere tas i juks på universiteter og høgskoler,” NRK, 25 January 2017. [Online]. Available: https://www.nrk.no/hordaland/flere-tas-i-juks-pa-universiteter-og-hogskoler-1.13340451. [Accessed 18 June 2017].

[13] J. Svarstad, “Slik avslører de studentene som jukser,” Forskerforum, 24 January 2017. [Online]. Available: http://www.forskerforum.no/slik-avslorer-de-studentene-som-jukser/. [Accessed 18 June 2017].

[14] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Transactions on dependable and secure computing*, pp. 11-33, Jan-March 2004.

[15] C. E. Reinholtsen, “Digital Exam,” NTNU, 11 October 2016. [Online]. Available: https://innsida.ntnu.no/wiki/-/wiki/English/Digital+exam. [Accessed 29 May 2017].

[16] S. Sahay and D. Robey, “Transforming Work Through Information Technology: A comparative case study of Geographic Information Systems in County Government,” Information Systems Research, 1996.

[17] J. Krogstie, Model-Based Development and Evolution of Information Systems - A Quality Approach, London: Springer, 2012.

[18] NTNU Teaching Excellence, “NTNU Teaching Excellence,” [Online]. Available: http://www.ntnu.edu/teaching-excellence. [Accessed 13 12 2016].

[19] NTNU, “Knowledge for a better world. NTNU - internationally outstanding,” NTNU , Trondheim, 2011.

[20] G. Sindre and A. Vegendla, “e-Exams and Exam Process Improvement,” in *Utdanning of Didaktikk i IT-faga (UDIT) / Norwegian Information Security Conference*, Ålesund, 2015.

[21] F. Barstad, B. Smilden and A. Sidselrud, “Digital Assessment - A National Coordination project,” in *EUNIS Conference*, Dundee, 2015.

[22] P. Hovde, “Sluttrapport fra forstudie,” Studieavdelingen, 2013.

[23] P. Hovde and S. O. Olsen, “Utredning - Digital eksamen NTNU 2015-2019,” Fundator, 2015.

[24] Ekspertgruppen for Digital vurdering, *Digital vurdering og eksamen - en juridisk vurdering,* 2014.

[25] C. S. Dweck, “Motivational Processes Affecting Learning,” *American Psychologist,* no. 41, pp. 1040-1048, 1988.

[26] E. Anderman, T. Griesinger and G. Westerfield, “Motivation and cheating during early adolescence,” *Journal of Educational Psychology,* no. 60, pp. 84-93, 1998.

[27] J. W. Michaels and T. D. Miethe, “Applying Theories of Deviance to Academic Cheating,” *Social Science Quarterly,* no. 4, pp. 870-885, 1 December 1989.

[28] D. A. Rettinger and Y. Kramer, “Situational and Personal Causes of Student Cheating,” *Research in Higher Education,* no. 3, pp. 293-313, 02 December 2008.

[29] D. L. McCabe and L. K. Treviño, “Individual and Contextual Influences on Academic Dishonesty - A Multicampus Investigation,” *Research in Higher Education,* no. 38, pp. 379-396.

[30] F. Farahmand, S. B. Navathe and P. H. Enslow, “Managing vulnerabilities of information systems to security incidents,” in *ICEC '03 Proceedings of the 5th international conference on Electronic commerce*, Pittsburgh, 2003.

[31] R. S. Kaplan and D. P. Norton, Strategy Maps: Converting Intangible Assets Into Tangible Outcomes, Harvard Business Press, 2004.

[32] A. Kambil, A. Ginsberg and M. Bloch, “Re-Inventing Value Propositions,” New York University, New York, NY, 1996.

[33] UNINETT, “eCampus,” [Online]. Available: https://www.uninett.no/ecampus. [Accessed 01 12 2016].

[34] A. Lindholm, “Flerdobling av antallet digitale eksamener,” Khrono, 14 July 2016. [Online]. Available: https://khrono.no/2016/06/digital-eksamen-varen-2016. [Accessed 29 July 2017].

[35] E. Tønnesen, T. Lie and H. Larsen, “Nå er det offisielt: NTNU blir størst i Norge,” Universitetsavisa, 19 June 2015. [Online]. Available: http://www.universitetsavisa.no/politikk/article51148.ece. [Accessed 28 May 2017].

[36] A.-L. Lande, “UiO Digital Eksamen,” in *Erfaringssamling digital eksamen*, Gardermoen, 2017.

[37] C. Heesch, “Nye eksamenslokaler i Silurveien 2,” 20 September 2016. [Online]. Available: http://www.med.uio.no/studier/aktuelt/aktuelle-saker/2016/nye-eksamenslokaler-i-silurveien-2.html. [Accessed 29 May 2017].

[38] O. P. Ottersen, “Milepæl for Digital Eksamen,” Rektors Blogg - UiO, 17 January 2017. [Online]. Available: http://www.uio.no/om/aktuelt/rektors-blogg/2017/milepel-for-digital-eksamen.html. [Accessed 28 May 2017].

