BACHELOR'S THESIS

Deployment of the agile risk management with Jira into complex product development ecosystem

Asmo Saarela

Supervisor: Jari Hannu

DEGREE PROGRAMME IN ELECTRICAL ENGINEERING

2017

Saarela, A. (2017). Deployment of the agile risk management with Jira into complex product development ecosystem. University of Oulu, Degree Program in Electrical Engineering. Bachelor's Thesis, 55 p.

ABSTRACT

This work is a descriptive case study of deployment of the agile risk management with Jira into complex product development ecosystem. The context is a Development Team in Finland that is leading distributed product development for a small cell radio base station (RBS).

The quality management requirements in the ISO 9001:2015 standard have been updated and the main impact is the deployment of the risk based thinking. The Development Team in Finland has gone through a transformation from release project driven development to continuous software development. This major change requires that development processes and development support processes are also updated. Focus is in the improvement of the risk management process, methods and tools.

Rationale for risk management improvement is based on the findings in the internal quality audit and the management's intent is also taken into account. The implementation contains a new risk management process, customized issue type for Jira tool, risk management hands on training and replacement of the old spreadsheet based risk management tools. The new process replaces two earlier processes making things simpler. The unified approach covers both normal risks in the product development and product security and privacy related risks.

Agile product development emphasizes the empowerment of the cross-functional team. The results show that deployment of the agile risk management has shifted the risk management ownership to development teams instead of the release management function. The benefits of risk management for software industry and for the case study are included to motivate the use of the risk management in the daily operations.

Key words: Software development, risk based approach, expected monetary value, operational excellence, technical, product, security, privacy, quality risk

Saarela, A. (2017). Ketterän riskienhallinnan käyttöönotto Jiralla monimutkaisessa tuotekehitysekosysteemissä. Oulun yliopisto, sähkötekniikan tutkinto-ohjelma. Kandidaatintyö, 55 s.

TIIVISTELMÄ

Tämä työ on kuvaileva tapaustutkimus ketterän riskienhallinnan käyttöönotosta Jiralla monimutkaisessa tuotekehitysekosysteemissä. Työ liittyy Suomessa olevaan kehitystiimiin, joka johtaa hajautettua tuotekehitystä piensolutukiasemalle.

Laatujärjestelmän vaatimukset ovat päivitetty ISO 9001:2015 standardissa ja päivityksen suurin vaikutus on riskipohjaisen ajattelun käyttöönotto. Kehitystiimi Suomessa on läpikäynyt muutoksen julkaisuprojektiohjatusta kehityksestä jatkuvaan ohjelmistokehitykseen. Tämä suuri muutos vaati kehitys- ja kehityksen tukiprosessien päivittämistä. Huomio on riskienhallintaprosessin, menetelmien ja työkalujen parantamisessa.

Perusteluina riskienhallinnan parantamiselle on havainnot sisäisestä laatujärjestelmän tarkastamisesta ja johdon tahtotila on myös huomioitu. Toteutus sisältää uuden riskienhallintaprosessin, räätälöidyt tehtävätyypit Jira työkaluun, riskienhallinnan käytännön perehdytyksen ja olemassa olevien taulukkolaskentapohjaisten riskienhallintatyökalujen korvaamisen. Uusi prosessi korvaa kaksi aikaisempaa prosessia yksinkertaistaen asioita. Yhdistetty lähestymistapa kattaa sekä normaalit riskit tuotekehityksessä, että tuotteen tietoturva. ja yksityisyysriskit.

Ketterä tuotekehitys korostaa vaikutusvallan lisäämistä rajat ylittävissä tiimeissä. Tulosten perusteella ketterän riskienhallinnan käyttöönotto on siirtänyt riskien hallinnan omistajuuden kehitystiimeihin julkaisun hallintatoiminnosta. Riskienhallinnan hyödyt ohjelmistoteollisuudelle ja tapaustutkimukselle on sisällytetty motivoimaan riskienhallintaa päivittäisessä toiminnassa.

Avainsanat: Ohjelmistokehitys, riskipohjainen ajattelu, odotettu rahallinen arvo, toiminnallinen erinomaisuus, tekninen, tuote, tietoturva, yksityisyys, laaturiski

TABLE OF CONTENTS

SYMBOLS AND ABBREVIATIONS

3GPP	3rd Generation Partnership Project
ATDD	Acceptance Test Driven Development
CAPEX	Capital Expenditure
CBP	Company Business Process
CFD	Cumulative Flow Diagram
CGMS	Company Group Management System
CI	Continuous Integration
CSPD	Continuous Software Product Development
DevOps	Development Operations
DPD	Digital Pre-distortion
DSP	Digital Signal Processing
EMC	Electromagnetic Compatibility
EMV	Expected Monetary Value
F&C	Finance and Control
FTE	Full Time Equivalent
GII	Global Innovation Index
GQM	Goal Question Metric
HW	Hardware *(collection of components that constitute a computer system)*
I&V	Integration and Verification
ICT	Information and Communications Technology
IPSec	Internet Protocol Security Architecture
IPv4 / 6	Internet Protocol version 4 / Internet Protocol version 6
ISO	International Standardization Organization
ISO 9001	Quality Management System Requirements
ISO 14001	Environmental management systems requirements
ISO 19011	Guidelines for auditing management systems
ISO 25010	Systems and SW engineering - Systems and SW Quality Requirements and Evaluation (SQuaRE) - System and SW quality models
ISO 27001	Information security management systems – Requirements
ISO 31000	Risk management – Principles and guidelines

ISTQB	International Software Testing Qualifications Board
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
LAA	License Assisted Access
LTE	Long Term Evolution
NFF	No Fault Found
OS	Operating System
OSHAS	18001 Occupational Health & Safety Management Systems Requirements
PA	Power Amplifier
PDM	Product Data Management
PMI	Project Management Institute
PLCM	Product Life Cycle Management
PMBOK	Project Management Body of Knowledge
PWB	Printed Wiring Board
QMS	Quality Management System
R&D	Research and Development
RF	Radio Frequency
RQ	Research Question
SAP	Systems, Applications & Products in Data Processing
SCM	Software Configuration Management
SDE	Software Design Environment
SDK	Software Development Kit
SoC	System on Chip
SW	Software *(encoded information or computer instructions parts in system)*
TL9000	Telecommunication Quality Management System (based on ISO 9001)
URL	Universal Resource Location
WCDMA	Wideband Code Division Multiple Access
WiFi	Wireless Fidelity
WoW	Way of Working
VCS	Version Control System
XFT	Cross-Functional Team

1. INTRODUCTION

The purpose of this study is to describe a case study, where agile risk management is deployed into product development for a Development Team in Finland. The Team has gone through a major transformation from traditional waterfall project management organization into more lean and agile organization. Therefore, the related processes, tools and methods needs to be updated to support the updated way of working for the Team. The product development is done together with an ecosystem that is forming a consortium dedicated for the long term collaboration. [1]

The ISO 9001:2015 compliant risk management system is prerequisite for the deployment of ISO 9001:2015 compatible quality management system (QMS) [2]. The biggest impact from the new version of QMS standard is the adaptation of a risk-based approach [3]. Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty. The International Standardization Organization (ISO) has published two to risk management related standards. These standards are ISO 31000 risk management and ISO 9001:2015 quality management systems requirements. [4][5]

This study contributes to agile risk management practices that are integrated into commonly used Jira tool. Jira tool is de facto standard for agile software development. Jira is a proprietary issue tracking product, developed by Atlassian. It provides bug tracking, issue tracking, and project management functions. According to Atlassian, Jira is used for issue tracking and project management by over 25,000 customers in 122 countries around the globe. Only about 1,5%, or about 350, of those have tried or are actively using any separate risk management plug-in for the Jira tool. Prior research is not addressing the use of the Jira tool for the risk management, since the focus in the past research is in the spreadsheet based tools that are adapted for the risk management. [6]

The research question (RQ) is: What actions are needed to define and deploy agile risk management for the Development Team in Finland?

The research design is as follows for the research strategy phase: research outcome is applied research, research logic is inductive, research purpose is evaluation, research approach is interpretivist. The research design for the tactical phase is including mixed approach for the research process and case study for the research methodology. The research design operational phase is using experiment for the data collection method and finally the data analysis is based on the grounded theory with the Straussian approach. This study is technical report expanded towards scientific publication containing characteristics from both approaches. [7][8][9]

The main contribution of the study is the proof of concept for the holistic agile risk management. The holistic approach means that multiple different risk management processes, methods and tools can be replaced with one process, method and tool fulfilling needs of different stakeholders of the Team. The developed solution is aimed to pass the internal quality management system audit and the solution is expected to be listed among one of the identified strong practices to be discovered during the internal quality system audit. The risk management is developed in parallel with the internal quality audit, hence the findings from the internal quality audit are used in the solution. The professional risks management to be used by the agile development teams will contribute to Company's operational excellence. The fundamental changes shall be deployed into people's mindset, risk management process and tools used for the agile risk management.

The structure of the thesis is as follows; First section is the introduction of the study. Second section describes the overview of the quality management and risk management.

Third section illustrates the context of the case study and the Development Team in Finland. Fourth section contains the implementation of the risk management. Fifth section reveals the results and sixth section is the summary of the whole study.

2. QUALITY AND RISK MANAGEMENT IN AGILE PRODUCT DEVELOPMENT

The quality management system (QMS) means everything that is used to translate needs into results in a controlled, integrated and repeatable manner. QMS helps employees to do the right things and to do things right, all the time. QMS can be based on the ISO 9001 standard that companies can be certified to. A certification provides assurance of independent 3rd party compliance confirmation for the customers. [10]

Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty. The ISO has published two to risk management related standards. These standards are ISO 31000 risk management and ISO 9001:2015 quality management systems requirements. [4]

Organizations use various methods to manage the effect of uncertainty on their objectives, i.e. to manage risks, by detecting and understating risk, and modifying it where necessary. ISO 31000 provides a generic risk management approach that can be applied to all organizations to help achieve their objectives. [5]

2.1 ISO 9001:2015 standard for quality management system

The ISO 9000 family addresses various aspects of quality management and it contains some of international standardization organization's (ISO) best known standards. The standards provide guidance and tools for companies and organizations who want to ensure that their products and services consistently meet customers' requirements, and that the quality is consistently improved. [2]

The ISO 9001:2015 sets out the criteria for a quality management system and is the only standard in the family that can be certified to (although this is not a requirement). It can be used by any organization, a large or a small, regardless of its field of activity. In fact, there are over one million companies and organizations in over 170 countries certified to the ISO 9001 standard. Briefly the standard provides a basic framework for defining processes. [2]

Certification provides assurance of independent 3rd party compliance confirmation for the customers. Many customers will have the ISO 9001 certificate as a prerequisite, hence the most obvious benefits of the ISO 9001 certification are in terms of sales and marketing. Internally the biggest advantage is the continuous improvement approach. [10]

From the individual employee point of the view ISO 9001:2015 can be described in one statement: "Document what you do; do what you document, retain documented information as evidence of doing it, while adhering to the ISO 9001 elements". See the figure 1. [11]

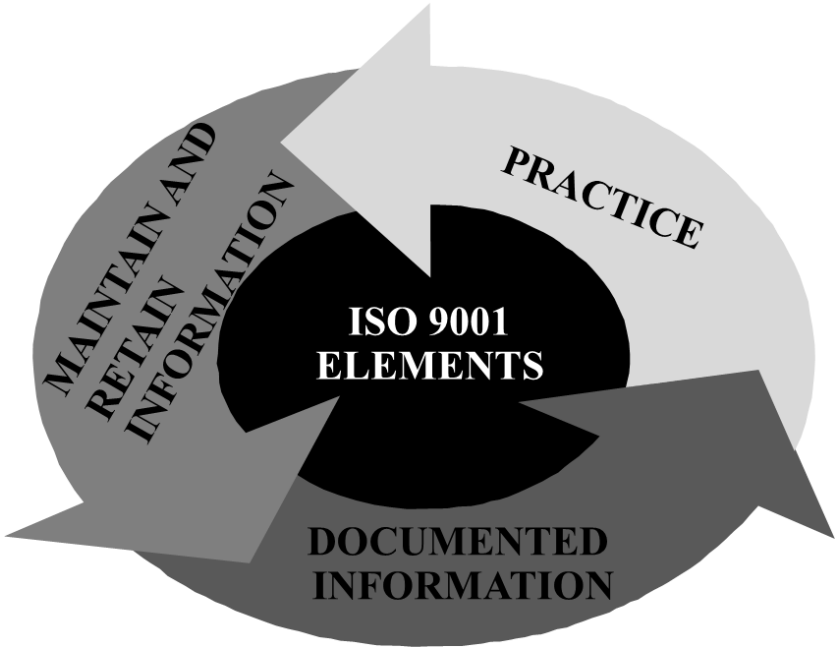

Figure 1. The ISO 9001 quality management system in nutshell.

The elements of the ISO 9001:2015 are illustrated in the figure 2. The element numbering refers to the standard's chapter numbering [4][42]. Chapter 4 contains context establishment, definition of relevant interested parties, the scope, general issues and process approach of the QMS. The standard defines QMS requirements for leadership, planning, support processes, operations, performance evaluation and continual improvement. The continuous improvement helps to evolve the leadership, planning, support processes, operations and performance evaluation.

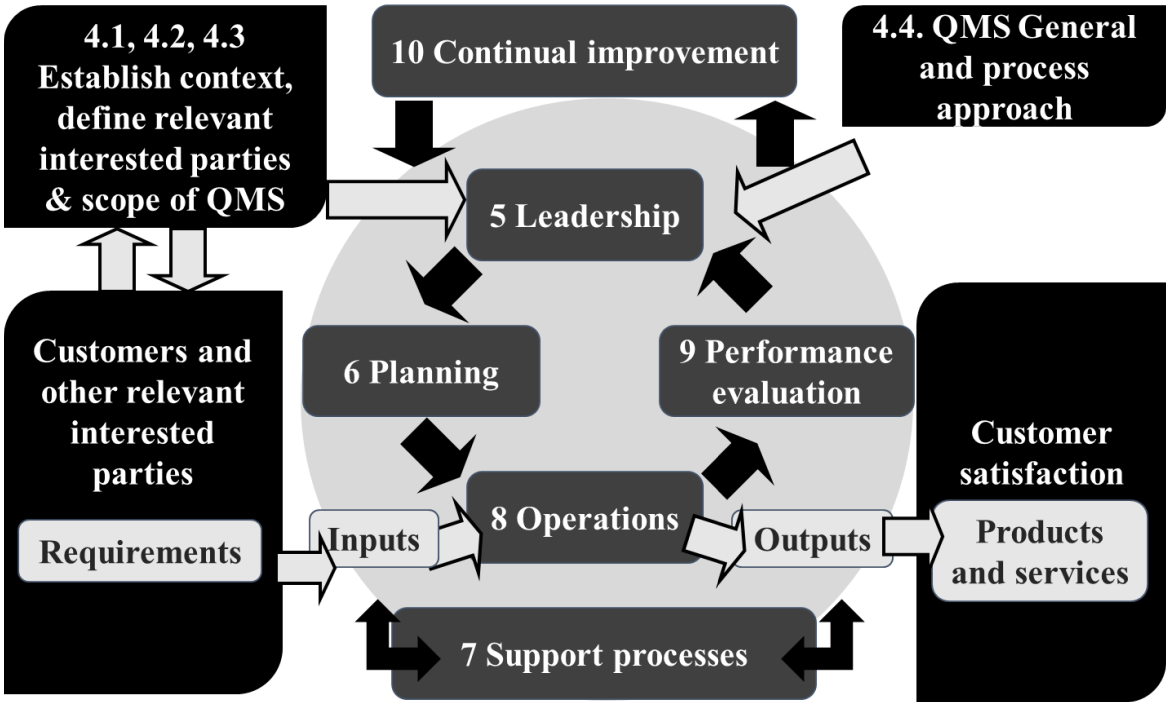

Figure 2. The elements covered by the ISO 9001:2015 standard.

