Haaga-Helia
University of Applied Sciences

Integration error monitoring in iPaaS environment and implementation model

Jonna Metso

Master's Thesis Degree Programme in
Information Systems Management
2019

Haaga-Helia
University of Applied Sciences

Abstract

Author
Jonna Metso

Degree programme
Master's degree on Information Systems Management

Report/thesis title	**Number of pages and appendix pages**
Integration error monitoring in iPaaS environment and implementation model	59+6

Company O is using Dell Boomi as an iPaaS platform for several hundreds of integrations and data format conversions. Company O is a publicly listed company and it has operated in Finland for over ninety years. Detailed information of the company is not shared in this thesis due to confidentiality.

Thesis is a case study and it is executed as a qualitative research. Data collection methods used in the thesis are literature review, interviews and observation. Other sources are scientific articles and web publications. Research questions in the thesis are related to integration error situations, implementation process model and further development suggestions on integration error monitoring.

The goal of the thesis and the heart of the case study is to develop implementation model for integrations in Company O's Dell Boomi platform. Already implemented P2P system's integration error messages are used as showcasing what kind of errors there has been in integrations. This study also suggests further improvement actions for the integration error monitoring so that it would be more automatized and efficient.

Key findings from P2P system integration error messages are that majority of errors are related to Master data, poor coordination of service breaks and data validation. The improvement suggestions in this thesis are general and not solely based on the P2P integration errors. Thesis introduces a four-step implementation process model which is adapted from COSO's internal control and process monitoring model. Risk evaluation questionnaire is also introduced in evaluating the integration criticality. The implementation model is adapted to fit into integrations.

Further development suggestions for integration error monitoring in the thesis are better Dell Boomi and Master data ownerships in the organization, enhanced communication, better automation level on integration design and to investigate future trends enablement on the Dell Boomi platform.

As a conclusion of the thesis is that the research questions were answered with the theory and other data collection methods and also an implementation model was created in case study based on the research data.

Keywords
Integration error monitoring, Dell Boomi, implementation model, iPaaS, automation, internal controls

Table of contents

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
APM	Application Portfolio Management -tool
AS/400	Application System/400, IBM series of computers
Atom	A single-tenant, single-node runtime engine
COSO	U.S. Committee of Sponsoring Organizations
Dell Boomi AtomSphere	Multi-tenant cloud integration platform
EC2	Elastic Computing Cloud
ERP	Enterprise Resource Planning
Groovy script	Java-syntax-compatible object-oriented programming language for the Java platform
HTTP	Hypertext Transfer Protocol
Integration	Process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole
iPaaS platform	Integration Platform as a Service
IT	Information Technology
ITIL	Information Technology Infrastructure Library framework
ITAC	Information Technology Application Controls
JAVA script	Programming Language for the Web
Jira Software	Jira is a proprietary issue tracking product developed by Atlassian
JVM	A single operating system process, running on the Java platform
KPI	Key Performance Indicator
Middleware	Layer of software that connects client and back-end systems and “glues” programs together
Molecule	A single-tenant, multiple-node runtime engine
Node	A single Molecule or Cloud JVM running as part of a cluster
P2P	Purchase-to-Pay process area

RPA	Robotic Process Automation
REST	Representational State Transfer
SaaS	Software as a Service
SLA	Service Level Agreement

1 Introduction

Company O is using Dell Boomi AtomSphere as an iPaaS -platform and there are hundreds of daily integrations through this platform. Company O is a publicly listed company and it has operated in Finland for over ninety years. Detailed information of the company is not shared in this thesis due to confidentiality.

Company O implemented new Purchase-to-Pay (P2P) -system in 2019 and in this project Information Technology Application Controls (ITAC) were implemented into Dell Boomi platform and to the sending and or receiving systems where applicable. These control messages were implemented as a risk mitigation instrument and it was also a requirement from the project's Steering group. Integration validation errors or unfunctional interface can have direct impact into the company's operations and business if for example the supplier invoices are not paid in time from the ERP system. Thus the ITACs were implemented for the new P2P system integrations in Company O's iPaaS Dell Boomi platform, there are now automated e-mail messages to system admins and to IT if any of the integrations are in error. Errors are visible also in the Dell Boomi developer dashboard.

P2P -system's application architecture consists nineteen integrations altogether for both inbound and outbound. With the integration error messages, IT application owners and system admins have now better visibility on the integrations statuses and errors are corrected in a more efficient way. P2P integrations are for example Company O's master data, purchase orders, supplier invoices and reporting data. There has been a lot of uncertainty with these integrations with the old P2P system so there was also an improvement needed from the current situation. These control messages are used as a basis in investigating integration error types in Dell Boomi and with literature review and other data collection methods thesis suggests further improvements for integration error monitoring. Study also introduces an implementation process how integration error monitoring could be driven forward in Company O.

Fundamental problem of the thesis are the integration errors and how monitoring can be improved and be more automated? What kind of implementation process could be used in Company O for integration error monitoring? What benefit integration error monitoring brings to the company?

This thesis is conducted as a case study using qualitative research methods. Statistical methods are also used in the qualitative research in order to analyse the what kind of error messages there has been in the P2P integration errors. Other research methods used

in this thesis are literature, scientific articles and web publications reviews, observation and stakeholder interviews. Thesis tries to find the simplest solutions with different research methods so that the improvement suggestions and implementation process is credible and reliable.

The initial phases and implementation of the P2P project and error messages as well as the testing and implementation phases of the control messages are out of scope from this thesis. While the iPaaS and Dell Boomi platform are widely described, the technical environment of Company O is not revealed due to reasons of confidentiality. In the improvement suggestions thesis outlines what is generally possible to implement in an iPaaS environment, it is not necessarily applicable for Company O's platform. The suggested implementation model's testing is also out of the thesis scope.

The goal of the thesis is to investigate the errors on P2P integrations and based on this analysis, literature review and other research findings to suggest improvements for integration error monitoring and current design. Case study introduces an implementation process model for integration error monitoring for Company O. This study also investigates what are the benefits of error monitoring and how the process could be more automated.

The first chapter is an introduction of the thesis. The second chapter is describing the qualitative research method, case study, research questions and data collection methods of the thesis. The second chapter studies also the theory of internal and application controls, iPaaS platform and Dell Boomi will be introduced as well. Chapter three is the empirical part of the thesis describing the error types of P2P system integration messages, case study for Company O and provides answers to the research questions. Last chapter is discussion and consideration of reliability on the results. Chapter four also includes conclusions and evaluation of the researcher's own learning.

2 Research methodology and theory

This chapter concerns defining and discussing the research strategy and approach. It describes the case study as a research method, used data collection methods and research questions. Chapter also contains theory from literature review and main findings gathering aspects and themes.

2.1 Case study

The methodology for the entire study is case study research. In case study the answer to the research problem is gathered from multiple sources. It is like a puzzle which the researcher gathers from multiple sources to get the whole picture. The pieces of the puzzle are the different data sources and from those a large and in-depth picture is created of the case. Usually these pieces are literature, theme interviews, questionnaires and observations. (Kananen 2013, 77.) There are multiple data sources used in this thesis so therefore case study should be quite suitable for this research.

Case studies are particularly well-suited for extensive and in-depth descriptions of complex social phenomena. As such, case studies provide an opportunity for the researcher to gain a deep holistic view of the research problem, and may facilitate describing, understanding and explaining a research problem or situation. (Baxter & Jack 2008.) According to Yin, (2009, 9) how and why questions are better answered through case studies as such questions “deal with operational links needing to be traced over time, rather than mere frequencies or incidence”.

Three strategies for improving construct validity include using multiple sources of evidence, having key informants review the case study report, and maintaining a chain of evidence. Employing multiple sources of evidence can contribute to construct validity by providing multiple measures of the same phenomenon. (Yin 2009, 9.) The reliability of the thesis will be enriched by studying a broad range of relevant literature and scientific articles on best practices in relation to the already existing ITAC process for P2P integrations. The idea of the thesis is to understand the phenomenon and reasons regarding integration error situations. In other words, answers to questions like “why” and “how” are needed and therefore case study and qualitative research methods are well-suited to this thesis.

Thesis describes Information Technology Application Controls (ITAC), and risk management controls, Dell Boomi and iPaaS environments with literature and web publications review on integration errors and further improvement suggestions. Different research

methods are used so that result would be credible, and continuity and reliability are ensured. Case study is a popular research method that can be used when the goal is to develop company's services, processes or operating models. (Ojasalo, Moilanen & Ritalahti 2014, 52.)