[39] Norwegian Business School BI, “DigiEx,” [Online]. Available: https://www.bi.no/forskning/learninglab/faculty-helpdesk/undervisning-og-eksamen/digiex/. [Accessed 24 11 2016].

[40] J. B. N. Trapnes, “Digitalization of Exams - Strengths and limitations of the Business Model Canvas when applied to Digitalization at NTNU,” Trondheim, 2016.

[41] S. Zahran, Software Process Improvement: Practical Guidelines for Business Success, John Wiley & Sons, Ltd., 1997.

[42] Appian, “What is Process Improvement in Organizational Development?,” Appian, 2017. [Online]. Available: https://www.appian.com/bpm/process-improvement-organizational-development/. [Accessed 1 June 2017].

[43] K. Sandkuhl, J. Stirna, A. Persson and M. Wiβotzki, Enterprise Modelling - Tackling Business Challenges with the 4EM Method, Springer, 2014.

[44] Felles Studentsystem, “Institusjoner som bruker FS,” FS, 1 June 2015. [Online]. Available: http://www.fellesstudentsystem.no/forvaltning/institusjoner/index.html. [Accessed 1 August 2017].

[45] N. Shahmehri, A. Herzog and C. Duma, “An Ontology of Information Security,” *International Journal of Information Security and Privacy,* pp. 1-23, 2007.

[46] Norges Offentlige Utredninger, “Digital Sårbarhet - sikkert samfunn,” Departementenes sikkerhets- og serviceorganisasjon, Oslo, 2015.

[47] R. Giustolisi, G. Lenzini and B. Giampaolo, “What Security for Electronic Exams,” in *Risks and Security of Internet and Systems (CRiSIS) - 2013 International Conference*, La Rochelle, 2013.

[48] CNN Staff, “Former Atlanta Schools Superintendent reports to jail in Cheating Scandal,” CNN, 3 April 2013. [Online]. Available: http://edition.cnn.com/2013/04/02/justice/georgia-cheating-scandal/index.html. [Accessed 14 June 2017].

[49] Y. Levy and M. M. Ramim, “A Theoretical Approach for Biometrics Authentication of e-Exams,” 2007.

[50] I. Rygg, “-Vanskeligere å jukse på digital eksamen,” Universitetsavisa, 29 May 2017. [Online]. Available: http://www.universitetsavisa.no/student/2017/05/29/%E2%80%93-Vanskeligere-%C3%A5-jukse-p%C3%A5-digital-eksamen-66572.ece. [Accessed 16 July 2017].

[51] M. Njåstad, “-Svært enkelt å juksa på digital eksamen,” På Høyden, 19 May 2017. [Online]. Available: http://pahoyden.no/2017/05/svaert-enkelt-juksa-pa-digital-eksamen. [Accessed 16 July 2017].

[52] K. Haug, “Store sikkerhetshull i nasjonalt eksamensprogram,” Universitas, 14 September 2016. [Online]. Available: http://universitas.no/nyheter/61708/store-sikkerhetshull-i-nasjonalt-eksamensprogram. [Accessed 16 July 2017].

[53] P. Dawson, “Five Ways to Hack and Cheat with Bring Your Own Device (BYOD) Electronic Examinations,” *The British Journal of Educational Technology,* 2015.

[54] J. Miguel, S. Caballé, F. Xhafa and J. Prieto, “Security in Online Learning Assessment Towards an Effective Trustworthiness Approach to Support E-Learning Teams,” in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA),* Victoria, 2014.

[55] S. Northcutt, “Security Controls,” 2009. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/security-controls. [Accessed 25 May 2017].

[56] J. M. Williams, “New Security Paradigms,” in *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, 2002.

[57] T. M. Søgaard, “Mitigation of Cheating Threats in Digital BYOD exams,” 2016.

[58] C. W. Phang, J. Sutanto, A. Kankanhalli, Y. T. B. C. Y. Li and H. -H. Teo, “Senior Citizens' Acceptance of Information Systems: A Study in the Context of e-Government Services,” *IEEE Transactions on Engineering Management,* pp. 555-569, November 2006.

[59] A. Osterwalder, T. Papadakos, A. Smith, G. Bernarda and Y. Pigneur, Value Proposition Design: How to Create Products and Services Customers want, John Wiley & Sons, 2014.

[60] Datatilsynet, “Biometri,” Datatilsynet, 29 February 2012. [Online]. Available: https://www.datatilsynet.no/om-personvern/bruk-og-misbruk-av-personopplysninger/biometri/. [Accessed 30 May 2017].

[61] D. Sedara, M. Rosemann and G. Gable, “Using Performance Measurement Models For Benefit Realization With Enterprise Systems - The Queensland Government Approach [Case Study],” in *Global Co-Operation in the New Millenium - The 9th European Conference on Information Systems*, Bled, 2001.