The Plan-Do-Check-Act (PDCA) cycle is not one of the ISO 9001 standard requirements but it is promoted by the standard. The ISO 9001 standard process model is actually based on the PDCA cycle which can be applied to all kinds of processes. The PDCA cycle was first developed in the year 1920 by Walter Shewhart. Later it became more popular due to W. Edward Deming. [12]

The major impact from the new version of the ISO 9001 standard is the risk-based thinking, that should be considered in each organization's quality management framework. By using the proactive risk mitigation for existing and new risk the business and quality can be ensured in the long run. The introduction of the new version in September 2015 has drawn lot of attention, since organizations need to understand the fundamental changes in the approach for the quality management. In contrast to past version the new version fits more easily to services organizations in addition to product organizations. By using the new version, the different management systems can be integrated under one umbrella as one unified system. [11]

2.2 Transition from the ISO 9001:2008 to 9001:2015 revision

The new version of the ISO 9001 standard aims to help organizations to reach operational excellence by stronger customer focus and enhanced business performance. Key enablers include definition and documentation of the processes, coaching employees, nurturing the relationships in the supply chains, deploying the risk-based approach to quality and especially binding the organizations management to quality management more frequently. While in transition from earlier version to recent version, there is a need to deal with the issue by having both corrective and preventive actions. Iterative and incremental internal quality audits can be used to minimize the non-conformances and to strengthen the adherence to new version. [3] [11]

The ISO 9001:2015 is based on seven principles: Customer Focus, Leadership, Engagement of People, Process Approach, Improvement, Evidence-Based Decision-Making, and Relationship Management. Complying with the ISO 9001 quality management system requirements has been a key organizational focus since the publication of the standard. However, the approach to compliance must be proactive and result-oriented, and not limited to achieving a certification. Many organizations can simply integrate the quality management system requirements with the relevant business processes and adhere to those in the daily activities through the whole value chain. [11]

While each organization is more or less unique what comes to its structure, business processes and operations, there are certain common things that can be considered by every organization, to align processes with risk-based approach and mapping with new version of the standard. There are many tools and options to choose from when mitigating risks, documenting information, evaluating performance and maintaining the controlled quality environment, while carrying out impact assessment and engaging people. Generally, the transition is a strategic opportunity to aim for higher level in the quality management and have continuous improvements mind-set. [11]

Practical guidelines that cover all clauses of the standard provide are very useful. Prioritization of task is easy by ranking importance of each clause in the quality management standard. Examples from both ordinary organizations and top performing ones can be used for the benchmarking. [10]

2.3 Internal quality system assessment

Internal assessment is a requirement of the standards ISO 9001, ISO 14001 and OHSAS 18001. Internal assessment is also a requirement in other standards, e.g., ISO 27001, TL 9000 where applicable, to which companies may subscribe. Internal assessment confirms that companies complies with the requirements of these chosen standards. [4][13][14][15][16][17]

Auditing is a means of evaluating the effectiveness of the QMS, in order to identify risks and to determine the fulfilment of requirements. In order for audits to be effective, tangible and intangible evidence needs to be collected. Actions are taken for correction and improvement based upon analysis of the evidence gathered. The knowledge gained could lead to innovation, taking QMS performance to higher levels. [4]

ISO 9001:2015 section 9.2 Internal audit lists the requirements for internal quality audit. Auditors need to be well informed and well qualified. Audit planning is coordinated and the risk-based approach must be included. Advice and guidelines for Internal Assessment can be found in the ISO publication, ISO 19011, "Guidelines for auditing management systems". [18]

2.4 Agile project management frameworks

Often agile and lean methods are somewhat tight together, it is a context dependent matter whether those should be discussed as under a same umbrella or not. The methods are sharing a lot of their characteristics with one another, but there are differences as well while the methods are commonly seen complementing each other's. Agile software development mainly focuses into development function, and is about ability to rapidly respond to changes that occur. Agile still sees the various research and development function as separate entities while aiming to make them as agile as possible. It aims into dynamic backlog handling taking the market conditions into account. It emphasizes the shift-left thinking, aiming to avoid i.e. the heavy back-end testing. It is more about people over the processes. [19][20]

When observing lean development methods, those aim to optimize the whole process without focusing too much into single entity. The entire process flow needs to be efficient avoiding waste – all the way from early studies to customer delivery. Lean sets weight to people aspects too, it facilitates learning and organizational culture as well, it needs to remain operational in the ever-changing conditions and environment. The flow thinking is seen as the core of the lean principles, it seen a primary method as well in transiting from agile into lean and development operations (DevOps). Once seeking a common umbrella for all the agile and lean thinking, it can be combined and under the continuous software product development (CSPD). CSPD covers it all, continuous planning, development and delivery. It covers all the tangible and intangible elements of the continuous movement, it emphasizes people and teams, it pays attention into cost and benefits, it values the technical grandeur in order to achieve the ultimate business value. Appendix 1 contains various characteristics of different agile and lean methodologies. [21][22][23]

2.5 Jira tool for agile product development

Jira tool is de facto standard for the agile software development. Jira is a proprietary issue tracking product, developed by Atlassian. It provides bug tracking, issue tracking, and project management functions. According to Atlassian, Jira is used for issue tracking and project management by over 35,000 customers in 122 countries around the globe. There are few risk management plugins for Jira tool. Total download number for all four risk management plugins is about 370, hence only about 1 % of the Jira customers might use commercially available plugin. [6][24]

The data inside in the Jira tool's database can be divided into different projects. Jira project is a collection of issues and its defined according to each organizations requirements. Examples of projects are a software development project, a marketing campaign, a helpdesk system, a leave request management system or a website enhancement request system. Every item inside a project are called in issue, and there can be many different types of issues. Examples of issue types are bug (a problem which impairs or prevents the functions of the product), improvement (an enhancement to an existing feature), new feature (a new feature of the product), task (a task that needs to be done), custom issue (a custom issue type, as defined by your organization if required). [25]

There are also some other characteristics associated with issues. Priority indicates issues relative importance. Status indicates where the issue currently is in its lifecycle, also known as workflow. Resolution tells how the issue was resolved. All of these can be tailored at need for different users' needs. Figure 3 illustrates the default workflow for issues in Jira. [26][27]

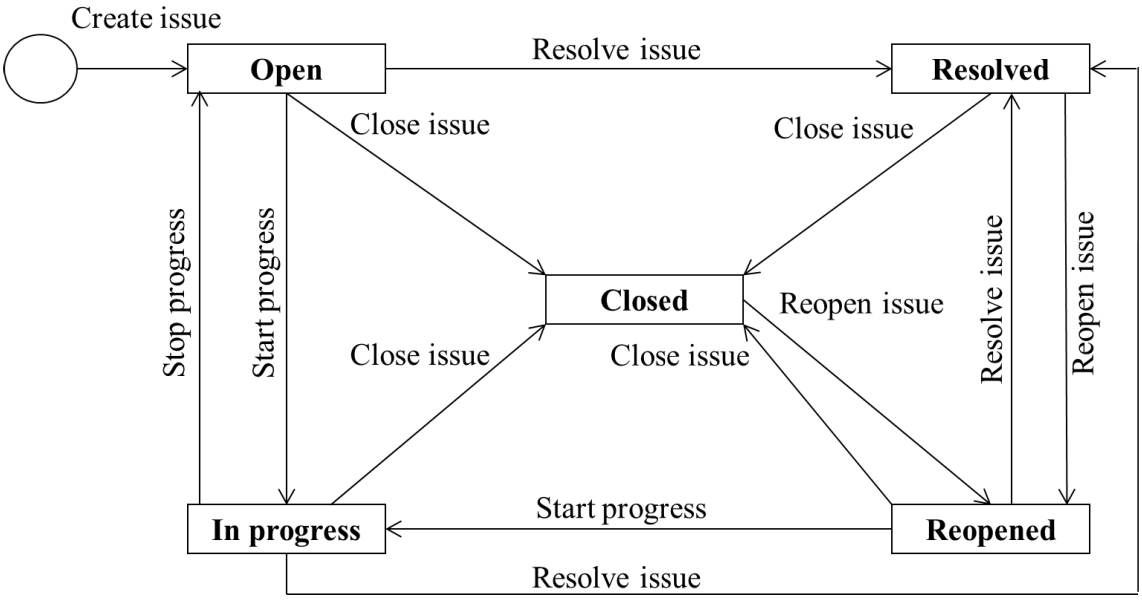

Figure 3. The default issue workflow in the Jira tool.

Different issues can be linked with each other by creating an association between the two issues. An issue may relate to another, or an issue may duplicate another or an issue may block an another issue. Link types can be tailored at need. The linked issues can be in the same Jira server in same or in different projects or fully reciprocal application links can be between different Jira servers can be made. Links can also be made to another

destination, such as Atlassian Confluence pages or to any web page internet address, officially known as universal resource location (URL). [28]

2.6 Monitoring and controlling of the knowledge work

Generally, the product development can utilize the goal, question and metric (GQM) approach to software metrics. GQM defines measurement model on three levels; Goal is the conceptual level, in which a goal is defined for an object, for a variety of reasons, with respect to various models of quality, from various points of view and relative to a particular environment. Question is the operation level, in which a set of questions is used to define models of the object of study and then focuses on that object to characterize the assessment or achievement of a specific goal. Metric is the quantitative level, in which a set of metrics, based on the models, is associated with every question in order to answer it in a measurable way.[29]

The Jira dashboards can be created to visualize the wanted information and related metrics. These metrics can provide answers to the questions that are asked to evaluate if the goals have been met. Typically, the outstanding issues can be listed and various charts can be displayed. The dashboards may contain one or more different kind of gadgets. There are tens of different available gadgets available and it is possible to program your own gadgets. [30]

Kanban is a method for managing knowledge work which balances demands for work with the available capacity for new work. Work items are visualized to give participants a view of progress and process, from task definition to customer delivery. Team members "pull" work as capacity permits, rather than work being "pushed" into the process when requested. In software development, Kanban provides a visual process-management system which aids decision-making about what, when and how much to produce. Although the method, inspired by the Toyota Production System and lean manufacturing, originated in software development and IT, it may be applied to any professional service whose work outcome is intangible rather than physical. [31][32]

Kanban boards can be used for teams that focus on managing and constraining their work-in-progress. Kanban boards have the backlog for the issues and mapping of workflow status to columns of a board. They are useful tools for the monitoring a work in a projects using the Kanban method. The process performance can be evaluated by two different methods. A cumulative flow diagram (CFD) is an area chart that shows the various statuses of work items for a particular time interval. The horizontal x-axis in a CFD indicates time, and the vertical y-axis indicates cards (issues). Each colored area of the chart equates to a workflow status (i.e. a column on a Kanban board). A CFD can be useful for identifying bottlenecks. If a chart contains an area that is widening vertically over time, the column that equates to the widening area will generally be a bottleneck. [31]

The control chart can show the cycle time (or lead time) for a product, version or sprint. Lead time is the time taken from when an issue is logged until work is completed on that issue. Cycle time is the time spent working on an issue — typically, the time taken from when work begins on an issue to when work is completed, but also includes any other time spent working on the issue. For example, if an issue is reopened, worked on, and completed again, then the time for this extra work is added to the cycle time. Control chart takes the time spent by each issue in a particular status (or statuses), and maps it over a specified period of time. The average, rolling average and standard deviation for this data is shown. Control charts can be used for analyzing team's past performance in a retrospective, measure the effect of a process change on team's productivity or provide

external stakeholders with visibility of team's performance. The past performance can be used to set targets for a team. [33][34]

2.7 Risk management

Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty [5]. Tom DeMarco has capsuled the software project risk management into following citation: *"If you've been in the software business for any time at all, you know that there are certain common problems that plague one project after another. Missed schedules and creeping requirements are not things that just happen to you once and then go away, never to appear again. Rather, they are part of the territory. We all know that. What's odd is that we don't plan our projects as if we knew it. Instead, we plan as if our past problems are locked in the past and will never rear their ugly heads again. Of course, you know that isn't a reasonable expectation."* [35]

There is no such thing as technical success, therefore the success is determined by the projects' impact to the business in companies. Based on the extensive SW project surveys in the United States, there is comprehensive understanding for the typical reason for failing SW projects. The software "failures" are defined as software projects that have any of these attributes: [36]

1. Termination of the project due to cost or schedule overruns.
2. Schedule or cost overruns in excess of 50 percent of initial estimates.
3. Applications that, upon deployment, fail to operate safely.
4. Law suits brought by clients for contractual noncompliance

Only half of the SW projects in all assessed areas are delivered on time, and 37% of the projects are late and 13% of the projects are cancelled. Schedule delays and canceled projects are distressingly common among all forms of software in the year 2016. Although there are many factors associated with schedule delays and project cancellations, the failures that end up in court always seem to have six major deficiencies:

1. Accurate estimates were either not prepared or were rejected.
2. Accurate estimates were not supported by objective benchmarks.
3. Change control was not handled effectively.
4. Quality control was inadequate.
5. Progress tracking did not reveal the true status of the project.
6. The contracts omitted key topics, such as quality and out-of-scope changes

Addressing above major deficiencies as risks and mitigating those before they turn into problems should have a major priority in the risk based approach. ISO 31000 standard provides good framework for risk management [5]. Risk management is also defined by the Project Management Institute (PMI). The commonly used risk management process is based on the PMBOK® (Project Management Body of Knowledge) Guide's 6 atomic processes [37][38].These atomic processes are as follows:

1. Process 11.1 (plan risk management)
2. Process 11.2 (identify risks)
3. Process 11.3 (perform qualitative risk analysis)
4. Process 11.4 (perform quantitative risk analysis)
5. Process 11.5 (plan risk responses)
6. Process 11.6 (control risks)

The outcome of the risk assessment is the list of risks for various areas. After qualitative risk analysis the risks have probability of occurrence and impact if the risk

will realize. Risk value is calculated by multiplying the risk probability level and risk impact level. The assessed risks can then be mitigated by planning risk responses and controlling Systematic approach to risk management process and prioritization of the risk with the highest risk values will help to reduce the probability and/or risk impact.

3. CONTEXT

The context for the study is a complex product development ecosystem containing multiple companies in global distributed product development. The Development Team in Finland is driving the product development and coordinating the various activities over the whole product development lifecycle (PDLC). First chapter in this section describes the organizational context and the sphere of the responsibilities. The risk management definition and deployment has holistic view over the all related activities. This enables overall value flow optimization and merging of various approaches into single entity. The Company quality policy is highlighted in the second chapter and it is the corner stone for all other quality activities. The quality standards requirements and requirements for the Company group management system (CGMS) are listed in the third chapter. The CGMS overview is illustrated in the fourth chapter. The fifth chapter provides practical view to the daily usage of CGMS and sixth chapter shows the mapping between the CGMS and ISO 9001:2015 quality management system requirements. The Company is globally ISO 9001 certified which requires an external audit by a certified agency to maintain the registration. [1][39]

3.1 Organizational context

The Global innovation index (GII) report reveals that Finland has been ranked to the fifth position in the innovativeness in the world in the year 2016. The ranking has been varying between 4 and 6 during the past four years. The creative output indicator category contains two interesting and convincing indicators; information and communications technologies (ICTs) & business model creation is ranked into the 1st position and ICTs & organizational model creation into the 3rd position in the whole world![40].