The aim of the thesis is to develop further the integration error monitoring for Company O. This study investigates whether already built monitoring process in Dell Boomi can be enhanced and improved. The implementation process is developed in the case study.

2.1.1 Qualitative research

Qualitative research is considered the basis of all research activity because quantitative research is also based on qualitive research. Qualitative research's aim is to understand the phenomenon and understand the texture, factors and relationships between them. The result of the understanding is theory alias generalization of the phenomenon. (Kananen 2013, 26.)

Qualitative research follows general research process chart as illustrated in figure 1. Qualitative research begins with the research problem and its determination which is followed by the research questions and those are answered with the material. If the phenomenon is not known, qualitative research is used. Qualitative research is well-suited to understand a new phenomenon and what is it about. (Kananen 2010, 36-37.)

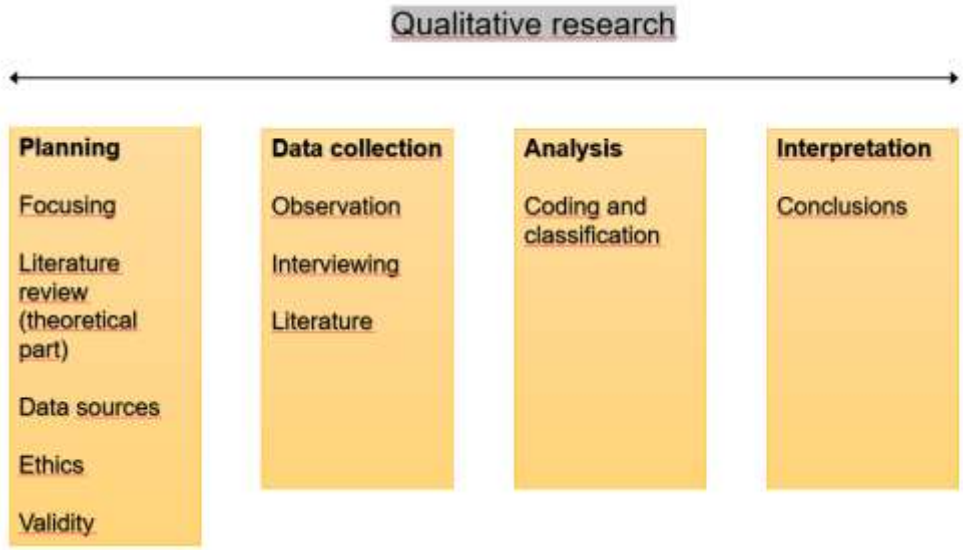


Figure 1. Qualitative research process chart (Kananen 2010, 36 adapted)

Qualitative research produces explanation from practice, this is also called induction. This is a form of reasoning used in pursuit of understanding and knowledge, establishing a relationship between observations and theory. In science it is common to ensure that the theory works in practice. It is common for science to constantly doubt everything. (Kananen 2013, 26.) Qualitative research, as opposite to quantitative studies, places more emphasis on the study of phenomena. Quantitative researchers attempt to remain independent of the phenomena they study with the aim of generalizing findings, where as qualitative researchers engage themselves in the study, viewing the phenomenon as more context and time-specific and in most cases, not generalizable. (Lapan, Quartaroli & Riemer 2011.)

Since the goal of the thesis is to understand the integrations errors and what are causing the errors, qualitative research is suitable for this thesis. Thesis also tries to discover and develop something new and that is also basis of qualitative research. The qualitative data collection methods used in this thesis are observations, interviews, literature, scientific articles and web publications review.

2.1.2 Data analysis with statistical methods

Statistical methods are quantitative research methods but those can be used to a limited extent also in qualitative research. Quantitative questions can be used but those are simple by nature and by scale, those are usually nominal or ordinal-scaled variables. Quantitative calculations can be for example different words, phenomenons or expressions appearance in the observable data. The purpose of the calculations is not to generalize the results as it is understood in the quantitative research but to understand the behaviour or phenomenon. (Kananen 2010, 67-68.)

Qualitative data can be quantified which makes it possible to use also statistical methods. The use of statistical methods requires that that there are adequate number of answers so that the analysis criteria is fulfilled. Quantitative research methods can be used to support the other qualitative data collection methods which strengthens the view gathered from different sources. (Kananen 2010, 68.)

The statistical method used in this thesis is the data collection of error emails from the P2P integration errors. The data is gathered from integration email errors which have been received since June to the end of October. There won't be any generalization done from the errors but the results are used to showcase basic error types and analyse if

these fit to the error types found with literature. The error types will be analysed in such a way that improvement actions are found for the existing P2P integrations and other ones in Dell Boomi as well.

2.1.3 Literature review

Literature helps to understand the phenomenon and provides tools to different phases of the work process. The necessary literature can be defined into substance related literature and methodology literature. Furthermore, literature review is needed to solve the research problems. (Kananen 2013, 81.)

Usually in thesis work, the writer becomes familiar with earlier researches on the topic and what has been written about the subject. Material shouldn't be too general but it should be substantially related to research problems. There should be a golden thread between the thesis and the chosen literature. External literature can be very helpful also on the results and conclusion of the thesis, broad literature brings more validity to the thesis. (Kananen 2013, 81-82.)

Researchers can take advantage of the preexisting related literature in order to see further. Literature can be used more actively in grounded theory studies, just as long as the researcher does not allow it to hinder creativity and get in the way of discovery. It is recommended that researchers remain open to the field they study and the data they are gathering, take a critical attitude toward preexisting theories and research findings throughout the research process, and subject all ideas to rigorous investigation. (Lapan & al. 2011.)

Literature and web publications analysis are used in the thesis to find theory on risk management and internal controls, Dell Boomi and on iPaaS environments. Literature is also used in finding a fit process for the implementation which is suitable for Company O's Agile way of working. Literature analysis is usually used combined to other data collection methods to bring more perspective and viewpoints on the development (Ojasalo & al. 2014, 43).

2.1.4 Observation

Another data collection method used in this thesis is observation. With observation it is possible to get information of the research phenomenon in a natural environment. Observation is systematic scrutiny and based on that the researcher makes remarks on for example on processes and on individuals. (Ojasalo & al. 2014, 114.) This data collection method is recommended to be used when there's no other ways to gather the information such as interviews or queries, and if data is not credible. There can be a lot of hidden information in the organization that cannot be obtained in other ways than with observation. The benefit of observation is the authenticity of the situation. Phenomenon is happening in its natural environment. (Kananen 2013, 88-89.)

According to Kananen (2013, 88), observation is divided into levels as illustrated in figure 2. In direct observation the researcher is following the events of the phenomenon on-site so that the other participants notice the observation. Sample uses of this are interviews, meetings, testing and factory work. In hidden observation the observer persons are not aware of the observant. Observing method depends on the subject of the phenomenon and can the observed persons change their behavior because they are being observed. (Kananen 2013, 88.)

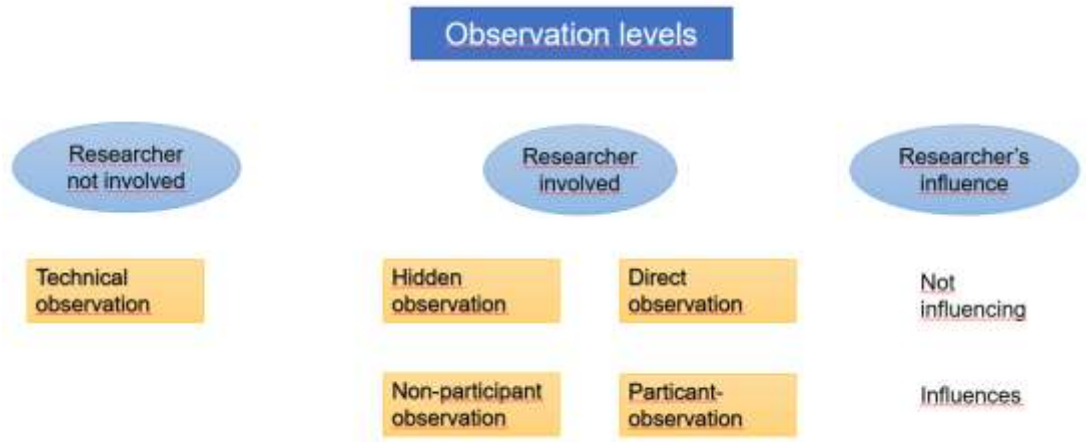


Figure 2. Observation levels. (Kananen 2013, 88 adapted)

Observation in this thesis are the P2P project meetings where the application control messages were defined, tested and implemented and also researcher's observation on the integration errors. This kind of observation is direct and participant-observation since researcher has been present in the meetings and influenced on the scope, defining and testing of the existing P2P integration error messages. Observational information can be

useful in providing additional information about the topic that is being studied. Observations can provide valuable help in understanding actual uses of new technology. (Yin 2009, 110.)