The background information shown in the figure 4 provides solid grounding for the organizational context in the ecosystem covered in this thesis. The Development team in Finland is about five years of old and the core team has best talents in it. The agile and lean approach with continuous improvements in the way of working and in business models has helped the ecosystem to deliver the results in a cost effective way in comparison with other existing internal organizations within the company group. The Development team in Finland has had the freedom to use own customized way of working. The management system of the mother organization has been applied only for the team's external interfaces and internal activities have been based on the local best practices. Initially the processes for the internal activities have been based on the partner companies' processes, but those have been evolved in the course of time.

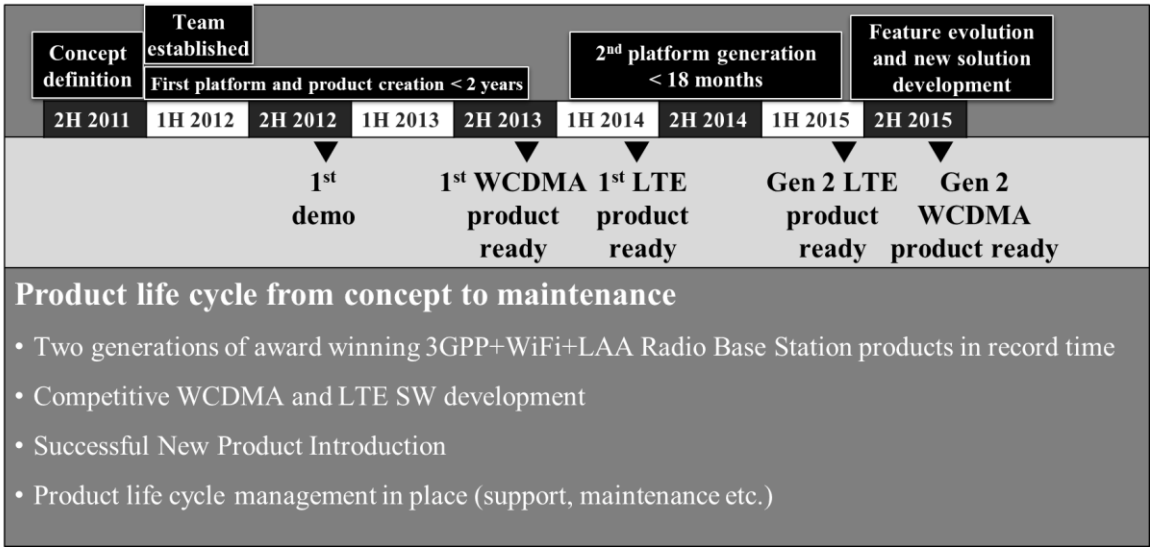

Figure 4. Overview of Development team in Finland history from 2011 to present day.

The Development team in Finland together with the ecosystem has been able to break all existing time to market records not only once but twice when new products and platforms have been created. The first platform generation was created from the scratch and the second generation platform was greatly improved version of the product. The whole development setup has been matured well enough for the internal quality audit during the course of time. The Development team in Finland has had the full end to end product creation responsibility and needed capacity due to the flexible ecosystem for delivering the needed solutions. Various responsibility areas are illustrated in the figure 5. [1]

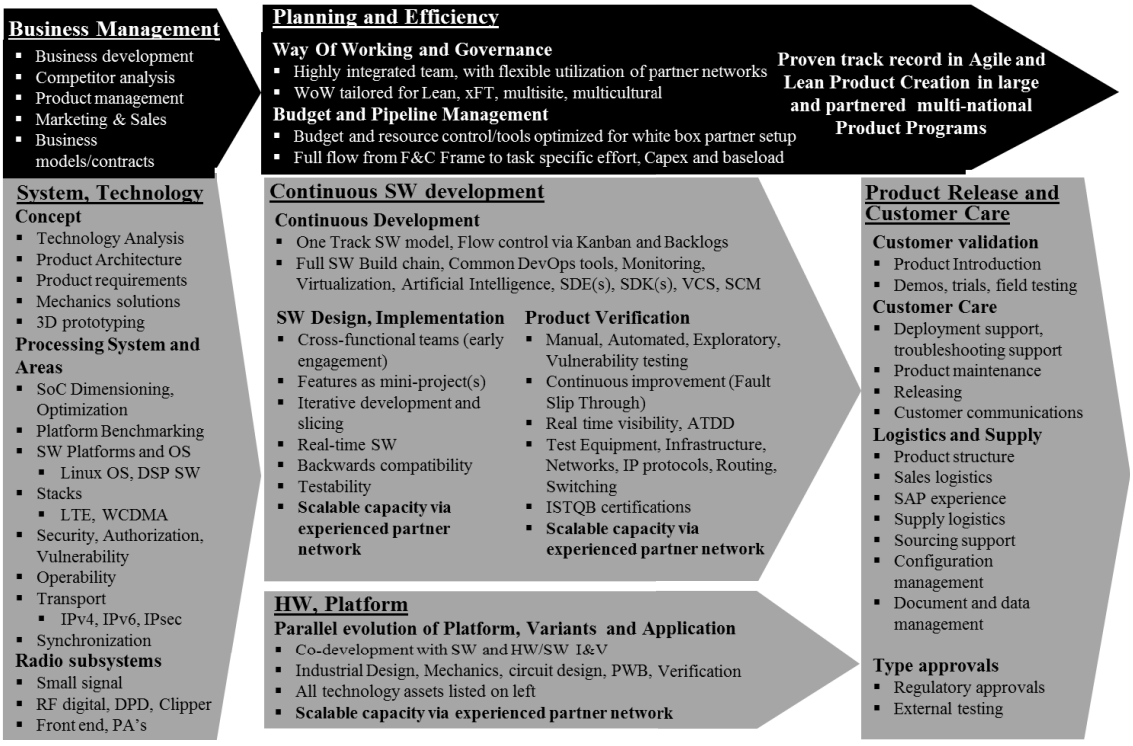

Figure 5. Everything for an end to end product creation.

The commercially available products delivered so far have already won many industrial awards and provide a competitive product portfolio. The complexity of the product and surrounding ICT environment is overwhelming. Multiple radio technologies suitable for global use squeezed into the smallest available product by its physical size with an awarded industrial design complemented by record breaking data transfer speeds, unique features, high configurability for different network environments and automatic network integrations describe the situation very well. [1]

The ecosystem utilized for the product development contains multiple companies, different business models and partnering relations, many different sites in various countries and last but not least, multiple organizational and cultures business strategies as well. This setup enables cherry-picking of the needed competencies, and scalable resourcing for the product development which on the other hand is far more difficult to manage and lead than a co-located team in one single company. Naturally the ways of working, values, skill and ambition levels, optimization of the short term versus long term are additional ingredients in the playground. This additional complexity is addressed in more details in the later chapters of this thesis.

3.2 Company quality policy

The Company stands for world class quality and operational excellence in all areas of its business according to company quality policy (CQP). One statement describes the whole system well; Putting the Customer First! Though CQP talks lot about customers, the operational excellence sets appropriate focus on all key stakeholders, and their needs. These stakeholders are seen as teams' internal customers in a large company.

The Company quality policy is the highest level quality document stating the following: "Company name stands for World Class Quality and Operational Excellence in all areas of our business as perceived by our customers and stakeholders. Our commitment to quality excellence is secured and demonstrated through a system of controls for the following: Providing products, services and solutions which satisfy customer expectations and requirements during the complete life cycle;

1. Operating effective and efficient processes aligned with our vision and strategies;
2. Releasing the full potential of our global workforce through thought leadership and inspiration;
3. Fostering a work culture dedicated to customer satisfaction;
4. Securing compliances to relevant external standards, applicable laws, listing requirements, governance codes, and corporate social responsibilities;
5. Systematically setting quality objectives, reviewing performance against targets and improving the quality of our products, services, solutions and operations.

Company Group Management System (CGMS) is the vehicle for delivering and securing our Group Quality Policy by defining, communication and applying best practice in our global operations. The effective implementation of the above policy and corresponding responsibilities is promoted by the commitment, support and active participation of our entire global workforce and management. Each employee is responsible for adherence to the parts of the Management System that are relevant for his/her responsibilities. Compliance is ensured in accordance with Group Directive, Company Group Management System (CGMS)." [41]

3.3 Quality standards and requirements for a company group management system

There are many quality standards and requirements that apply to a company group management system (CGMS). The following items are built into CGMS [42]:

1. ISO 9001 – Quality Management System [4]
2. ISO 25010 – Systems & SW Quality Requirements and Evaluation [43]
3. ISO 14001 – Sustainability and the Environment [13]
4. ISO 27001 – Information Security [14][15]
5. OSHAS 18001 – Occupational Health and Safety [16]
6. Sarbanes-Oxley Act [44]
7. Company Policies and Directives, including Company Business Processes (CBP) [45], Product Life Cycle Management (PLCM) [46], generic requirements for products (GPR) and security [47]
8. Local Laws and Regulations [48]

The Sarbanes–Oxley Act is also known as the "Public Company Accounting Reform and Investor Protection Act" or "Corporate and Auditing Accountability and Responsibility Act". It was enacted in the United States as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. [44]

3.4 Company group management system

The company has one management system for the group - the company group management system (CGMS). ISO 9001 provides requirements, that constitute the platform and enables the company to aim for one global ISO 9001 certificate. The most obvious benefits of ISO 9001 certification are related to the sales and marketing, since the company's customers have the ISO 9001 certificate as a prerequisite for the business relationship. Certification provides assurance of independent 3rd party compliance confirmation for the customers. CGMS can be illustrated as in the figure 6, where examples of the different elements are presented. The picture illustrates the role of CGMS ensuring that the company is managed to pro-actively meet expectations and demands from different stakeholders and from changes in its business environment. [39]

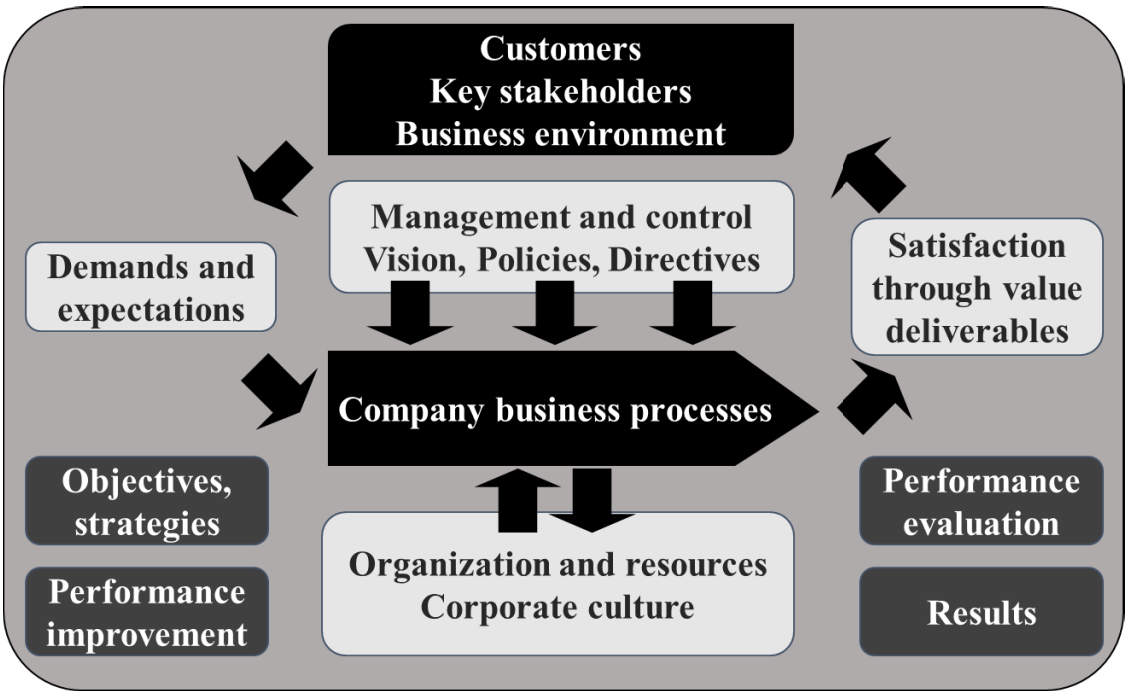

Figure 6. The elements of the company group management system.

The system is defined as a set of elements for the systematic management of all company's operations, based on the Company Business Process (CBP), structured according to Company's defined CGMS framework and accessed via the company's intranet. Overview of the Company business processes is shown in the figure 7. [45]

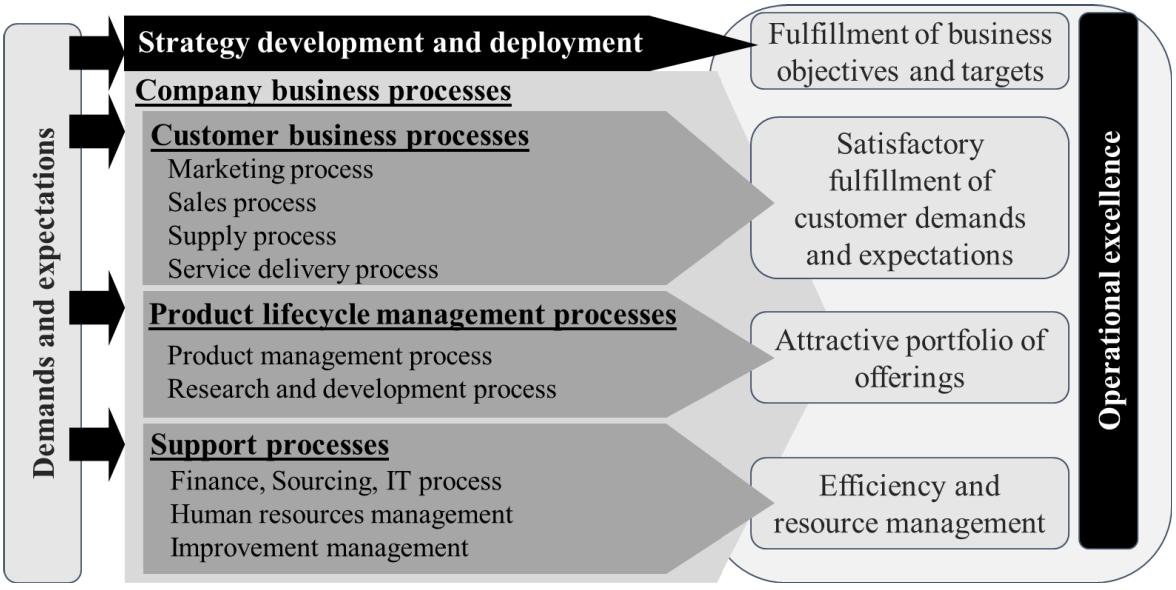

Figure 7. The company business processes overview.

CGMS shall manage the quality of the products and services by describing roles and responsibilities, organization, processes and other characteristics which are vital for the operational excellence. CGMS shall also support the fulfillment of business targets and it

should be kept updated and aligned with actual business focus as well as with organizational and managerial changes**.** An accurate and valid management system is a prerequisite for operational excellence, which results in increased customer satisfaction, reduced cost and increased competitiveness. Operational excellence requires several success factors. The strategy development and deployment yields to fulfillment of business objectives and targets and CBP execution yields to satisfactory fulfillment of customer demands and expectations. Product life cycle management (PLCM) process output is the attractive portfolio of offerings. The efficiency and resource management is achieved via the various support processes. [1][46]

The Company business process contains all process areas required for a large company. The scope in this thesis is in the product life cycle management process, more specifically in its product development process. Different organizations within the Company must comply with the Company's high level product life cycle management (PLCM) process. Detailed processes can be tailored for the different teams depending on their needs.

3.5 Daily usage of company quality management system

Previous chapters provide the introduction and visualization of the various elements of the company group management system including the quality management system viewed from a high level. The management system also includes components such as operational descriptions, organizational info, decision fora as well as process and quality guidelines. The concept has three layers as drawn in the figure 8 [42]. Most of the development work is done in projects that produce documented information from actions.

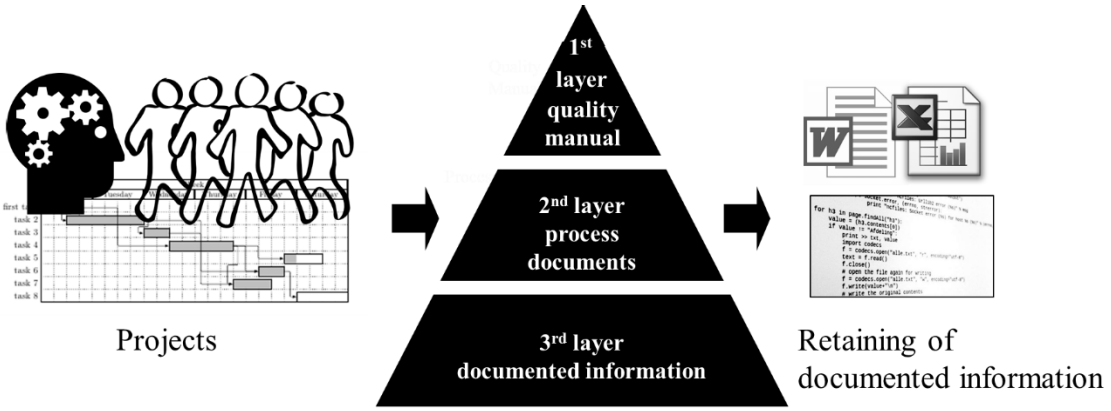

Figure 8. Daily usage of the company quality management system.

The organization needs to define which documented information must be retained for the future use.

3.5.1 *Quality manual*

The highest layer in the three-layer concept contains the operative quality manual, which defines how the company is securing its world-class quality [49]:

"Together we ensure that the policies, directives and guidelines set forth in the Company Group Management System are implemented in our operation. We rely on our organizational structure to provide:

1. effective communication
2. management commitment and follow-up
3. clear accountability and responsibility
4. support in the implementation of selected methods and good practices."

The quality manual and other supplementary documentations define who are responsible the for the quality management in the organization and the mandatory compliance with the requirements of ISO 9001 Quality Management Systems [4]. The compliance is controlled by management reviews, audits and certification [50]. Employee responsibilities are also stated, and each employee of the company shall sign the acknowledgement towards the group policy "Code of Business Ethics" [51]. All employees are to adhere to the parts of CGMS that are relevant for his/her job and role, such as process work instructions and delegation of authority within the unit. [39]

3.5.2 *Definition for a process*

The process is a collection of role-based activities to transform inputs into outputs (what should always happen, and who should do it, irrespective of how) [42]. All employees are applying various processes on a daily basis in their work, even if it may happen unconsciously, as an undocumented process is still a process. It is good to mention that processes are meant for people and not vice versa. The process discipline is a prerequisite for the continuous optimization, which happens by process updates with stakeholders, since you can only control what you can measure [52].

The product development related processes can be divided into several categories to cover the whole product life cycle management (PLCM). A process can be either a development process or a development support process, and may be either mandatory or recommended. The categories are as follows [53]:

1. Overall *(generic processes)*
2. Early phase flow *(prestudy process etc.)*
3. Development flow *(SW and/or HW development work related processes)*
4. Release flow *(processes for validation and commercial availability)*
5. New product introduction *(processes for manufacturing the product)*
6. Product line maintenance *(these processes also includes the customer care)*
7. Product development support *(for example error management process)*

There are two key performance indicators (KPI) for the development showing the business value creation. The first one is the feature lead time meaning the overall time spent between early phase flow and release flow until the feature is ready for the market. In practice this KPI measures how fast the customer requests for the new features can be fulfilled. This also reflects the time for bringing value add for the customers, and for Company's shareholders.[54]

Another KPI the is incident management response time covered by the development support process. The incidents are typically defects in the product itself, but also incidents may be related to customer product information or test environment hick-ups. It is good to note that all incidents are not defects. Defects are detected by testing activities or they can be reported from the field. The average time for defect's the entire life cycle is being measured and reported. This is related to customer satisfaction.[54]

3.5.3 *Documented information*

The documented information is new definition in the section 7.5 in the ISO 9001:2015 standard while the previous version ISO 9001:2008 had definition of a record. The previous record definition is replaced by operational planning and control for the

documented information in the section 8.1 of the ISO 9001:2015. The earlier definition of a record is shown to provide the needed background information from past practices. [4]

A record is a clearly-defined document, file, or memorandum:

- that serves as evidence of process execution,
- from which it is possible to trace the history of an event or issue,
- that is valuable to keep from a business perspective as a source of information that will be used in the future

For example, a record may document an important decision such as an agreement or an approval. Another examples of records are minutes of meeting, review & approval, test results, etc. [42]. Another definition of a record states that records are all documented information, regardless of its characteristics, media, physical form, and the manner it is recorded or stored. Records include accounts, agreements, books, drawings, letters, magnetic/optical disks, memos, micrographics, etc. Generally speaking, records function as evidence of activities, whereas documents function as evidence of intentions [55]. Note that all document and binary deliverables are also records, such as the software source code or binary, the hardware schematics, generated test data and the test logs etc.

3.5.4 *Importance of maintaining and retaining documented information*

The primary purpose of retaining documented information is as a source of useful information. Keeping the right documented information contributes to organizational learning; for example, repeating a success or learning from a mistake. Retained documented information also serves to demonstrate process compliance during the audits – compliance protects the Company's brand! [42]

There are many repositories and archives for the documented. The Development team in Finland is using the separate repositories for managing the document's working copies. This approach enables the smooth collaboration in the multi-company setup. The information confidentiality, integrity and availability can be ensured in a satisfactory way. The documented information archival is done in the official document management system separate from the collaboration workspace. The product data management (PDM) systems are used for managing the product structure related documented information.

3.6 Company group management system mapping with the ISO 9001:2015

A definition exists how the clauses in the ISO 9001 shall be interpreted in the context of the company group management system. Number of the company's related high level practices with the standard are presented in the table 1. Each clause has been analyzed and meaning of it to the company explained in the actual map. A related practice can be policy, directive, instruction, guideline, framework, manual, process, template, etc.[56][56]

Table 1. The number of related practices for each clause in the standard

Element	Clause in the standard	Practices
4	**Context of the organization**	**Total 21**
4.1	Understanding the organization and its context	7
4.2	Understanding the needs and expectations of interested parties	9
4.3	Determining the scope of the quality management system	2
4.4	Quality management system and its processes	3
5	**Leadership**	**Total 13**

Element	Clause in the standard	Practices
5.1	Leadership and commitment	8
5.2	Policy	2
5.3	Organizational roles, responsibilities and authorities	3
6	**Planning**	**Total 13**
6.1	Actions to address risks and opportunities	7
6.2	Quality objectives and planning to achieve them	4
6.3	Planning of changes	2
7	**Support**	**Total 30**
7.1	Resources	9
7.2	Competence	4
7.3	Awareness	1
7.4	Communication	6
7.5	Documented information	10
8	**Operation**	**Total 24**
8.1	Operational planning and control	3
8.2	Requirements for products and services	3
8.3	Design and development of products and services	4
8.4	Control of externally provided processes, products and services	5
8.5	Production and service provision	3
8.6	Release of products and services	3
8.7	Control of nonconforming outputs	3
9	**Performance evaluation**	**Total 8**
9.1	Monitoring, measurement, analysis and evaluation	3
9.2	Internal audit	4
9.3	Management review	1
10	**Improvement**	**Total 13**
10.1	General	2
10.2	Nonconformity and corrective action	7
10.3	Continual improvement	4
	Grand total of the related practices	**122**

The amount of the related material is quite high, and mastering the whole scope requires dedicated subject matter experts. The high level practices are often described in more details in lower level documents. The applicable process maps show actual processes for each area. The processes are complemented with guidelines and working instructions.

3.7 Rationale for risk management improvement

Risk management is conducted by using the existing processes, tools and methods from the partner companies. Actually there is no separate risk management process description available, but only the spreadsheet based tool that has the risk management fields.

The deployment of the quality management system, which is based on the ISO 9001:2015, requires risk based approach to be taken into use. The internal quality audit survey contains also the questions for risk management. The gathered data can be used to determine the current state of practice in the risk management. The wanted position in the risk management is to fulfill the ISO 9001:2015 requirements and to support the agile cross-functional development teams in their daily work. Once the gap between the current

state of practice and wanted position is identified, action planning can be done to take needed improvement steps towards the wanted position.

There are six questions in the quality audit survey related to the risks. These are divided into three categories as follows:[57]

1. Current state of practice of risk based thinking
   a. WA4QA010 - Do you monitor risks and opportunities towards strengthening customer/stakeholder perception of quality?
   b. WA4QA011 - Do you demonstrate personal engagement by promoting the process approach and risk-based thinking?
2. Current state of practice of risk management
   a. WA4QA017 - Is risk management conducted on the activities to ensure actions are applied to effectively prevent defects or other adverse impacts to quality/plans?
   b. WA4QB053-Are risks managed (i.e. are they identified, reviewed and appropriate mitigation plans documented)?
3. Currents state of practice of product security risk management
   a. (WA4QA019): "Are there established and maintained methods for the identification and analysis of security risks and vulnerabilities for the product?"
   b. (WA4QA020): "Are actions taken to prevent or mitigate the security risks or vulnerabilities in the product design and operational controls?"

It is worth of mentioning that depending on the role of the auditee, they answer different set of questions in the internal quality audit survey. The analysis of the answers is based on the mixed mode research process, where both quantitative and qualitative answers are analyzed.

3.7.1 *Mixed mode analysis of current state of practice of risk based thinking*

Two questions are related to evaluating the current state of practice of risk based thinking. First question is WA4QA010 - Do you monitor risks and opportunities towards strengthening customer/stakeholder perception of quality? There are three different answering options that are yes, somewhat and no. [57]

Auditees answered "yes" commented: [57]

- Balancing the quality versus schedule is typical situation in WCDMA release projects. What fault fixes will be prioritized; do we take risk on implementing some correction earlier to keep customer satisfied but having risk of regression in some other functionality. Release planning is also good example where the risk and opportunities are being checked and monitored, new features vs. quality improvement.
- In the maintenance projects.
- Risk analysis done and updated during HW project.

Auditees answered "somewhat" commented: [57]

- Just recently we have got few major customer exercises, which educating us a lot how customers are perceiving our quality
- Recommended risk management procedure exist, but some variation by different project managers
- Risk are monitored in WCDMA SW release work
- Risks are identified and valuated in the beginning of project and followed up during the project.
- Trying as much as possible in the HW project.

Auditees answered "no" commented: [57]

- Mostly project related risk are addressed in high level, not on feature development level. Quality risks are not systematically used, depends on the sub-project

The second question is WA4QA011 - Do you demonstrate personal engagement by promoting the process approach and risk-based thinking? There are three different answering options that are yes, somewhat and no. [57]

Auditees answered “yes” commented: [57]

- Arranging trainings, coaching, planning, requiring associated that milestone acceptance criteria are handled in professional manner. But in the past the leaders haven't been so keen on this topic.
- If process is defined, we need to obey those. Several times when we haven't gone by the process, we have gone wrong
- In WCDMA release project we work according to agreed processes and principles. Risk management is essential part of project working practices.
- Process training, new processes.
- Work are done according agreed work in processes and risk are constantly identified in WCDMA projects

Auditees answered “somewhat” commented: [57]

- By project planning and risk analysis. HW team weekly meetings.
- Depends partly on project managers
- Processes will be followed as much as possible in HW development.

Auditees answered “not applicable” commented: [57]

- What does the "personal engagement by promoting the process approach" mean? Risks are discussed within the team and followed up during the project.

The distribution of different answering options is presented in the figure 9. The results of the first question show that 67% of the auditees think that risk are somewhat monitored, 8 % say no and 25% choose yes. [57]

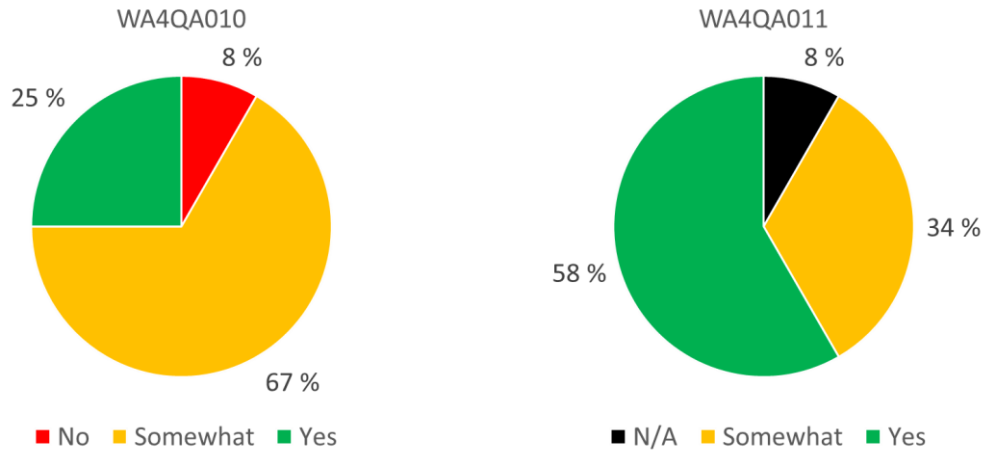

Figure 9. Risk based thinking existence and personal commitment responses.

The results of the second questions answers tell that 34% of the responders show personal engagement by promoting the process approach and risk-based thinking. Somewhat answer is 56% of total. Not applicable answer is 8%. [57]

3.7.2 *Mixed mode analysis of current state of practice of risk management*

Two questions are related to evaluating the current state of practice of risk management. First question is WA4QA017 - Is risk management conducted on the activities to ensure

actions are applied to effectively prevent defects or other adverse impacts to quality/plans? There are three different answering options that are always, mostly and rarely. [57]

Auditees answered “always” commented: [57]

- Project plans have the risk assessment done and mitigation plans.
- Release project has separate risk database which is being updated and checked as daily/weekly routine.
- I have been participating the product risk assessment and analysis work organized by the subject matter experts
- Risk management Excel in new release project is regularly updated and follow up is make in weekly leadership team meeting

Auditees answered “mostly” commented: [57]

- By risk analysis in HW projects
- Depending of the project variation used. Software feature risks management is part of weekly follow-up process
- In the product maintenance work releases are done with small steps, and ensuring by verification that later releases are better that previous ones
- New SW feature test analysis documents have risk management section.
- Project is using risk management Excel and risk meetings. This is mostly for HW platform project
- Risk management can be found in SW feature level, Release level and product level. The milestones include check-items for risks.
- Risks are listed to the Excel when those are noticed. It is followed up that risks have been handled in a proper way and taken into account.
- We have done risk scenarios and recovery planning document about continuous (CI) environment and network risks
- With risk planning and follow up during customer validation

Auditees answered “rarely” commented: [57]

- For some activities yes, but not for all. Some improvement needed here for the test environment management point of view.
- I am not sure how risk management can help current work. We need to improve it in future.
- Risk management is not considered enough, but we are about to take risk management better into use i.e. in our software feature development
- Some project risks are handled by project managers but not so well organized way. We need to improve our risk management.