Observation can be challenging method to use because it is time-consuming. It's characteristic that it takes a lot of time and it's not always possible to use enough time to the data gathering by observation. The researcher also needs to understand the phenomenon well enough to separate the observations from own interpretations. (Hirsjärvi, Remes, & Sajavaara 2013, 214-217.) Since this challenge is known by the researcher, it's maybe easier to identify only analytic and worthwhile observations and use also literature to support the findings.

2.1.5 Interviewing

Interviews are considered as one of the most important sources of case study information. Interviews can be vital source of case study evidence because in most case studies the subject is about human affairs or behavioural events. Interviewees can provide important insights into such events or processes. A good approach in case study is to corroborate interview data with information from other sources. Usually interviews are guided conversations rather than structured queries. (Yin 2009, 106-109.)

In interviewing the researcher is in direct linguistic interaction with the examinee and in that way this data collection method is quite unique. The biggest advantage of interviewing compared to other data collection methods is that the data collection can be done flexible in a manner that the situation requires and go along with the interviewee. Usually research interviews are categorized based on how structured and formal it is. Structured interview is done with a fixed form and the order of the questions is set. Theme interview is an intermediate from a structured and open interview, the topic and theme are known but the exact format and order is not set. The third format is open interview and it's almost like a conversation, it's un-structured and free discussion on opinions, feelings, perceptions and so on. (Hirsjärvi & al. 2009, 204-209.)

Thesis uses interviews to fill in the gaps of knowledge especially on the Dell Boomi process configuration and on the platform's capabilities. The interviews have been conducted as a theme interview with Company O's Dell Boomi developer, the questions and the order were not set before the interview, but the topic was. Researcher has held two inter-

views with the developer and this information will be used in the thesis along with the literature sources and observation. Researcher has also had an open interview with the Company O's Head of Technology and Cyber Security on the Dell Boomi platform. Researcher has also had open discussions with Dell Boomi developer and with IT colleagues in the Company O. This data is used on defining the research problem and questions and to get more information on the platform history, capabilities and awareness of the platform in the organization.

2.2 Research problem

Company O has hundreds of integrations via Dell Boomi and currently the error situations are not detected efficiently, there isn't active monitoring in place especially for data content (Dell Boomi developer 31st Aug 2019). Researcher has observed many integration error cases in the organization and sometimes there has been big impacts to the business due to data loss. There is a need to improve the current situation and automate more integration error handling. Thesis research questions were defined after discussion with Company O's Head of Technology & Cyber Security, currently there's no best practice how integration criticality is evaluated or how the integration is monitored in the iPaaS platform. There are over 500 integration processes in Dell Boomi and only approximately five percent of those are monitored actively. (Dell Boomi developer 31st Aug 2019, Head of Technology & Cyber Security, 15th July 2019.)

The fundamental research problem are the integration errors, how to evaluate the criticality and further improve and automate the process. Another important problem is to find an implementation model for integration error monitoring.

Main research questions are:

- What kind of integration errors there has been in P2P -integrations?
- How the error monitoring process could be improved?
- What kind of implementation model there could be for integration monitoring?
- What benefits integration error monitoring brings to the organization?

Research problem defining was sketched with Mind mapping to help in amplifying the case and research questions, see figure 3. MindMap -technique can be used in develop-

ing and sketching ideas and it is easy to use, fast, simple and illustrative. Mindmap is particularly handy on problem solving. (Kananen 2013, 68.) There wasn't any particular Mindmap tool used in the thesis, the sketch was first done on paper and then in Powerpoint.

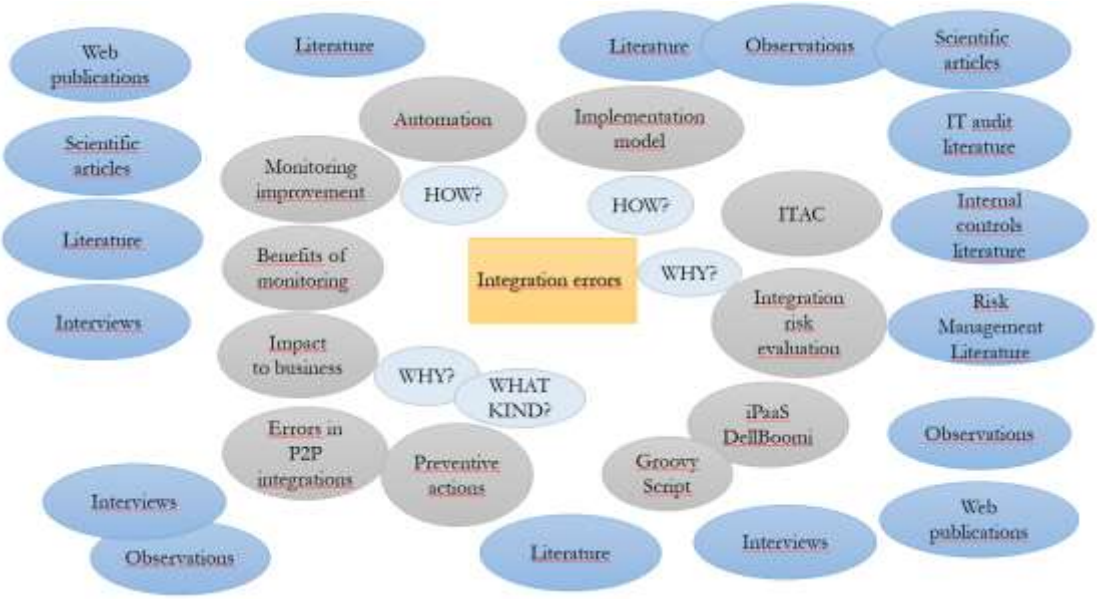


Figure 3. MindMapping of thesis research questions and data collection methods

Mindmapping helped in illustrating and defining the research questions and also how different qualitative research methods will be used in the thesis. Mindmapping also helped finding the main topics of the thesis. Mindmap was slightly changed during the thesis process because the research questions were changed slightly along the way.

2.3 Integration Platform as a Service

Integration Platform as a Service, in short iPaaS, is a set of cloud services or tools used to connect software applications that are deployed in different environments. iPaaS platform allows faster integrations, data sharing and removes barriers in integration projects. Modern integration techniques through APIs and digital transformation go hand in hand to help a company be more open and deliver with consistency the data to support innovation. The benefits of iPaaS platform are for example cost efficiency, real-time data transfers, modern technology, enhanced IT Security on data transfers and technology for data validations. (Siegel 2019.) The most important benefit of iPaaS is that it helps to connect different software applications and synchronize data when data can be accessed from a more centralized location (Reddy 2019).

Middleware is a mechanism that allows one entity whether it's application or database, to communicate with another entity or entities. Middleware is any type of software that facilitates communication between two or more software systems. (Linthicum 2003.) iPaaS platform supports real-time integration and supports all different integration formats and platforms. Usually the iPaaS platform is able to take in and transform data from any of the sources shown in figure 4 and the output can be pushed to one or multiple target systems at any speed. (Gartner 2019a, 3.) A good iPaaS solution should be able to integrate not just cloud but also on-premises applications, making cloud-to-cloud, cloud-to-ground and ground-to-ground integrations easily possible (Reddy 2019).