The second question is WA4QB053-Are risks managed (i.e. are they identified, reviewed and appropriate mitigation plans documented)? There are five different answering options that are always, mostly, rarely, don’t know and not applicable. [57]

Auditees answered “always” commented: [57]

- See the spreadsheet risk database
- Risk are managed in the project risk management meetings according to risk spreadsheet
- Risk list existing.
- HW risks are tracked and mitigations planned in weekly meeting at all levels of the project organization. Meeting minutes contain evidence. There was also Excel summary of risks. Risk probability, severity and impact were used for arranging risks in priority order. Most important ones handled first.
- Yes, we have a risk list for project.
- WCDMA Risk database updated and followed-up on daily/weekly basis

Auditees answered “mostly” commented: [57]

- See HW project risk excel database

- At least risk management is used weekly in WCDMA/MSMM release work.
- In platform project and frequency variant. Special project Excel.
- Release project risk management is in place on project level. Also SW feature development teams are managing SW feature related risks and escalates them to the project level if necessary.
- Project level risk management in place. Now also in SW feature planning / tracking tool taken in the use.
- Risks are identified and listed, mitigation activities planned if applicable.
- What comes to the testing, our approach is risk based.

Auditees answered “rarely” commented: [57]

- Risk management is currently not good. Even in the best case, risks are identified but not managed in a proper way.
- Some project risks are handled by project managers but not so well organized way. We need to improve our risk management.

Auditees answered “don’t know” commented: [57]

- I have not been introduced risk management process
- I use requirements from Jira
- In project monthly meeting and weekly error status report mails and immediate 'big' risk information is given to developer but about review and documentation is not informed.

Auditees answered “not applicable” commented: [57]

- Haven't been working with risk analysis in this project.

The distribution of different answering options is illustrated in the figure 10. The results of the first question tell that 26% of the auditees consider risk management is always conducted, 53% say it is done mostly and 21% are stating it is done rarely. [57]

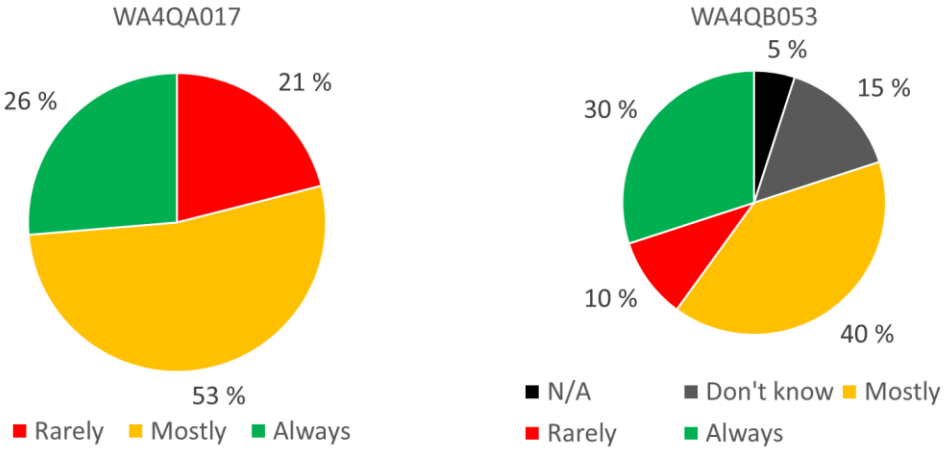

Figure 10. Risk management responses.

The results of the second questions answers reveal that 30% of the auditees think risks are managed. Mostly answer has 40% share while rarely option got 10% share. 15% of the people don’t know and 5% says that risk management is not applicable. [57]

3.7.3 *Mixed mode analysis of current practice of security risk management*

Two questions are related to evaluating the current state of practice of product security risk management. The first question is (WA4QA019) “Are there established and maintained methods for the identification and analysis of security risks and vulnerabilities

for the product?" The second question is (WA4QA020) "Are actions taken to prevent or mitigate the security risks or vulnerabilities in the product design and operational controls?" There are four different answering options for both of the question that are yes, somewhat, don't know and not applicable. Figure 11 depicts the distribution of the answers. Answer distribution for the first question is as follows: 17% of the people consider product security risks and vulnerabilities are managed and 63% say those are somewhat managed. Don't know answer got 14% share and not applicable is 6%. The second question got following distribution of the answering options: Risk mitigation actions for product security and vulnerabilities are seen by 14% of the responders, 69% of the responders consider actions are done somewhat, 11% share for the don't know and 6% for the not applicable answer option. [57]

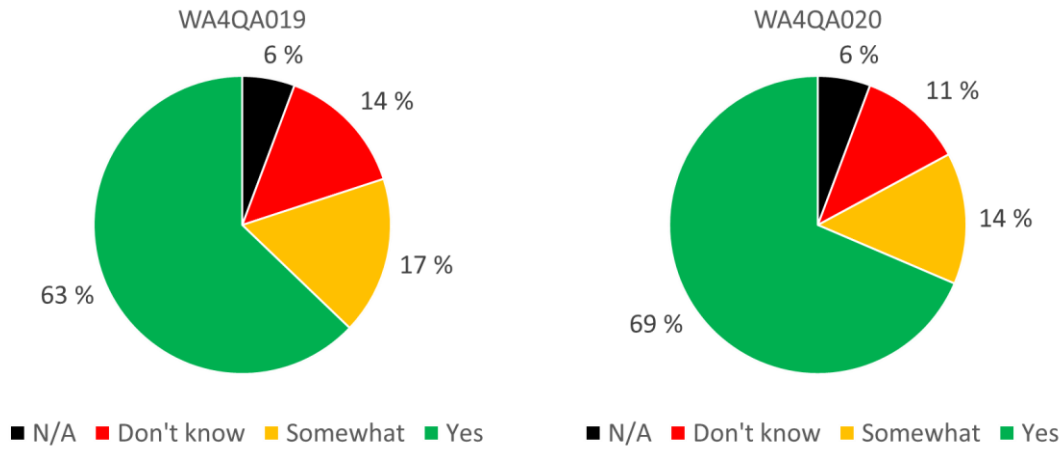

Figure 11. Product security and vulnerability management responses.

The qualitative data about the details of the comments have been ruled out from this study. The details of the product security and vulnerability management are sensitive material that cannot be disclosed in this study.

3.7.4 *Management's intent*

Another view point for the risk management improvement is the management's intention. Past realized risks that were not even identified or managed has led to following guideline written prior the internal quality audit. Risk management principles include the goals, practices and lean approach. Management's intent contains following statements:[58]

- "Goals:
  - Raise up and ensure actions for items that can likely violate targets
  - Put adequate pressure on those actions on correct level
  - Enable understanding of overall research & development (R&D) and project situation
- Practices:
  - Top five risks on release project identified and actions actively managed
  - Top five product and quality risks brought in product leadership team to be managed
  - Top risks on new scenarios are reviewed and are one basis of decision
  - Risks are understood and managed in sub-projects and escalated as needed
  - Minimum risk data: risk definition, likelihood, impact, owner, actions and status
- Lean and minimal waste:
  - Use common sense, "Delay of SW design" as a risk does not add value
  - Do not get blinded by extreme process or tools - action is only real value"

Above principles needs to be taken into account when planning and implementing the risk management improvement. Management ‘s intent also contains a statement that once the feature development schedule commitment milestone has been achieved, the feature completion date estimation and actual date must not deviate from the commitment unless there is an identified and managed risk that has been realized. The tolerance for deviations is +/- two weeks and the typical feature development time is between three to six months. [59]

4. IMPLEMENTATION

The risk based approach starts by defining the risk management process that can cover the entire product development lifecycle and the product maintenance. The process must also cover both usual kinds of project and product risks and the product security and privacy risks. In the past these have been addressed separately in different forum, so there has not been holistic view on risk management. Risks can be identified in any phase of the feature development. A risk can be related to a feature development and/or product release. The earlier the risks are being managed, the better change there is to succeed avoiding and/or mitigating the risks. Typically project related risks are avoided or mitigated by project management activities. The technical risks, known also as product or quality risks, are typically mitigated by testing activities. The product security or privacy related risks are also managed with same renewed process and tools. For these risks the information shared in the risk item can be considered case by case according to the confidentiality level of the risk.

4.1 Updating the risk management process

The earlier risk management process used by the Development team in Finland is a legacy process inherited from the partner company in the ecosystem. The new process is based on the same atomic processes, so the major difference is in the iterativeness of the process. Continuous risk management is highlighted for the agile development instead of do it once in the sequential type of project models [60].

Figure 12 illustrates how the atomic six processes are embedded into the process. First step in the continuous risk management is the risk management planning covering the entire feature lifecycle. The risk identification yields to preliminary risk lists. The identified risks are assessed by using qualitative risk analysis that is at need complemented by quantitative risk analysis. Contingency planning is done for the assessed risks and continuous risk monitoring and controlling is performed for the risks and actions. Some details of the atomic processes are tailored but otherwise the process is compliant with the Company's common risk management process. It is good to mention that the same approach is used for both for the all kind of risks such as project, technical and product security and privacy risks [61].

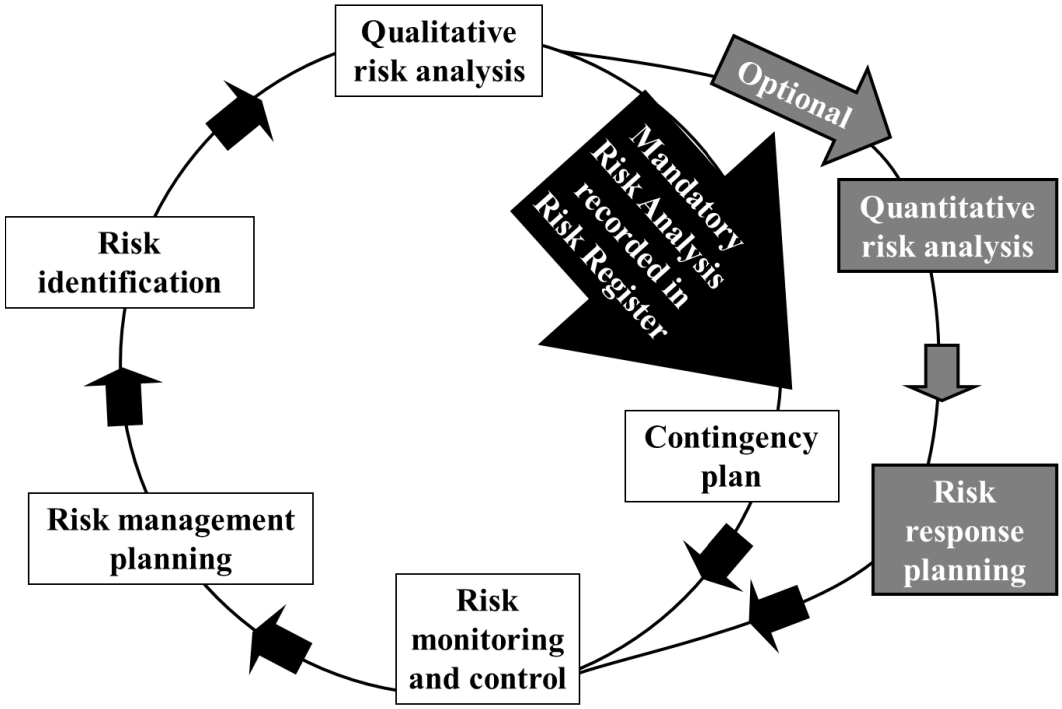

Figure 12. Overview of common risk management process elements.

The agility of the risks management is enable by starting the risk management in the early phase and involving the correct stakeholders. Continuous execution allows that associated activities are conducted in iterative and incremental way. Any changes in surrounding world can be easily taken into account and the focus can be kept on the risks with the highest risk level.

4.1.1 *Risk identification*

Risk management planning begins with definition of different kind of risk categories to be able to cover the entire planned scope. The past approach had only three options for the risk categories; Project risk, technical risk or both. The new approach has more categories that will help the users of the risk management process to think out of the box when they perform risk identification in the risk workshops.

Project risks category contains items: team, steering group, project goals/objectives, tollgates and milestones, time constraints, time plan, configuration management, change management, quality assurance, economy/budget, communication/information and logistics. Organization risk category contains items: assignments, resources, competencies, experience, collaboration other organization, consultants, process, methods & tools, information technology (IT) system, receiving organization, maintenance. Technical (or solution) risk category contains items: requirements, deliverables, partner agreement, 3rd party product availability, compliances, intellectual property rights (IPR), environment including electromagnetic compatibility (EMC), production (yield, costs), integration, installation, HW quality (claims, no fault found (NFF)) and SW quality (incident reports). External risk category contains items: contractual, customer validation, customer expectations and culture. There is also own category for product security and privacy risks. If any of the pre-defined categories are not suitable, then category other can be used. [60]

4.1.2 *Qualitative risk analysis*

The qualitative risk analysis has two main aspects. First is the probability for the risk occurrence. The probability can be expressed as quantified percentage number between zero and 100 percent, but that approach is mostly used by insurance business, where the past incident history can be used to determine the likelihoods of risks. Other approach is to use qualitative predetermined steps about relative likelihood. The number of predetermined steps typically is either three, four or five. The earlier spreadsheet approach uses three level options for the probability (high, medium, low), but this is seen as too coarse approach.

The product security risk guidelines use four level options and this forces to think the actual selection among the even options instead of choosing the middle one from the odd options. The company risk management guidelines define five level approach and that is selected to achieve the compatibility with the guidelines. The same number of levels are also selected for the risk consequences, although it would also be possible to choose different number of levels for the probabilities and consequences. For example, 3x3, 3x4, 3x5, 4x3, 4x4, 4x5, 5x3 and 5x4 are also possible matrix sizes. Suitable description for the levels are also provided to help the users selected correct level among the options.

Estimate the probability of its occurrence

1. Very low probability e.g. “You would be surprised if this happened”
2. Low probability e.g. “Less likely to happen than not”
3. Medium probability e.g.” Just as likely to happen as not”
4. High probability e.g. “More likely to happen than not “
5. Very high probability e.g. “You would be surprised if this did not happen”

Estimate the consequence of its impact on the project

1. Very low consequence e.g. “Less than one-week delay on critical time line”
2. Low consequence e.g. “Two weeks’ delay on critical time line”
3. Medium consequence e.g. “One month’s delay on critical time line”
4. High consequence e.g. “Two months’ delay on critical time line”
5. Critical e.g. “More than four months’ delay on critical time line”

These two parameters can also be visualized in the form of matrix as drawn in the figure 13. The risk value is the product of the risk probability level and consequences of impact level. The risk level in 5x5 matrix varies between one and 25. The risk levels are divided into three categories. Risk level high category contains values 15, 16, 20 and 25. The moderate risk category contains risk levels 10 and 12. Lower risk values belong into low category.

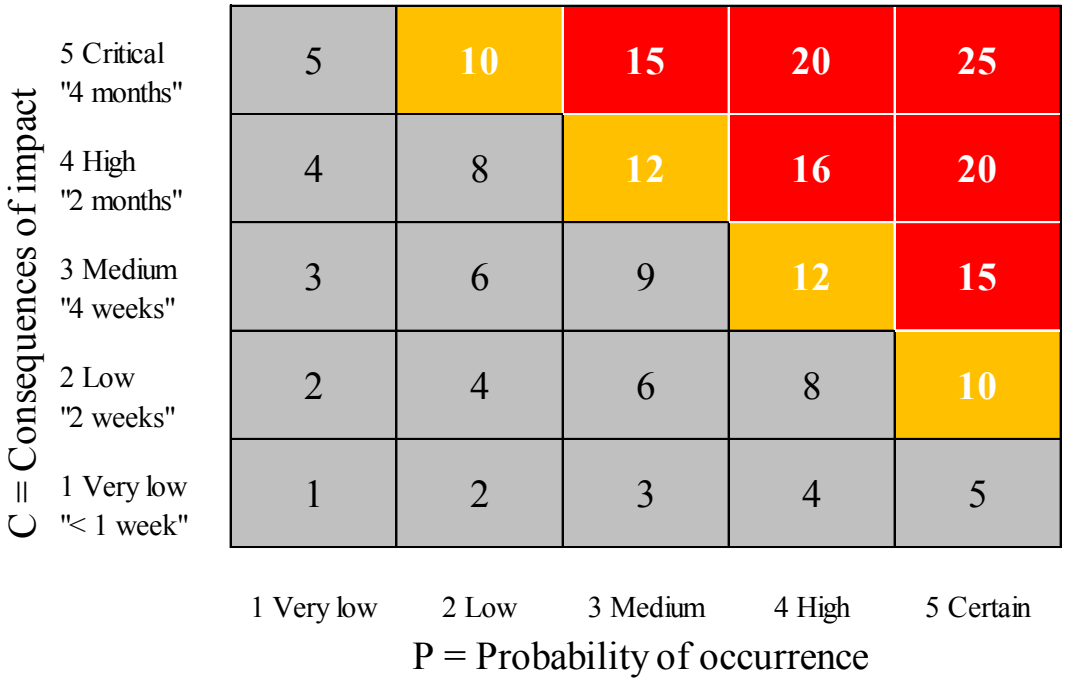

Figure 13. Risk assessment matrix of size 5x5.

Product security or privacy related risks in earlier process uses 4x4 matrix that is mapped to the 5x5 matrix for the unified approach. In practice the product security risk lowest probability and consequence levels begin from 2 in the 5x5 matrix. The schedule impact point of view is just one alternative for the consequences of the risk. Depending on the project the focus could be either in the project costs or product realization or in the customer perception. The priority and business model for the product development defines which viewpoints are emphasized. See table 2.

Table 2. Description of risk consequence levels

Conse-quence	Critical timeline for certain phase	Project cost in certain phase	Product realization	Customer perception examples
5 Critical	More than four months	Very high costs (> 40%)	Product cannot be delivered to customer	Network failure, several products lose all traffic handling or critical incident and escalation from customer
4 High	Two months	High extra costs (20-40%)	Features not according to assignment	Complete product entity failure, the system loses all traffic handling or top priority incident reported by customer
3 Medium	One month	Quite high extra costs (10-20%)	Exemption request	Partly product entity failure, e.g. sector loses all traffic functions completely or medium priority incident report
2 Low	2 weeks	Little extra costs (< 10%)	Major change request	Capacity reduction where sector is affected by traffic

Conse-quence	Critical timeline for certain phase	Project cost in certain phase	Product realization	Customer perception examples
				function loss or minor remarks from customer
1 Very low	Less than week	Negligible extra cost	Minor change request	Negligible product operational notice or negligible customer notice

The consequences in the table are exemplar, and they can and should be adapted for each team based on the applicable parameters.

4.1.3 *Quantitative risk analysis*

The quantitative risk analysis can be applied when there is a need to define the expected monetary value (EVM) of the risk. The EMV is calculated by multiplying the value of each possible outcome by its probability of occurrence and adding them together The EMV calculation formula (4-1) is as follows: [63]

EMV = (estimated cost if risk happens without any actions * probability) + (estimated cost if risk happens after actions * (100% - probability)) (4-1)

Estimated costs if risk happens without actions is the cost of the impact, and this is the maximum cost when the risk realizes. Estimated cost if risk happens after actions is the residual maximum cost for the realized risk after all actions are done to reduce the risk. The estimated costs for actions to reduce the risk are preventive cost. Project specific default values can be defined for the different parameters of quantitative risk analysis. The risks belonging to highest risk level category can have risks' detailed costs calculated in a separate risk response document. [60][63]

4.1.4 *Contingency planning*

Risk response planning contains action planning for risk level reduction. The risk contingency planning needs to be always started for the risks in the high risk level category. The medium category can be covered after the top risks have been addressed. The contingency planning is very important for the proper risk management, since the actions are only real value. Just identification or risk assessment phases do not add value.

There can be many approaches for the risks that will reduce the risk level of the selected risks. Approaches are avoiding the risk, mitigation of the risk, transferring the risk to another organization or accepting the risk. The definition of the risk approaches in the risk management guidelines is a bit vague, hence simplification for the ordinary developer is preferred to ensure proper deployment of the renewed risk management process. Risk avoidance is used changing the project assignments, the project steering documents, or resources to eliminate its occurrence or its impact on the project goals. Although the project team can never eliminate all risk events, some specific risks may be avoided. Risk mitigation seeks to reduce the probability of its occurrence and/or consequence of its impact of an adverse risk event to acceptable threshold. Taking early action to reduce the probability of a risk's occurring or its impact on the is more effective

than trying to repair the consequences after it has occurred. Mitigation costs should be appropriate, given the likely probability of the risk and its consequences. [60]

Risk can be transferred to other organization in cases where the risk ownership and action driving is done elsewhere than in the organization identifying and assessing the risk. Examples of such risk in the context of the Development Team in Finland are other network nodes, customer unit activities or network management solutions or 3rd party solutions. Risk can be accepted if a project team has decided not to change the projects steering documents to deal with a risk or is unable to identify any other suitable response strategy. Risk acceptance strategy is however recommended only for the low level risks.

4.1.5 *Risk monitoring and controlling*

Risk monitoring is risk management task that deals with the activities related to periodically checking the status of the risks in the project. Reports are prepared that compare the actuals to that which was planned. Risk control is a risk management task that deals with developing and applying set of corrective actions to get a project on track when monitoring shows a deviation from what was planned.

GQM method can be used to set the both goals for the project and various items and processes used in the projects. Monitoring can be done by using Jira dashboard with suitable gadgets displaying wanted metrics. Following items form a good starting point for monitoring the risks with the Jira tool:

- Gadget 1: open risks for the new release project sorted by risk value in descending order
  - Key items related to risk to display include issue id, summary, status, quantitative probability level, quantitative consequence level, value, level, flow phase, feature id, release, risk category, approach, labels, revisit date, assignee, last update
- Gadget 2: Actions related to risks shown in the gadget 1
  - Key items related to action are issue id, summary, priority, status, due date, assignee
- Gadget 3: closed risk displaying achievements and added value of the risk management
  - Same items included than in the gadget 1
- Gadget 4: product security and privacy risks separated from normal risks in gadget 1
  - Same items included than in the gadget 1
- Gadget 5: open security or privacy vulnerability incident reports for all projects
  - Key related items to show are project, issue id, summary, priority, severity, status, feature id, impacted components, responsible team, assignee
- Gadget 6: open risks for maintenance projects sorted by risk value in descending order
  - Same items included than in the gadget 1

Jira Kanban boards can also show the risks and related actions. These can be added to any team's existing Kanban boards and new dedicated risk management Kanban boards can be created. Default reporting tools for a Kanban board includes both cumulative flow diagram and control charts. Each involved issue, be it risk or action, can have one or more optional labels, that help sorting and filtering of the issues.

4.1.6 *Risk management planning*

Risk management planning covers all phases of the risk management process. The planning, estimating, monitoring and control of risk management activities shall be taken into account like any other key process in the project.

Risk management planning contains both non-recurring actions and recurring actions for each project and milestone. Non-recurring actions are related to process establishment, tool definition and deployment, milestone checklist updates and guidelines sharing via internal Wiki-pages. Recurring actions for each feature and release project contains risk

workshop in the early phase of the project and continuous risk management process execution. The development milestones have certain acceptance criteria for the risk management discipline. When managing the project risks, confidence interval is the period of time within which a contingency action must be implemented in order to be effective in reducing the impact of the risk. The due date means the revisit date when specific risk needs to be paid attention to.

Generally, the risk management should be part of the daily activities and the information should be transparent and visible for all. Therefore, using the existing projects in Jira for the risk management information is default choice, unless there is a need to limit the visibility of future work planning, such as technology analysis. In the latter case the risks can be added to own project containing the other confidential data. At need the high level risk may be taken into more consideration and separate risk response document can be created to deal with the risk. This allows to include as much information as possible for the risk and these separate documents can be added as attachments to the risk issues in the Jira. For example, the risk EVM can be addressed in the attachments.

4.2 Customized issue type for risk management in Jira

The risk management tool must provide seamless user experience for the users. That will help employee's adherence to the process work instructions relevant for his/her role. Major part of the Team's development activities is already managed with the Jira tool equipped with suitable agile add-ons, so integrating the risk management into the same tool is the best approach. The benefits of using Jira for risk management also include the task management for the risk mitigation activities and linking of the tasks and risks with other issues. These tasks can be easily displayed in the team specific task backlogs. People do not need to learn new tools and they can focus on applying the process while also getting rid of the old tools and methods. [62]

Implementation of the risk management in Jira requires several activities. First the reasoning for the tool selection and that argumentation can be used when motivating the people to change their way of working. Workflow must be planned for the risk management in the tool. The new issue type must be created and tailored for the risk management.

4.2.1 *Risk management tool change reasoning*

The tool for implementing the risk management process is selected. Instead of earlier spreadsheet based tool (Excel file in the SharePoint teamsite), the Jira tool is preferred. The key facts for using the Jira tool also for the risk management are as follows:

- From the user perspective
  - Same user experience (the look and feel) than for most of the processes used in daily development by most of the people in the organization
  - Information is always up to date and available in known location
  - Easy linking of the issues with feature requirements and tasks (actions)
  - Issues can be shown in the team backlog (centralized backlog for actions)
  - No need to wait until the file is available, parallel use of the database
  - Commenting the issues within the tool instead of email communication
  - Adding / removing stakeholders as watchers for the changes in the issues
  - Free and dynamic use of the labels to tag the issues (e.g. top risk, or customer XYZ specific risk etc.)
- From the process optimization perspective

  - Various dashboards can be used to monitor and control the progress
  - Items in project milestone checklists in Jira can have links to the risks
  - Kanban boards and related tools can be used for optimization
    - Cumulative flow diagrams
    - Control charts
  - KPI generation from the process performance
  - Reduction of both email communication and separate file management
  - Similar tools and methods used for all risk management purposes
    - Unified approach instead of separate process for normal risks and product security risks
    - No more tailored Excel spreadsheets for each project that makes post-processing of the process performance data laborious
- From the information management perspective
  - Maintain only one master location of the data
  - Reuse of the common technology assets / methods used
  - Share the information at need with different stakeholders in the ecosystem, define access case by case for each issue instance, if there is a need to share the information with the technology vendors / companies.

4.2.2 *Workflow planning*

Second thing in the risk management planning is to define the workflow for the dedicated risk issue type in the Jira tool. Figure 14 depicts the workflow and state transitions. There are four different states that are: new, open, ongoing and closed. State transition from the new state goes only to open state when a new issue is created. Open risks can be set ongoing state or it can be closed. Ongoing issue can be either closed or set open again. A closed issue can be reopened.

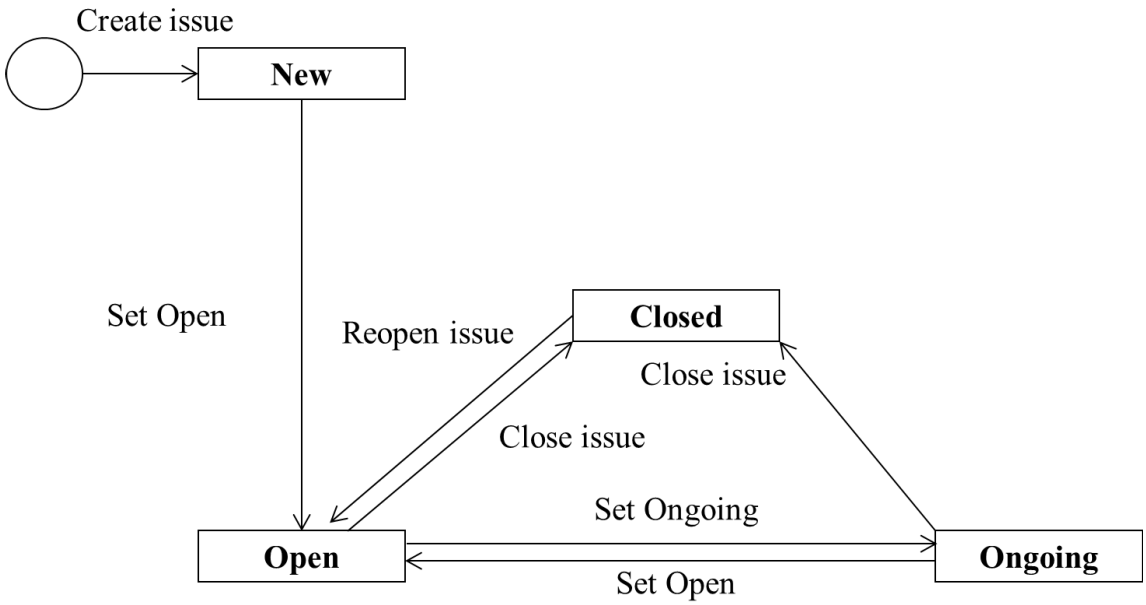

Figure 14. Jira risk issue type workflow.

Workflow status is specified in a following way:

- New: When a risk has just been added and not yet analyzed

- Open: When a risk has been analyzed, but nothing has happened concerning the actions
- Ongoing: When the activities to reduce the risks are ongoing
- Closed: When a risk has been closed and no more actions needed
  - Closed issue has risk resolution (single select):
    - None
    - Controlled
    - Realized
    - Ignored
    - Transferred

The risk issue has own resolution when it is closed. It is possible to reopen the closed issue if it needs to be updated for any reason. For example, the controlled risk might still realize despite of the actions or ignored risk may be taken under control.

4.2.3 *Issue type customization*

A new issue type has been defined for the risks [64]. Table 3 provides an overview of the essential fields. Some common fields for all issue types are excluded. The same tool will be used for both normal and product security/privacy related risks. Centralized data location provides full transparency via dashboards for all different organization levels.

The amount of the specified fields is kept in minimum reasonable level without sacrificing any essential information that can be utilized later on. The options for risk approach are simplified in order to avoid confusion of the concepts among the users that are not familiar with the details of risk management literature. The avoiding approach is used when the likelihood of the risk is being lowered by the actions. The mitigation approach is used when the consequences of risk are being lowered by the actions. Some fields are mandatory to fill before the issue can be saved to database. The new issue can be created and when all mandatory fields are filled, then the saving for the drafted issue is possible. In order to have low entry criteria for new risks, the number of mandatory fields are kept in minimum level. This allows the storing of the risks easily in the Jira tool's database and the optional fields can be filled later on. Mandatory fields are marked with the bold sequence number and field name in the table 3. These are number 1, 2, 3, 5, 13, 14, 15 and 16.