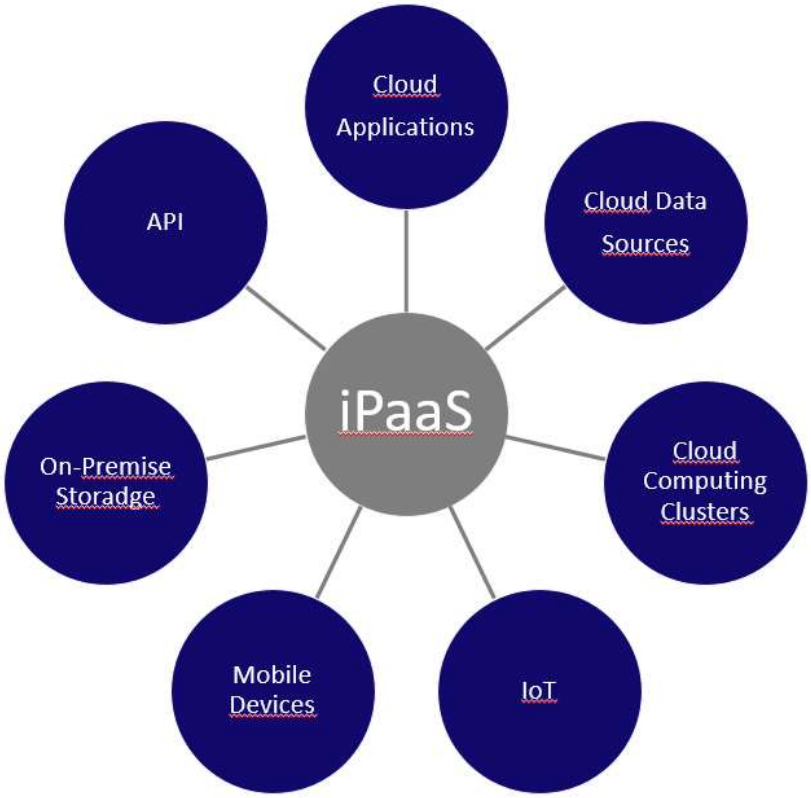


Figure 4. iPaaS as the Centerpiece of the Data Integration (Gartner 2019a, 3 adapted)

According to Gartner (Gartner 2019b, 12), iPaaS offers many benefits such as:

1. **Improved agility and speed**: iPaaS improves agility and delivery time since application integrations and data delivery functions out of the box. Companies respond to business needs and innovations more efficiently.
2. **Lowered initial costs**: iPaaS provides hybrid functions of data and application integration with minor cost.
3. **Empowerment of self-service integration**: iPaaS wizards and tools are easy to learn and use effectively. Administration is also simpler than with traditional on-premises approach.

4. **Less integration complexity**: Integration logic is separated from sources and targets and development can be simplified with iPaaS.
5. **Improved reuse and governance**. Processes can be easily copied to and the governance is easier in a modern environment.

Data integration is becoming more difficult and the tools of the past cannot anymore answer to business needs. The integrations are increasing complexity and therefore organizations need to deploy more flexible iPaaS solutions. iPaaS can be a simple combination of one or two targets and sources but can also support more complex designs using data and database connectors, both on-premises and in multiple clouds. (Gartner 2019a, 5.) An iPaaS solution provides usually prebuilt connectors, business rules, catalogs and transformations that facilitate the development of integration flows and Application Programming Interface (API) management (Reddy 2019).

Different iPaaS providers along with Dell Boomi Atomsphere are for example Informatica, Mulesoft, Workato, Jitterbit and Oracle. There are some trends noticed on the iPaaS providers. First, leading vendors are increasingly including more features that qualify their products as enterprise iPaaS solutions, hybrid integration platforms, or both. Secondly iPaaS vendors offer their platforms with companion products like data quality, master data management, data governance and workflow management. (Gartner 2019a, 17-18.) iPaaS has generated highest revenues from cloud based data services in the industry globally and demand has had significant growth (Singh 2018).

Every platform has weaknesses and iPaaS is not different on that sense. Companies should be aware of the shortcomings in order to mitigate risks. According to Gartner (2019a, 19 & 2019b, 10) some companies may end up implementing several iPaaS platforms and this adds complexity to the enterprise architecture and operational requirements since there can be several overlapping capabilities on these platforms. Company can then have more complicated and an environment which is difficult to manage. Cloud-hosted iPaaS also suffers from shared compute resources and cloud outages just like traditional on-premise platforms. Companies should also take into consideration the total cost of the iPaaS solution since the running costs can be significantly higher than initial implementation cost. iPaaS platform governance need also IT resources and ownership unless this is outsourced to a third party. (Gartner 2019a, 20 & Gartner 2019b, 14-15.) Companies should balance the weaknesses and strengths when deploying an iPaaS solution that it fits into their landscape and business needs.

2.4 Dell Boomi Atomsphere

Company O uses Dell Boomi Atomsphere as iPaaS provider and as a middleware in integrations. Dell Boomi is listed as one of the iPaaS platform leaders (Gartner 2019c, 7). Dell Boomi was based in Chesterbrook, U.S., is a wholly owned subsidiary of Dell Technologies. The original Boomi company was incorporated in 2000, entered the iPaaS market in 2005 and was acquired by Dell in 2010. Dell Boomi is used by over 9000 customers worldwide. Dell Boomi AtomSphere is an on-demand multi-tenant cloud integration platform for connecting cloud and on-premises applications and data. The platform enables customers to design cloud-based integration processes called Atoms and transfer data between cloud and on-premises applications. Each Atom defines what is necessary for the integration. (Boomi 2019.)

Although Dell Boomi's tools are web-based and are in the cloud, architecture is usually executed so that the actual integration and process engine Dell Boomi Atom is installed to client's data center for example on virtual server. Dell Boomi offers five different tools and clients can choose which want they need in their environment; Boomi AtomSphere, Boomi EDI, Boomi API Management, Boomi Master Data Management and Boomi Flow. (Boomi 2019.) In this thesis the focus is on the Boomi Atomsphere and API Management capabilities and how those are enabling the integration monitoring.

Dell Boomi Atom enables customers to integrate any combination of cloud and on-premise applications without software, appliances or coding. Dell Boomi iPaaS platform has been used in Company O since 2015 and over 500 integrations are now flowing through this platform (Dell Boomi developer 31st Aug 2019). According to Company O's Head of Technology and Cyber Security (15th July 2019), Dell Boomi platform was implemented to support company's digital strategy and to enhance IT Security. Company O was using an old AS/400 platform for integrations which was out-of-date technology and didn't support complex business needs anymore nor was it in the accepted IT Security level. Company O was one of the first companies in Finland implementing Dell Boomi platform. Interview questions are listed in appendix 4.

Dell Boomi supports two deployment models: an in-the cloud that is used when all the integration endpoints are cloud-based and on-premise deployment that is used when any of the integration endpoints are within a corporate network. If customer uses the in-the-cloud model, they can deploy integration processes to a Dell Boomi Atom Cloud. In on-premise model, Dell Boomi provides a capability called an Atom, lightweight Java application that is deployed on a host with Internet access. Atoms, Molecules, and Atom Clouds use the

same basic technology but there are differences between them. A Molecule is an Atom with multiple nodes. An Atom Cloud is a Molecule that is available to multiple tenants. Dell Boomi Atom Cloud provides the most features compared to other solutions. (Dell Boomi User Guide 2019.

2.5 Information Technology Application Controls

The importance of risk management in information management has become more pronounced as business becomes more and more dependent on information systems and networks. There are always risks involved in day-to-day decision-making that can jeopardize business continuity and hinder the achievement of the results set for them. Risk management's purpose is to ensure the continuity of the company and the well-being of its personnel. Good risk management is therefore proactive, informed and systematic. It is a way-of-life that helps company's strategy planning and cascade it through the organization when the possibilities, pitfalls and boundaries are identified. (Kuusela & Ollikainen 2005, 15-16.)

Company O has implemented Information Technology Infrastructure Library framework, (ITIL) V3. It is especially used in IT Service Management and Service Design. The ITIL service management life cycle is a series of interrelated best practice processes that support the management of the IT infrastructure and management of the enterprise. IT applications are in the center of this puzzle and are a key central area of internal controls and IT governance concerns. ITIL's message is that management processes should be installed to link business needs and requirements with the IT infrastructure, including its operations, applications, and management. A strong set of ITIL processes will result a wide range of improvements, including a better internal control environment. (Moeller 2013, 88-91.)

U.S. Committee of Sponsoring Organizations (COSO) internal control framework emphasizes that control procedures are needed over all significant IT systems—financial, operational, and compliance-related. COSO internal controls break down information systems controls into the well-recognized general and application controls. The COSO internal control framework has become the worldwide standard for building and developing effective internal controls. (Moeller 2013, 60.)

In the scientific article by Bounagui (2019, 98-118), it is pointed out that COSO solely is not enough for adequate IT governance but it should be a combination of different frameworks. Bounagui (2019, 98-118) also states that the unification of multiple models can help organizations better overcome also the Cloud computing (CC) governance challenges. According to Bamberger (2006, 56), good IT governance begins with good corporate governance and that COSO is known as “the gold standard” of corporate governance. Good IT governance means complying and anticipating with change since it is constantly occurring. IT governance is development and enforcement of effective policies and procedures. The commonly used IT management and governance models are ITIL, COBIT, and ISO/IEC 27001/2. (Bamberger 2006, 56.)