Table 3. The essential fields for the new risk issue type in the Jira tool

#	Field	Field type	Description
1	**Security level**	Single select list	Visibility of the instance of this issue type for different user groups in the ecosystem
2	**Summary**	Text	Short headline for the description
3	**Root cause**	Text	What are the reasons that caused the risk
4	Risk impact	Text	What happens if the risk will realize? Impacts in different areas, such as implementation, testing, quality, schedule, costs etc.
5	Flow phase	List	Which phase in the product development life cycle the risk is hitting. Also includes generic selections.
6	Feature ID	Label text	Which feature(s) the risk is related to
7	Release labels	Label text	Which release(s) the risk is related to
8	Component/s	Multiselect list	Which component(s) the risk is related to (e.g. certain SW module/component, HW etc.)
9	Risk owner	User name	The assignee for the risk responsible for actions

#	Field	Field type	Description
10	Labels	Label text	Free form and dynamic labels, e.g. TopRisk
11	Revisit date	Date	Can be used to put the risk on hold when waiting something to be done first, e.g. test execution.
12	Description	Text	Further background information and relations
13	**Risk category**	Multiselect box	One or more categories: none, project, organization, technical, external, product security/privacy, other.
14	**Approach**	Radio button	Approach for risk management: Avoid, mitigate (minimize impact), accept, transfer
15	**Probability**	Radio button	How likely is the risk realization? This needs to be updated in the course of time. Five options for this.
16	**Consequence**	Radio button	How severe are the impacts of realized risk? This is updated in the course of time. Five options for this.
17	Risk value	Calculated	Value of probability and consequence multiplication varying between 1-25. Jira calculates this automatically.
18	Risk level	Calculated	Quantitative risk level (high, moderate or low). Jira calculates this automatically.
19	Attachments	File	Additional attachments, e.g. risk response plans

The risk issue can have any of the labels and the labels can be easily created on the need basis. The risk issue can be linked with other issues, such as various levels requirement related issues, or actions by using the linked to link type. Risk related actions should be created as sub-tasks for the risk issue instance and those actions should have the label risk. The use of the label risk enables easy inclusion of the risk actions in the suitable gadget in the Jira dashboard.

4.3 Risk management hands on training

Risk management training is planned to be done for each new cross-functional team (XFT) in the early phase. When XFT start working with a new feature development, they will have risk workshop that begins with the training for the agile risk management. This enables just in time training with instant feedback and initial output of the risk management process instead of instead of massive lectures for all employees.

The fundamental mindset about risk based approach and empowered teams is needed first. Risk-based thinking is using a mindset of considering how assumptions people make during planning may not play out as expected, and acting accordingly based on the probability (likelihood of occurrence) and impact (negative or positive effect in case of occurrence). For example, the XFT may be able to take steps to mitigate the negative effects of a risk (reduce its likelihood or potential impact). The XFT may also plan for contingency actions (what would be “plan B” should a risk be realized). Risk-based thinking in all the activities/changes XFT plan and manage helps XFT take a preventative approach into what XFT do, and avoid being caught off-guard. The focus on the high level risks means that risks found to be low probability and low impact are normally just “accepted”. Risks change and must be continuously assessed in a practical way. A realized risk is called an “issue”, and that triggers the contingency plan.

The definition of risk management in brief training in the beginning of the workshop contains following items:[60]

- Risk is the possibility of suffering loss. The loss describes the impact to the project which could be in the form of diminished quality of the end project, increased costs, delayed completion or failure. Examples of factors that can contribute to risk:
  - Unproven technology
  - Unstable requirements
  - Inability to measure real time
  - Dependencies on other projects
  - Resource availability or capability
- The objective of risk management is to:
  - Migrate the unknown risks into the known type
  - Capture the known risks (ongoing throughout the life cycle of the project)
  - Reduce or eliminate the probability of a risk occurring
  - Reduce or eliminate the impact of a risk by developing contingency plans

Activities during the risk workshop contains following phases

- Recap project and set focus
  - Recap project and achievements
  - Set workshop scope and limitations
- Risk identification
  - Identify the risks in small parallel groups with focus areas
  - Present and sort the risk among the whole workshop
- Qualitative risk analysis
  - Estimate the probability of occurrence
  - Estimate the consequence of risk impact
- Contingency planning
  - Choose the risks with highest risk value
  - List expected outcome to reduce the risk
  - List action to reduce the risk
  - Appoint a person to manage the risk
- Optional quantification risk analysis
  - Estimate the preventive cost
  - Estimate the impact cost
  - Calculate the expected monetary value

Last but not least activity is to agree the possible continuation and follow-up for the risk workshop. One must also ensure that XFT is capable of continuously executing the risk management process and they are aware of risk related checklist items for the forthcoming milestones. Proactive project milestone checklist completion makes project progress smoother than reactive approach.

4.4 Replacing the old spreadsheet tool with Jira

The earlier risk management tools have been based on the Excel spreadsheet template. There have been own instances of Excel files for each one of the development release project. These Excel files have had some deviations in the structure making direct data comparison laborious. This has been useful when the development has been done in the traditional way with massive SW release project organizations, but it has not been serving the needs of individual cross-functional teams' nor needs of higher level product development program. Some SW and HW release projects and feature development teams utilized the joint spreadsheet for the risk management reasonably well, while some SW release projects omitted the risk management totally. Additionally, the reporting to various decision fora has used own risk lists embedded into reports. These risks were not

the same ones than in the spreadsheet, but they were added for the leadership team to fill the required sections in the report. This way the software project management can avoid the next management layer to inspect the full risk list and top risks in it. Manual continuous report drafting requires efforts and does not guarantee real time information. There is some waste to be optimized from lean development point of view. Simultaneous editing of the individual file has not been possible, because the document version control allows only one editor at a time [65]. The new feature development has been organized into the smaller projects, where the individual software features have had an own dedicated cross-functional team assigned to it. These XFTs report to development leader instead of the SW release project management. The cross-functional feature project teams have been trained in the early phase of the project to use the new risk management process and tool [60]. The existing ongoing release project's risk data shall be imported into the Jira tool. The stakeholders have been trained to utilize the Jira dashboards for managing the risk list and associated actions. They either reduce the risk's occurrence likelihood or they plan the mitigation the risk impacts if the risk would realize. Any realized risk, or risk with 100% likelihood of realization are not anymore risk, but they are actual problems that have own process for to be followed.

5. RESULTS

The impact of the new agile risk management process with Jira tool can be briefly evaluated by examining selected key performance indicators (KPI) before and after the gradual change. Some early adopting teams have actively started to use the new risk management process, while some other teams prefer to use email as main tool for the project management. Main projects risk management data from the separate project risk database spreadsheets have been analyzed and the totals have been counted manually. Distribution of risk statuses in all risk management excels is shown left in figure 16 and the distribution of the risks between hardware and software development right in figure 15. [66]

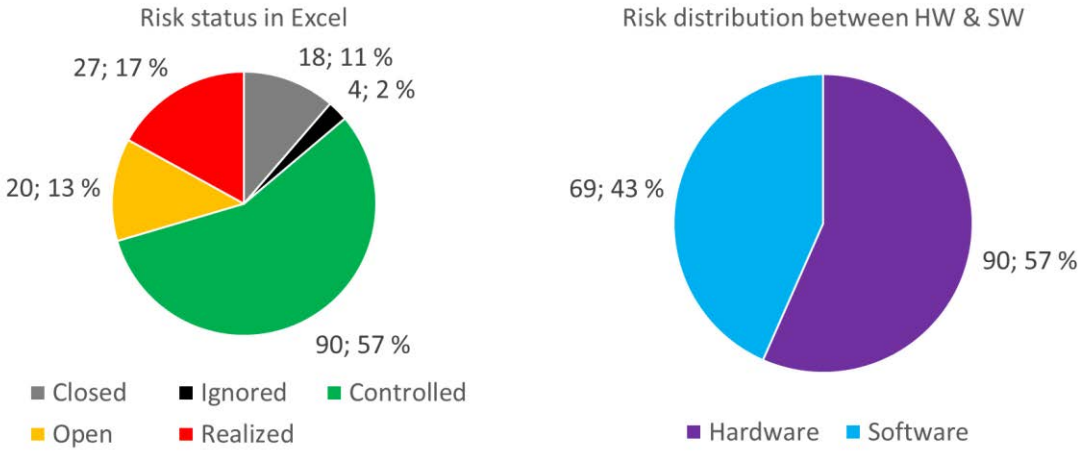

Figure 15. Risks distribution per status and project type.

Over half of the risks (57%) are controlled, while 17% of the identified risk have been realized and 13% of the risks are still open. Closed risks have share of 11% and 2% of the risks have been ignored. Risks are divided into project categories; 43% are software related and 57% are hardware related. While the headcount in the software project is significantly higher, this means that hardware projects put more focus in the risk management. [66]

The severities of realized and open risks are worth examining more since these are contributing to the realized costs and potential costs, or schedule delays, or product quality or customer perception or any and all of those. Severities of realized and open risks are shown in the figure 16. [66]

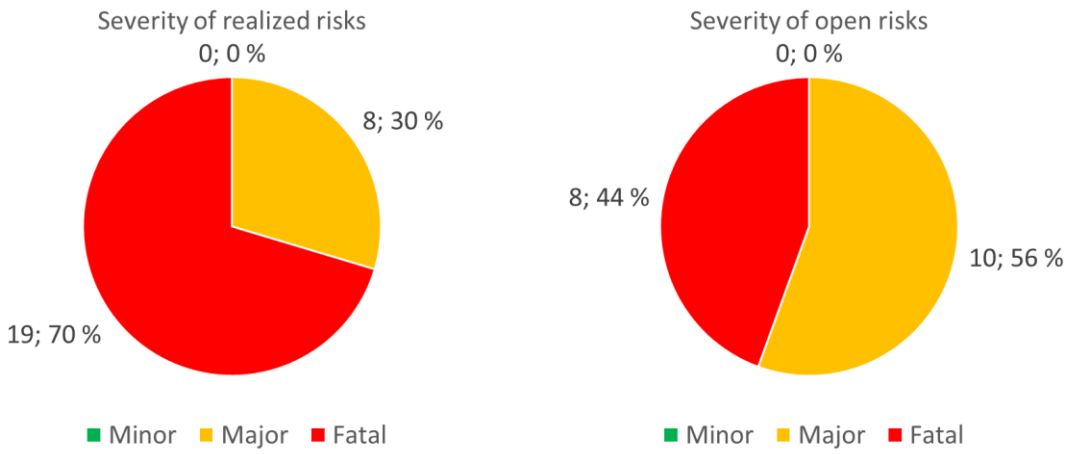

Figure 16. Risks severity distribution for realized and open risks.

Majority (70%) of the realized risks have fatal severity and remaining 30% have major severity, while the low level risk realization has not been tracked. Open risk has 44% fatal risks and 56% of major risks. [66]

Organizational level that is responsible for managing the SW related risk is worth of mentioning, while the HW related risk management is more mature. Figure 17 shows the responsibility division before and after the change. [66][67]

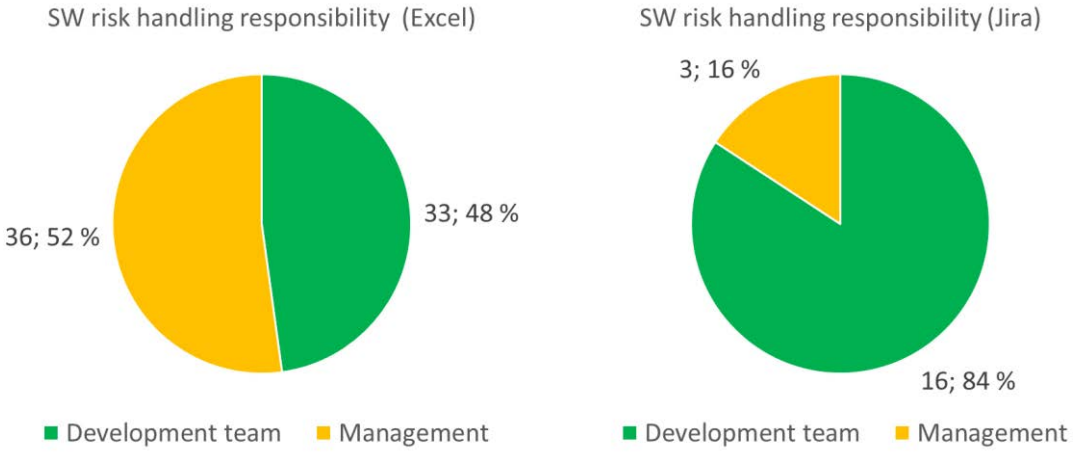

Figure 17. Software related risk handling responsibilities before and after the change.

Prior the change the development team was handling a little bit less (48%) than half of the risk while next management layer was handling 52% of the SW risks. The risk management responsibility is greatly changed after the new risk management process. Although the process roll-out is gradual, the early data shows that development team is handling 84% of the risks while the management is handling 16% of the risks.

It is also worth of mentioning that in any of the cases the risk coverage is far from the full coverage, where all realized problems would be somehow related to the identified risks. There is one new feature project that has actively running the risk management process and they are processing 8 risks in the Jira in agile manner. These 8 risks form half of the risks in the Jira tool defined for the feature development teams. [67]

Evaluating the risk management conducted in the same context but with different approach is useful for benchmarking the different approaches. In addition to spreadsheet or Jira database based risk management there seems to exist a third way of working for the risk management. That is the use of the email system for nearly all leadership and management activities in a release project.

Weekly project status report is created by the development leader working on top of the XFTs. Development leader is reporting to the release project manager. The weekly status report in email format has about 640 – 840 rows of text and with the embedded pictures requires some 22 pages when copied into blank Word document. The email is distributed to 25% of the people working for the release project in a distributed development. [68]

The lengthy report contains 25 risks and only the risk headline is included without any additional information about the risk. Some actions are identified for these risks, there is one ongoing action listed and another action that is in the not started action backlog list. In this case the risk management is limited to the risk identification phase and that information is being reported also to the next management level. [68]

The data shows that 19 fatal and 8 major risk have been realized before the risk management process updates. There also were 8 fatal and 10 major open risks [66]. Expected monetary value (EMV) for these is not known exactly, but the dimensioning can be done by using some selected EMV value for fatal or major risk. If average XFT size is ten people, and project duration is 6 months, the total effort is 60 full time equivalent (FTE) personnel months. Also if the XFT is using high cost laboratories, whom cost is same as resource cost, then one feature project could cost 120 FTE costs in total. If fatal risk yields to average 40% cost increase, this means 48 FTE costs. Similarly, if major risk yields to 15% cost increase, that means 18 FTE costs.

Cumulative EMV for realized risks is 19*48 FTE + 8*18FTE = 1056 FTE cost over the years. Cumulative EMV for the open risk is 8*48FTE + 10*18FTE = 564 FTE. In ideal cases the maximum value from risk management 1620 FTE cost saving. During the five years this means 324 FTE annual cost saving opportunity, which is significant amount! The maximum risk management cost potential in the monthly level is 324 FTE divided by average 10,5 months working time per year equaling about 31 persons per month. This number of persons form typically three or four cross-functional development teams.

While there are major changes done for the risk management process, methods and tools, there are still some more work to be done in the future. In order to evaluate the effectiveness and efficiency of the risk management, the impact of the actions needs to be evaluated. The initial risk value and residual risk value needs comparison but there is only one field indicating this value. Although the change history for the issue is visible, there is no explicit information about the evolution of the risk value available. There are few alternative approaches to evaluate this. One option is to perform post-processing in a spreadsheet tool and the risk value changes in the past can be extracted into own fields enabling comparison. Second option is to apply labels for the risk issues indicating the initial level or change in the level and use the risk value field for the current rating. Third option is to modify the issue type and add separate field for initial risk value.