As illustrated in figure 7, the COSO internal framework is considered as a pyramid model with the information and communication components not a horizontal layer but a side element that spans across other components. Information and communication are important portions of the internal control framework but are each distinct internal control components. Adequate information must be communicated up and down of the enterprise in a manner and timeframe that allows people to carry out their responsibilities. Enterprise needs information at all levels to achieve its operational, financial, and compliance objectives. (Moeller 2013, 60.)

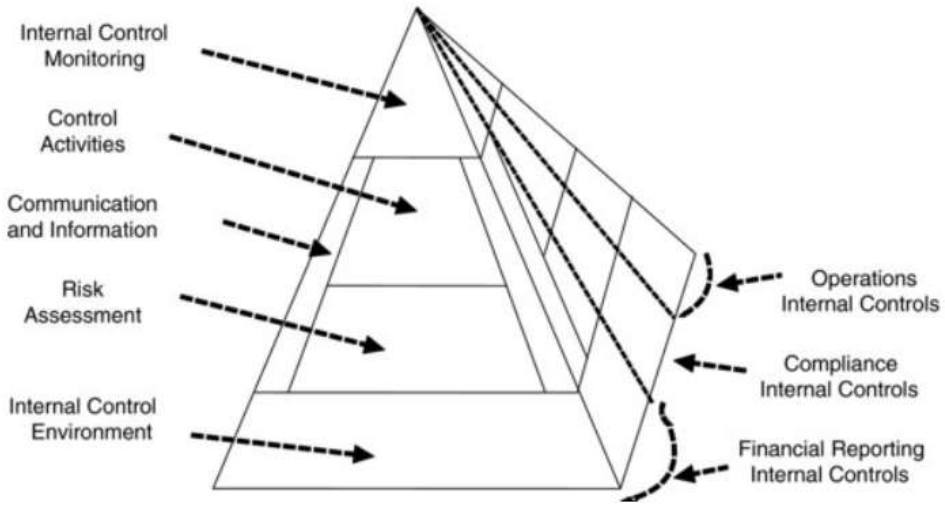


Figure 7. COSO Internal Control Foundation Components (Moeller 2013, 60)

The pyramid view of COSO internal controls in figure 7 shows the monitoring component as the upper level of the COSO internal control components. While internal control systems will work effectively with proper support from management, control procedures, and both information and communication linkages, processes must be in place to monitor these activities. Inadequate internal control processes can result into inefficient or ineffective processes. (Moeller 2013, 62.)

Application controls are controls over the input, processing and output functions. These controls help to ensure data accuracy, completeness, validity, verifiability, and consistency, and thus ensure the confidentiality, integrity and availability of the application and its associated data. In error reporting and handling, controls are needed which determine what happens to a batch that has an error, do we reject only that transaction or the whole batch, who takes action on the error and is there a need to flag an error? In addition to integration errors, it is also important that unauthorized access is prohibited to the data (Magee, 2014).

Usually key control points in today's IT environment are those which directly affect confidentiality, integrity, and availability (CIA). Confidentiality means that a person should only have access to the data, systems, hardware, and so on that they need to be able to do their tasks. This access should be reviewed periodically, no less than annually and definitely if there's a change in employment status. Integrity refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification. And then finally availability means the data and or system is available when it is needed. Usually IT auditor want to look at disaster recovery plans, recovery time objectives and recovery point objectives. (Magee 2014.)

Application controls refer to the transactions and data relating to each application. According to Mendez (2015, 16-18), different types of Application Controls are:

A. **Input Controls**
   Controls which are designed to assure that the information processed by the system is valid, complete and accurate

B. **Processing Controls**
   Controls over processing are designed to assure that data input into the system is accurately processed

C. **Output Controls**
   Controls which are designed to assure that generated data by the system is valid, accurate and complete

D. **Controls over master data**
   There should be procedures in place to verify that the correct version of Master data is being used

The first and second point refer to data validation controls in terms of data correctness and processing and most systems already have these controls in place. Output controls most likely are in place already since most systems have a control usually for the batch job whether it has been successful or not. Sometimes systems are not checking whether

the data is valid and complete so this kind of control could be implemented into the middleware.

Tähtinen (2005, 103) writes that the enterprise architecture should be designed in a way that there is a control level between the integrated systems. This model is illustrated in figure 8. Co-operation between all the systems in the enterprise architecture should be organized in a way that the data transfers are possible to be controlled and monitored from one or multiple centralized point. It is important to ensure that data integrations are working what they are designed for and without interruptions. (Tähtinen 2005, 103.) In Company O the data transfers are in most cases transmitted via middleware and not as point-to-point integrations. This architecture design enables the centralized controlling and monitoring of the integrations.

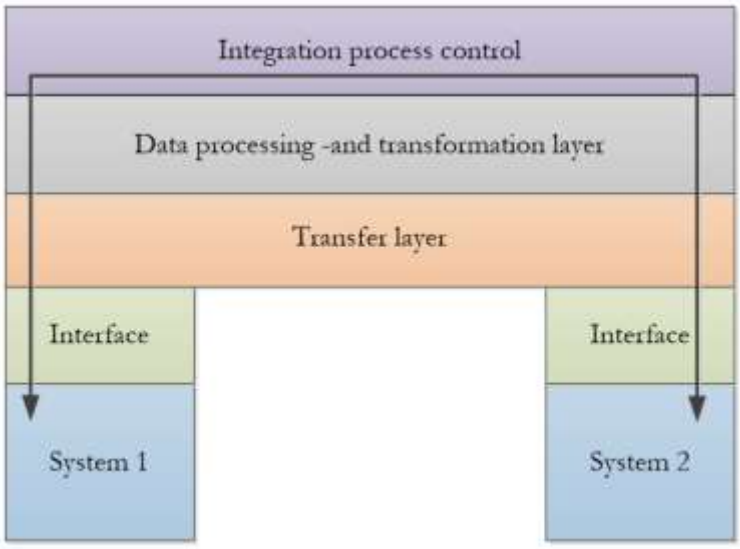


Figure 8. Architecture model with integration controlling (Tähtinen 2005, 64 adapted)

While getting a business through integration it should be remembered that the processes and applications are likely to error. There must be strong monitoring and management for any errors that come about in the process of integrating data and workflows. There must be a separate system looking after the error chances. (Abbas, Chawla & Hussain 2015, 75.) IT auditors often emphasize the security measures implemented to protect information in transit across interfaces and to control access to interfaces produced by each system. Interface audits rely on both documentation such as formal interface specifications and tests that demonstrate the correct function of each interface. (Gantz 2014, 119.)

2.6 Implementation process for integration controls

Enterprise IT architecture sets the over all big-picture rules for enterprise activities and IT governance. Figure 9 is illustrating series of other activities of IT governance. IT governance affects business performance and it ideally helps an enterprise to improve its competition. Moeller (2013, 6) states that IT governance defines business performance, specifically the performance of IT resources as they are used to achieve the business's strategic objectives. It is no more likely that a single IT governance process will work for all IT business processes, a number of IT governance-related processes must be considered. Once organization has decided the best IT governance frameworks, tools and best practices, it is time to implement them. (Moeller 2013, 5-6.)

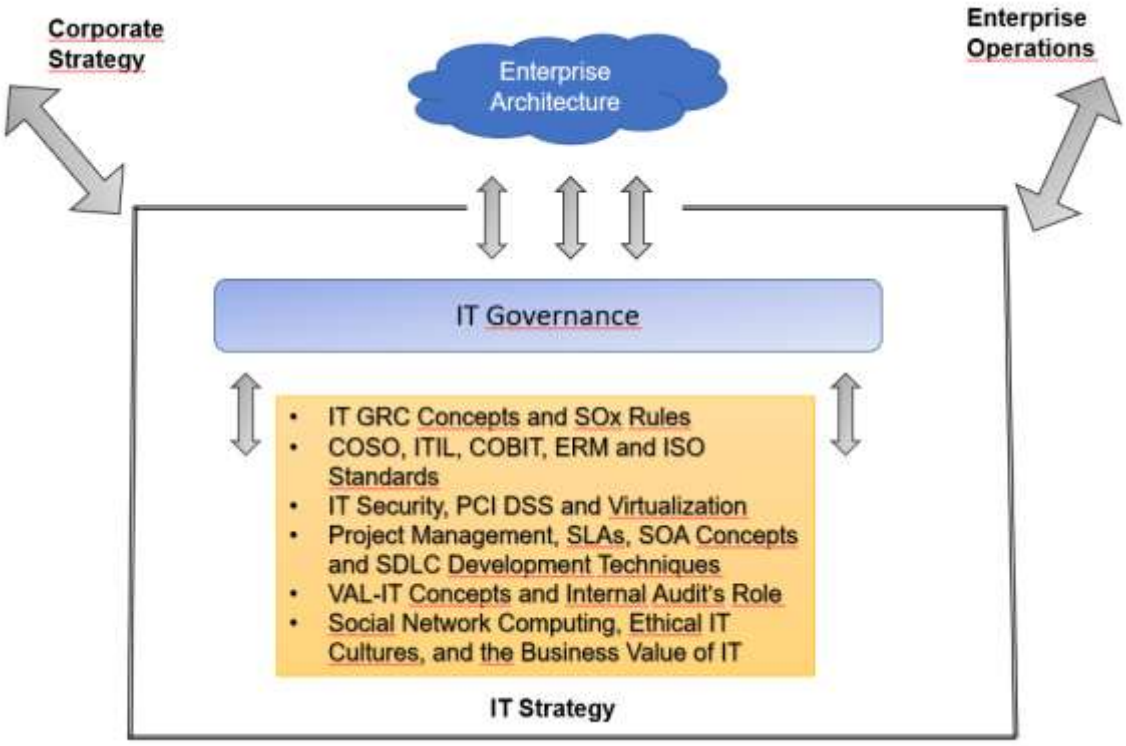


Figure 9. IT Governance concepts (Moeller 2013, 5 adapted)

As stated in previous chapter, Company O has already ITIL V3 framework in use and for example PCI DSS 3.2 and other standards implemented in several systems and processes. But currently there isn't any standard implementation process in use for integrations in Dell Boomi nor are there any integration control messages implemented as default. iPaaS platform and Dell Boomi capabilities don't seem to be widely known in the organization and therefore the implementation process is currently handled as the respective IT application owner sees fit (Dell Boomi developer 31st Aug 2019). Company O is moving towards the Agile way of working so the future implementation model should fit into Scrum, Kanban and other Agile frameworks. There was also a requirement that the

implementation model should be simple, use already existing systems if possible but still have necessary controls in place (Head of Technology and Cyber Security 15th July 2019).

Researcher has found couple implementation processes that could fit to the Company O's current IT architecture, best practices and Agile way of working. These models have been gathered from internal control and IT audit literatures. First one is COSO's framework which suggests that enterprises could establish a four-phase monitoring process as shown in figure 10. This approach says that the enterprise should first prioritize and understand the risks to its organizational objectives, and then identify the controls that address those prioritized risks. The third step is the identification of information that will persuasively indicate that the internal control system is operating effectively. The suggested model calls for implementing cost-effective procedures to evaluate the information gathered through monitoring processes. (Moeller 2013, 65.)

Figure 10: COSO Monitoring Design and Implementation Process (Moeller 2013, 65 adapted)

COSO released the report entitled "Internal Control-Integrated Framework" in 1992 in an attempt to illustrate a systematic framework for internal control. But the report failed to list additional criteria in the implementation and assessment of IT controls. (Chang, Yen, Chang & Jan 2015.) COSO's Enterprise Risk Management (ERM) framework didn't tell more guidance or standards to IT -related issues. Nevertheless considerable detail and attention should be allocated to an organization's IT controls and processes. (Moeller 2013, 147.)

ASQ Auditing Handbook (Russell 2005, 236-238) lists three processes for problem solving and process improvement: PLAN-DO-CHECK-ACT (PDCA), Sig Sigma Model (DMAIC) and Lean Manufacturing. From these processes PDCA cycle, that is also known as Shewchart or Deming cycle, is chosen to be an option for implementation of integration monitoring. PDCA cycle illustrated in figure 11 is an iterative approach for continually improving products, people and services and it is part of Lean management. The model includes solutions testing, analyzing results and improving process. In the first stage there needs to be a plan what needs to be done, what is the core problem that needs to be solved. Second phase is to determine whether actions will achieve the desired result. Third phase is compilation and analysis of the results and last phase is the decision in which the management determines whether actions have achieved the desired benefit and result. The repetitive approach helps the team to find and test solutions and improve them through a waste-reducing cycle. (Russell 2005, 236.)

PDCA enables continuous improvement, as well as evaluation and verification of the effects achieved. Different applications of PDCA cycle have been implemented with positive results achieving the reduction of costs and defects, as well as improving the quality of process and products. It is a useful method to decrease the number of defects of different processes or products. (Realyvásquez-Vargas, Arredondo-Soto, Carrillo-Gutiérrez & Ravelo 2018.)

Figure 11. PLAN-DO-CHECK-DO -cycle (Russell 2005, 236 adapted)

Third option for the implementation process is, that it is done fully as an Agile development. Company O has Agile way of working already in use and such frameworks as Scrum and Kanban are used daily in some teams. Agile software development is an umbrella term for a set of frameworks and practices based on values and principles expressed in the Manifesto for Agile Software Development and the 12 principles. Agile should be considered as a mindset and not as a framework to get full potential for the development. (Agile Alliance 2019 & Agile Manifesto 2019.) Many organizations adopt agile practice to deliver the project on time and faster than other approaches (Agrawal, Singh & Sharma 2016, 1). Agile software development cycle is presented in figure 12.

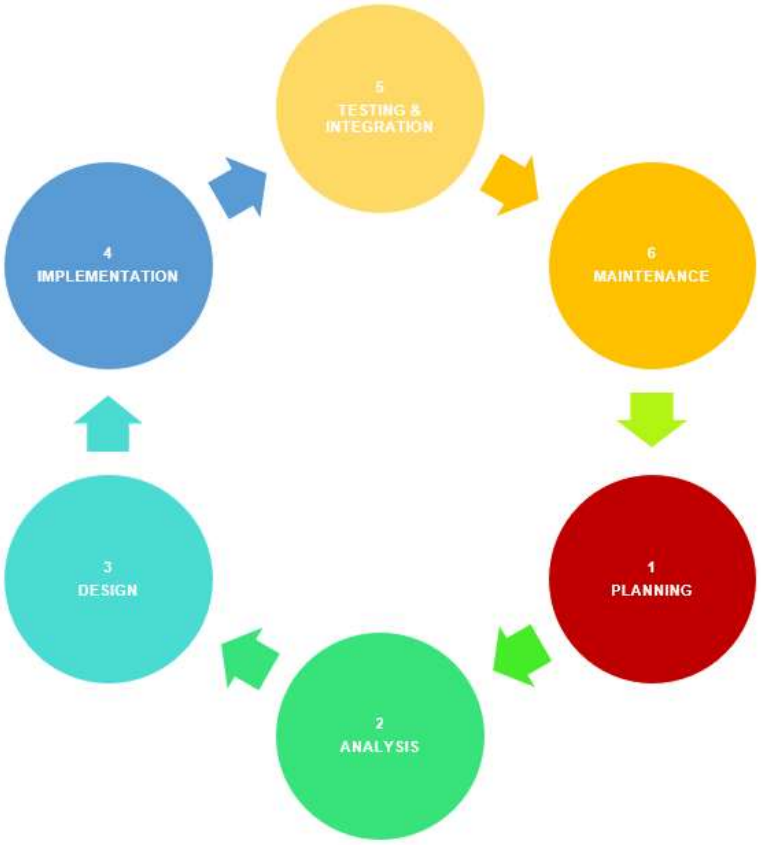


Figure 12. Agile Software Development cycle (Agile Alliance 2019, adapted)

Ylimannela (2011, 1-2) has written that Agile software development doesn't always consider the risk assessment and the Agile methods have created new challenges in the field of risk management. Risk management in agile software development is not an easy as risk management is a heavy process. But risk management is a key to increase security and there are ways to integrate it so that the Agile development does not suffer. (Ahola, Frühwirth, Helenius, Kutvonen, Myllylahti, Nyberg, Pietikäinen, Pietikäinen, Röning, Ruohomaa, Särs, Siiskonen, Vähä-Sipilä & Ylimannela 2014, 29.)

Ylimannela (2011, 2) has created a model for managing risks in Agile environment and it contains all the major risk management phases. The model is designed to be part of Scrum but it could be applied to other Agile frameworks as well. Model is using a risk board that the team can use to get an idea about the general risk level in the project or development. The size of the risk is calculated by multiplying impact and probability. The risk is showcased with sticky notes which is stating the field where the risk is related, who is responsible for implementing the feature and a short description of the risk. The sticky notes for risks have two colors, red and yellow. The red notes are risks and yellow notes response solutions. There are also a checklists for the risks identified from past experiences and high-risk components which indicate for example security requirements. The person who is responsible for a feature is also responsible for applying necessary risk responses so he or she is the risk owner. (Ylimannela 2011, 3-5.)