6. SUMMARY

The thesis begins with an overview and brief introduction to deployment of the agile risk management with Jira into complex product development ecosystem. The main research question is: "What actions are needed to define and deploy agile risk management for the Development Team in Finland?". The research work is a descriptive case study and focus is in the use of the Jira Agile tool for the risk management. Agile development emphasizes empowerment of the team where the XFT manages also risks instead of separate release project management function. Lean and agile way of working yields to use of Jira tool instead of former spreadsheet based tools. Jira is a de facto standard for the tool used in the agile software development globally.

The second chapter covers essential parts of the quality management, risk management and agile product development. Quality management system and new standards impacting to quality management system requirements are covered. One important change in the quality management system standard is the risk based approach. Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.

Third chapter is all about the context for the empirical case study. The applicable quality management system and rationale for the risk management improvement is discussed in detail. The daily use of the quality management system by individual developers helps binding the high level system into daily routines. The rationale for the risk management improvement is based on the internal quality audit results. Both qualitative and quantitative data shows there is a room for improvement in the risk management. The management intent shows that practical approach and value adding via the actions based on the risk management is needed.

The fourth chapter defines how the implementation has been done and provides also answer for the research question. Risk management process has been updated and it is compatible with the Company's risk management guidelines. Risk management is based on the risk management planning, risk identification, qualitative risk analysis, optional quantitative risk analysis, contingency planning and risk monitoring and controlling. Jira tool is customized by adding new issue type for the risk management. Deployment of the new risk management is done gradually. Each new feature development project team is having hands on training combined into risk workshop in the early phase of the project. The existing release project risks from the spreadsheets are imported into the Jira database.

Fifth chapter shows the results and benchmarking of the previous risk management with the renewed risk management. The results show that agile principles and team empowerment in the risk management will improve the performance of risk management process. The benefits of risk management are calculated by using the example project sizes and actual amount of realized and still open risks. Expected monetary value from ideal risk management working flawlessly shows that fully loaded costs of three XFT team per month can be saved in the Development Team in Finland.

The risk management is well known topic and quite often tools used for it are based on the spreadsheets. There are no earlier publications about the Jira usage for risk management. There are few commercial plugins meant for Jira tool, but download amount of those are counted in few hundreds. This is about 1,5 percent of the Jira installations globally. Contribution of this study is the adaptation of Jira tool for the agile risk management use, that can be implemented without any 3rd party commercial plugins.

The limitations of the study are in the monitoring period of new process and tool. While there is a lot of risk management data from the case study prior the change, there are only few feature development projects that have adapted the new risk based thinking into use. However, the initial results are encouraging when the development teams are managing the risks within the team and escalating only few risks to next management level.

Recommendation for further research can be divided into two areas. First option is to continue research in the same context and provide further case studies about risk management. The effectiveness and efficiency of risk management process and especially the value of the actions needs more focus. The monitoring and controlling of the risks' mitigation actions and residual risk levels in comparison with the initial levels is uncovered area. More research could be done in form of case study to compare how well the risks are aligned with the general SW related risks listed in other studies. The agile risk management usage in agile SW projects is also key topic to study more.

REFERENCES

[1] Case material (accessed 18.1.2017). Development team in Finland, 2016. Looking for new opportunities.

[2] International Standardization Organization. (accessed 18.1.2017). ISO 9000 quality management. URL: http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

[3] International Standardization Organization. (accessed 18.1.2017). Moving from ISO 9001:2008 to ISO 9001:2015. URL: http://www.iso.org/iso/iso_9001.pptx

[4] ISO 9001:2015, 2015. Quality Management System Requirements. Swedish Standards Institute SIS: 29 pages. [network document] (accessed 18.1.2017)

[5] ISO 31000:2009, Risk management – Principles and guidelines. Swedish Standards Institute SIS: 24 pages. [network document] (accessed 18.1.2017)

[6] Atlassian Jira software web pages. [network document] (accessed 18.1.2017). URL: https://www.atlassian.com/software/jira

[7] Koulutusohjelmatoimikunta (2015) Kandidaatintyön teko-ohjeet. Oulun yliopisto, sähkötekniikan tutkinto-ohjelma. Kirjoitusohje, 21 s. URL: http://www.oulu.fi/sites/default/files/content/SahkotekniikanKandintyoOhje2016_0.pdf

[8] Runeson, P. and Höst, M. (2009) 'Guidelines for conducting and reporting case study research in software engineering', Empirical Software Engineering, Vol. 14, No. 2, pp.131–164.

[9] Wohlin, C., Aurum, A. (2015). Towards a decision-making structure for selecting a research design in empirical software engineering. Empirical Software Engineering, Vol. 20(6), pp.1427–1455.

[10] Tuominen K, Moisio J. (2015) Laatua, luotettavuutta ja varmuutta: ISO/DIS 9001:2015: itsearvioinnin työkirja: 53 hyvää kysymystä ja esimerkkiparia. Benchmarking, Turku. ISBN: 9789522285195.

[11] MetricStream. (fetched 18.1.2017) ISO 9001: 2015 The 10 Core Elements of an Enterprise Quality Management Program. URL: http://www.metricstream.com/insights/10-core-elements-quality-management.htm

[12] The Plan Do Check Act (PDCA) cycle. ISO 9001 – Quality management knowledge center. [network document] (accessed 18.1.2017). URL: http://9001quality.com/plan-do-check-act-pcda-iso-9001/

[13] ISO 14001:2015, 2015. Environmental management systems - Requirements with guidance for use. Swedish Standards Institute SIS: 35 pages. [network document] (accessed 18.1.2017)

[14] ISO/IEC 27001:2013, 2013 Information technology - Security techniques - Information security management systems - Requirements. Swedish Standards Institute SIS: 23 pages. [network document] (accessed 18.1.2017)

[15] ISO/IEC 27001:2013/Cor.1:2014(en), 2014. Information technology - Security techniques - Information security management systems - Requirements TECHNICAL CORRIGENDUM 1. Swedish Standards Institute SIS: 1 page1. [network document] (accessed 18.1.2017)

[16] OSHAS 18001, 2007. Occupational health and safety management systems. Requirements. Swedish Standards Institute SIS: 54 pages. [network document] (accessed 18.1.2017)

[17] TL 9000 Quality Management System (QMS) Standard. QuEST Forum. [network document] (accessed 18.1.2017) URL: http://tl9000.org/handbooks/requirements_handbook.html

[18] ISO 19011:2011, 2011 Guidelines for auditing management systems. Swedish Standards Institute SIS: 44 pages. [network document] (accessed 18.1.2017)

[19] Fitzgerald, B. (2014). Continuous software engineering and beyond: Trends and challenges.

[20] Dennehy, D. (2016). Going with the flow: An activity theory analysis of flow techniques in software development. The Journal of Systems & Software

[21] Khurum, M. (2010). Requirements management for continuous software product development.

[22] Helakari, H (2017). Value Creation by Agile and Lean methods. Master's Thesis. University of Oulu.

[23] Comparing agile project management frameworks (2017). [network document] (accessed 18.1.2017) URL: http://www.cio.com/article/3175445/project-management/comparing-agile-project-management-frameworks.html

[24] Atlassian Jira Marketplace web pages. [network document] (accessed 2.5.2017) URL: https://marketplace.atlassian.com/addons/app/jira

[25] Atlassian Documentation. What is a Project. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/jira061/jira-user-s-guide/jira-concepts/what-is-a-project

[26] Atlassian Documentation. What is Workflow. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/jira061/jira-user-s-guide/jira-concepts/what-is-workflow

[27] Atlassian Documentation. What is an Issue. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/jira061/jira-user-s-guide/jira-concepts/what-is-an-issue

[28] Atlassian Documentation. Linking Issues. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/jira061/jira-user-s-guide/working-with-an-issue/linking-issues

[29] Wikipedia. [network document] (accessed 2.5.2017) URL: https://en.wikipedia.org/wiki/GQM

[30] Atlassian Documentation. Customizing the Dashboard. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/jira061/jira-user-s-guide/customizing-the-dashboard

[31] Atlassian Documentation. Tutorial - Tracking a Kanban Team. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/agile/jira-agile-user-s-guide/jira-agile-tutorials/tutorial-tracking-a-kanban-team

[32] Wikipedia. [network document] (accessed 2.5.2017) URL: https://en.wikipedia.org/wiki/Kanban

[33] Atlassian Documentation. Viewing the Control Chart. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/agile063/jira-agile-user-s-guide/using-a-board/using-report-mode/viewing-the-control-chart

[34] Atlassian Documentation. Viewing the Cumulative Flow Chart. [network document] (accessed 2.5.2017) URL: https://confluence.atlassian.com/agile063/jira-agile-user-s-guide/using-a-board/using-report-mode/viewing-the-cumulative-flow-chart

[35] DeMarco T., Lister T. (2013) Waltzing with Bears: Managing Risk on Software Projects. Dorset House eBooks Addison-Wesley, 2013. ISBN 9780133492231, 208 p.

[36] Capers, J. 2016. Minimizing the Risk of Litigation Problems Noted in Breach of Contract Litigation. CrossTalk, The Journal of Defense Software Engineering. The USAF Software Technology Support Center (STSC). Vol. 29 No. 5. 36 p. ISSN 2160-1593 URL: www.crosstalkonline.org

[37] Wikibooks, 2016. Project Management/PMBOK/Risk Management. [network document] (accessed 19.1.2017). URL: https://en.wikibooks.org/wiki/Project_Management/PMBOK/Risk_Management

[38] What is PMBOK® Guide's Project Risk Management Process? [network document] (accessed 19.1.2017). URL: http://www.pmbypm.com/pmbok-risk-management-process/

[39] Case material. Company Group Management System (CGMS). [network document] (accessed 18.1.2017).

[40] Cornell University, INSEAD, and WIPO (2016): The Global Innovation Index 2016: Winning with Global Innovation, Ithaca, Fontainebleau, and Geneva. ISSN 2263-3693 ISBN 979-10-95870-01-2. URL: https://www.globalinnovationindex.org/gii-2016-report

[41] Case material. Company Quality Policy, 2014. [network document] (accessed 18.1.2017). Document ID: 011 03-3163 Uen

[42] Case material. Process and Quality System. Quality System Essentials Training Module, 2016. [network document] (accessed 18.1.2017).

[43] ISO/IEC 25010:2011, 2011. Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models. Swedish Standards Institute SIS: 34 pages. [network document] (accessed 18.1.2017)

[44] Wikipedia, 2017. Sarbanes-Oxley Act. [network document] (accessed 18.1.2017). URL: https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

[45] Case material. Company Business Processes (CBP). [network document] (accessed 18.1.2017).

[46] Case material. Product Life Cycle Management (PLCM). [network document] (accessed 18.1.2017). Available only internally.

[47] Case material. Generic Product Requirements (GPR). [network document] (accessed 18.1.2017). Available only internally.

[48] Finland's Ministry of Justice. Finlex Data Bank, up-to-date legislative and other judicial information of Finland. [network document] (accessed 18.1.2017) URL: http://www.finlex.fi/en/

[49] Case material. Company operational quality manual, 2012. [network document] (accessed 18.1.2017). Available only internally. Document id: EN/LZT 108 5252 R4

[50] Case material. Group Directive Audit, Assessment and Certification of Management Systems. [network document] (accessed 18.1.2017). Available only internally.

[51] Case material. Group Policy, Code of Business Ethics (CoBE). [network document] (accessed 18.1.2017). Available only internally.

[52] Wikiquote. Quotes from Tom DeMarco. [network document] (accessed 18.1.2017) URL: https://en.wikiquote.org/wiki/Tom_DeMarco

[53] Case material. Process and Quality System. Map of the PLCM related processes. [network document] (accessed 18.1.2017). Available only internally.

[54] Case material. Process and Quality System. Development unit performance dialog report, 2016. [network document] (accessed 18.1.2017). Available only internally.

[55] WebFinance Inc. The Business Dictionary. Definition of a record. [network document] (accessed 18.1.2017). URL: http://www.businessdictionary.com/definition/record.html

[56] Case material. ISO 9001:2015 and correlation to the Company Group Management System, CGMS, 2016. [network document] (accessed 19.1.2017). Available only internally.

[57] Case material. Process and Quality System. Quality Assessment Data of Development team in Finland. [network document] (accessed 1.2.2017).

[58] Case material. Risk Management Wikipedia. Development team in Finland. [network document] (accessed 1.2.2017).

[59] Case material. Product development milestone KPI guidelines. [network document] (accessed 1.2.2017).

[60] Case material. Process and Quality System. Risk Workshop Guidelines. Document Id: 3/000 21-FEA 202 8683 Uen. (accessed 19.1.2017).

[61] Case material. Process and Quality System. Security Reliability Model (SRM) [network document] (accessed 20.1.2017).

[62] Case material. Process and Quality System. Process instructions: Manage Risks in JIRA. [network document] (accessed 20.1.2017).

[63] Project Management Institute 2004. A Guide to The Project Management Body of Knowledge (PMBOK Guides) Appendix D 286-D-22. ISBN:193069945X

[64] Case material. Process and Quality System. Process instructions: Entering New Risk in JIRA. [network document] (accessed 20.1.2017).

[65] Case material. Extranet collaboration teamsite for the Development team in Finland. [network document] (accessed 20.1.2017).

[66] Case material. Earlier Risk Management Spreadsheets for the Development team in Finland. [network document] (accessed 20.1.2017).

[67] Case material. Risk Management Dashboard of the Development team in Finland. [network document] (accessed 20.1.2017).

[68] Case material. Project weekly email report. [network document] (accessed 20.3.2017).

Table 5. Characteristics of different agile and lean methodologies [23]

Item	Scrum	Lean	Kanban
Definition	A predefined and recurring set of rules, roles and processes used to expedite the release of higher quality products.	The manufacturing and technology principles that are used to reduce waste and increase learning and integrity.	A visual framework that meant to encourage continuous improvement and involves the use of visual workflows to limit work in progress, and match requirements to the ability to deliver.
Industries	Originally applied to software development but now applied within many other industries.	Originally applied within manufacturing industry, but now applied within many others.	Originally applied within the manufacturing supply chain process, but now applied within many other industries.
Primary focus	Focuses on expediting product turnaround and improving quality.	Focuses on eliminating waste (anything that adds no value), system improvements, learning and process integrity.	Focuses on the tasks and improving the processes.
Need determined by push or pull system	Based on a customer pull system (customer pulls when a need exists).	Based on a customer pull system (customer pulls when a need exists).	Based on a customer pull system (customer pulls when a need exists).
Prioritizing work and work in progress (WIP)	Uses backlog to prioritize future work in progress (WIP).	WIP prioritization is triggered exactly when a customer need is determined.	Work in progress (WIP) is matched with a team's ability to deliver.
Collaboration	Requires highly self-organizing teams.	Requires sophisticated processes and precise team collaboration.	Requires less management oversight and highly self-organizing teams.
The development process	Uses formal sprints (repeatable work cycles) with specific roles assigned.	Uses formal processes and team roles.	No formal sprints or specific roles are required.
Flexibility	More formal/less flexible.	More precise processes.	Highly flexible.
Timelines	2 - 4 week timelines for each sprint.	There is no specific timeline but the process should be streamlined.	There is no pre-determined timeline but work is broken down and displayed visually.
Meetings	Limited to 15 minutes/day.	As early and often as required to promptly address issues.	Meetings are as needed.
Changes to requirements	Changes to requirements during sprints are avoided.	Changes are identified and resolved as they arise within the process.	Flexibility allows for changes throughout the process.
Roles	Three roles are key to success (scrum master, product owner and scrum team).	Teams align based on common goals and work closely together.	There are no specific roles.
Measures success	Based on speed of delivery and improve quality.	Based on the use of a just-in-time flow/fast turnaround.	Based on the process duration.