As a conclusion of the three implementation models, COSO's monitoring process model seems to work better for Company O since there's possibility to utilize centralized monitoring and tools to prioritize integrations and identify controls for monitoring. The model also contains a step to analyze the integration criticality and risks which is required from the future model. The model is simple and doesn't require extra tools or applications to be implemented, Company O's current Application Management tool could be used with this model. Model calls for implementing cost-effective procedures to evaluate the information gathered through the monitoring process. (Moeller 2013, 66.) COSO model will be just adjusted slightly to fit into integrations.

PDCA cycle and full use of Agile development were not chosen since those haven't been used widely yet in the organization. Agile development with Scrum and Kanban are used to some extent but only in the digital teams and the Agile way of working still requires further trainings in the organization. The model by Ylimannela (2011, 2-5) is considered however in the last phase of the implementation since this phase of the model is done with Scrum.

The model created by Ylimannela (2011 2-4) is simple with the risk board and sticky notes so it is fits well to Scrum and could be used together with the COSO model. It is not known by the researcher whether current Agile teams in Company O are already using risk board or sticky notes in their development so this would be checked from the respective teams to establish same model within the organization. The implementation model can be a hybrid from several frameworks and models since it has been stated in the internal control theories that usually not only one framework is enabling adequate controls.

2.6 Risk evaluation on integrations

There should be an understanding in the company of the risk assessment process. Internal control -related risk assessments should be performed in all levels and in the whole enterprise. (Moeller 2007, 166.) The COSO internal control framework describes risk assessment as a three-step process (Moeller 2007, 166):

1. Estimate the significance of the risk
2. Assess the likelihood or frequency of the risks's occurring
3. Consider how the risk should be managed and assess actions

Management has responsibility to go through the steps to assess whether risk is significant and if yes, necessary actions must be taken. COSO emphasizes that risk analysis can be critical to the company's success. The risks can be due to external or internal factors or be specific to an activity such as information systems. (Moeller 2007, 166-167.)

What constitutes risk and what are necessary actions to take part in risk management vary from organization to organization. According to ASQ's Auditing Handbook (Russell 2005, 196-107), risk has four main components: probability, hazard, exposure and consequences. A simple approach to the classification of the elements of risk can be done by category, such as "high", "medium", "low" or defining by colours "red", "yellow" and "green". Evidence of such assessments can be used to demonstrate the cautiousness and due care by establishing what risks were evaluated, how they were classified and what was done to address or mitigate the effects.

Risks analysis is a tool to evaluate risks. Risk analysis is effective if risk targets are identified, in practice this means that organization should be able to identify risk situations with different methods. (Chorafas 2007, 27.) According to Suominen (2003, 35), risk analysis's task is to find out:

- risk targets
- risk probability
- risk severeness
- risk consequences

ISO27002 has listed that additional controls may be required in systems that process or have a link to systems that process for example confidential data. Risk assessments will define the need for these controls and there are four sections (Calder & Watkins 2012, 269-271):

- input data validation
- control of internal processing
- message integrity
- output data validation

Since application systems are vulnerable to incorrect or corrupted data, there should be a control for the data validation when data is input to the system. This applies to controls for example data related to customers, vendors or a log that records the activities of people involved in data input. Control for internal processing means validation check in the system when the data is processed. Risk assessments should identify problem areas or vulnerabilities in the system. These consists such as batch controls, run logs, validation of system-generated data and hash totals of records. Third section is message integrity that requires the organization to use message authentication for applications when the integrity of the message content needs to be protected. The last sections in for output data validation and this is for the requirement to validate data output from an application system to ensure that processing data is correct. Although there would be input and data processing controls in place, it doesn't ensure that the output data from the system is correct or corrupted. (Calder & Watkins 2012, 269-271.)

As Company O already has a four-step evaluation in use for application criticality, the steps described by Suominen (2003, 35) seems to work better for risk evaluation questions on integrations. The model should be simple enough so that it doesn't cause too much extra work to IT Application owners but is nevertheless comprehensive, contains risk evaluation and is fit to integrations. Company O's Application Management tool (APM) has already Criticality and risks evaluated from 0 to 100 and with different colors so this model will be used also for integrations but in addition to that there would be also risk assessment questions for the IT Application Owners. The risk assessment questions are compiled to find out risk targets, probability, severeness and consequences.

3 Empirical part

In this chapter the nature of P2P system integration errors are investigated and thesis suggests improvement actions for further development. In the case study there's introduced an implementation model for integration monitoring in Company O. This chapter answers to the research problem and questions and presents improvement suggestions. The last chapter in this section is a summary of the findings and the case study.

3.1 P2P integrations error messages

With the use of an integration platform, a business can gain a competitive edge in the market with the least errors and redundancy (Singh 2018). iPaaS platforms usually provide different kind of visual dashboards showing both the system health and integration status. Figure 13 is showing a sample of Dell Boomi platform showing integration errors and the dashboard for one day.

Figure 13. Dell Boomi dashboard from Company O platform (Dell Boomi 21st Oct 2019)

In the interview with Dell Boomi developer it was discovered that the dashboard is only showing process errors from 1, 6, 12 hours or from 1 day. The dashboard is not showing errors for a whole month or more. (Dell Boomi developer 31st Aug, 2019.) Therefore it is hard to analyze thoroughly how many errors there has been on daily or monthly basis on all integration processes since there's no stored records of it. There are reports available which are fetched with an API integration from Dell but those are showing only 35 days of data executions and the processing errors. This report is in csv format. It would give some indication how many errors there has been on a daily basis on one month but since the

data is available only of the last 35 days then it is not so credible to base thesis analysis on that data.

As the Dell Boomi dashboard has data only for one day, P2P system integration error monitoring e-mails are used as a basis data showcasing different integration error messages triggered by Dell Boomi. Dell Boomi is used as a middleware in all integrations for the new P2P application and these nineteen integrations have customized monitoring e-mails in place. New P2P application had go-live on 10th June 2019 so monitoring e-mails are considered from June onwards and only from production integrations. Table 1 is illustrating the error monitoring e-mails count and types since June 2019.

P2P application go-live in June is shown also on the error messages as there's only 70 error e-mails generated. The go-live in June was only with two Company O subsidiaries which didn't have much invoices or other data transfers. July has also been a quite error free month due to the above reasons and the fact that many of the people were on holiday, so data wasn't processed much in the system. But in August the error monitoring messages have multiplied when the whole Company O was using the system and there were thousands of purchase orders, invoices, Master Data and other data sent in and out of the system.

Table 1. P2P integration error e-mail types and counts (Dell Boomi 31th Oct 2019)

Count of Subject	**Column Labels**					
	june	**july**	**aug**	**sep**	**oct**	**Grand Total**
Row Labels						
Master data	57	148	924	519	611	2259
Service Break error			53	6	246	305
Technical error	12				1	13
Validation error	1		1	1	2	5
Data content error			2	35	756	793
Grand Total	**70**	**148**	**980**	**561**	**1616**	**3375**

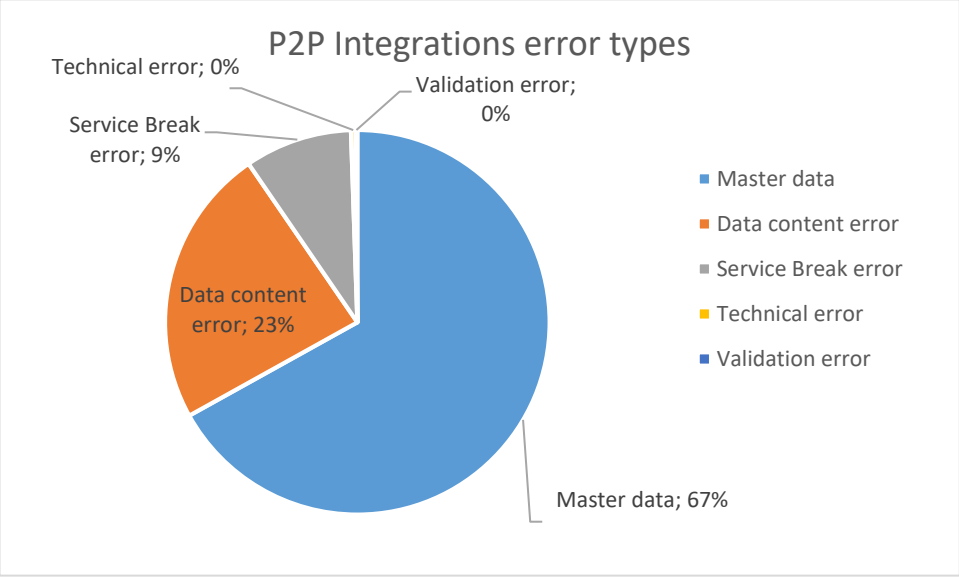
After analyzing the errors with observation, majority are related to Master data issues between the Company O's ERP and the new P2P system. There was also scheduled service break in the company's ERP and the new P2P integrations were not considered in the break which caused also several error messages. In September there has been less integration errors but then again in October the count has tripled. In October there was a new Dell Boomi process taken into use on incoming invoices and this has caused many data content related error messages which indicates that maybe testing hasn't been very thorough or there are some data inconsistencies. In October there has been more of

these error messages than Master data errors. Uncontrolled service break between P2P and ERP system has also caused a lot of error messages, especially on October.

The different error type percentages have been categorized in table 2, majority of issues in all months are related to Master data. Data content errors are second most common type and Service breaks are third largest reason. In this perspective, the technical errors due to connectivity or other reasons are not so common. Nevertheless if there's a connectivity issue, the whole traffic between the systems can seize so the impact on technical issues can cause issues to several files where data content issues can only have minor impact.

The Master Data error count is over 67% of the errors, on average there's seventeen error messages per day only for MD. After analyzing the e-mail contents, the same errors have persisted since June. The count of messages has increased in October, perhaps some new MD hasn't been aligned between the systems. Since the count of MD errors hasn't been getting lower during these months, a question rises of the daily tasks related to checking these emails and correcting the MD. Is data really been corrected by the team and are necessary action been taken to prevent the error from happening again? There can be new vendors daily but the general MD with general ledger accounts and cost centers are not changing frequently which could explain the increase in error messages. These results require more investigating of error handling in the company.

Table 2. P2P different error message type percentages (Dell Boomi June – October 2019)



In Dell Boomi dashboard there's daily process monitoring as well. Dell Boomi developer (Oct 21st 2019) mentioned that in many integrations the errors are related to Master data,

there's a lot of mismatch between different systems and the developers cannot correct those errors. And if the error is related to data content, Dell Boomi team cannot help. Dell Boomi team only corrects whether there is a connectivity error or other technical issue on the integration. (Dell Boomi developer 31st Aug & Oct 21st 2019.) It seems that there is not enough attention or ownership in Company O to the Master data and its cleanup activities significance in projects, this causes a lot of integration errors which leads to unnecessary manual work and causes risks to business continuity.

iPaaS platform's dashboards are handy for the developers to get information on daily basis on integrations and follow-up on errors. But there can be a lot of errors, how the developers know which ones are meaningful for them to fix? As showcased with P2P integration errors, the Dell Boomi developers cannot do anything and they shouldn't because they do not own the Master or business data. It is not good policy due to auditing that incoming data is changed into something else if the failure is originating from the sending system, data integrity must be ensured. iPaaS platforms should be considered only as a tool for data transfer and conversion but not to correct erroneous business data content. The corrections of master data should be done by the business system administrators or other owners and therefore they should be informed of the errors.

In the Dell Boomi processes, Groovy script is used in 75% of the cases because it has more capabilities (Dell Boomi developer 31st Aug 2019). The Apache Groovy script is described to be powerful, optionally typed and dynamic language which improves the developer's productivity with familiar and easy to learn syntax. (Groovy Apache 2019.) The current error messaging process in Dell Boomi is executed with Groovy script as a Try/Catch -process. If any error occurs in the transformation stream, error message gets generated and passed to Catch terminal where there is a subprocess Error Handling to for further processing. The Error Handling -subprocess consists email notification to required recipients, error message logging and further stop the transactions/processing. If the further transaction or processing needs to be stopped in case of any error, Dell Boomi uses Exception Shape. The error messages can be seen in the Errors section under Process Reporting of Dell Boomi platform (Dell Boomi developer 31st Aug & Appendix 6). Sample Error Handling process is illustrated in figure 14.

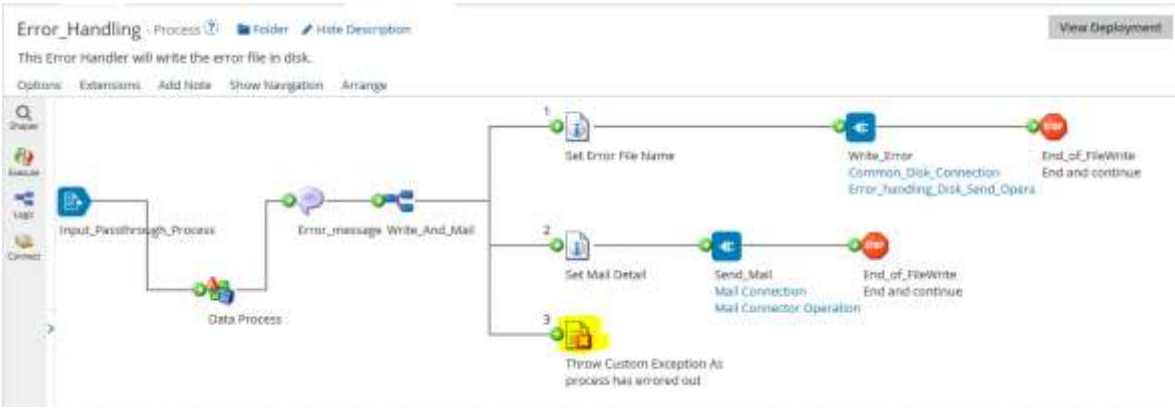


Figure 14. Dell Boomi Error Handling process (Dell Boomi Oct 2019)

Integration error monitoring in iPaas environment should in minimum have a log functionality in place to show which integrations have been successful and which haven't. When an error message is generated, it is vital to understand why the error has happened and solve it. And solving should be done in a way that it doesn't happen again. Information about the error should also be delivered to all necessary stakeholders and agree what action is taken place when the error message is received.

Data quality is a continuous process that requires discipline and a well-planned out maintenance process (Data Integration Handbook 2019, 8). Master data clean up before integration go-live and maintenance plan must be in place. Integration errors can also be avoided if Master Data is validated between the systems. ERP system can store for example company address is multiple tables and fields where as the receiving system is having data only in one table and in different format. The systems can also have the Master data in different format, other is having for example commas in figures and other is having dots. (Data Integration Handbook 2019, 9.)

The most common errors on integrations are (Data Integration Handbook 2019, 11):

- Connectivity issues
- Bad or missing data in the source system causing validation errors in the target system
- A new, untested system update either in the source system or in the target system
- Integration setup failures
- Poorly coordinated service breaks

To get full benefit of the iPaaS platform, it is critical to understand and address the root causes of the current integration issues. Organizations may have data redundancy issues due to immature governance such as unclear data ownership and ineffective problem resolution processes. Governance needs to be addressed upfront to avoid unnecessary integration work. (Gartner 2019b, 16.) It is important to integrate data

quality validation checks throughout the business workflows to ensure long-term data quality. Data integration projects shouldn't go live without a thorough clean-up of data as well as a firm plan to maintain its integrity. (Data Integration Handbook 2019, 8.) This can be proven true in the Company O's P2P integrations, most of the integration errors are occurring due to Master data mismatch between the systems.

3.2 Benefits on integration error monitoring

The most efficient way to control integrations is centralized controlling. This ensures that integrations and data conversions between systems are controlled from one server or work station and this also eases to get the full picture on the information flows. The less there are point-to-point integrations between systems, the easier it is to add more systems or simplify the architecture by changing or upgrading applications. Companies also want to control and monitor their business processes and it is important to business people also to understand how processes work, be able to control and monitor these. (Tähtinen 2005, 66-68.) Abbasi, Chawla & Hussain (2014, 74) also mention that centralized controlling covers whole organization and centralized integrations bring the existing platforms and systems together.

Kozlov (2019) mentions below benefits in IT infrastructure monitoring:

- IT experts gain better insight to potential issues and can make faster and better decisions
- proactive monitoring tools mean that alerts are received before the issue has evolved into a disaster
- early warning signs of upcoming issues
- monitoring can point out areas which need to be prioritized in upgrades and therefore IT budget planning can be enhanced
- less downtime which brings less loss of productivity
- better end-user satisfaction

Calder & Watkins (2012, 19) state that regulations and compliance requirements will increase. They also mention that corporations need to take appropriate information security actions that will drive up the cost and complexity of information security. Directors must be able to identify the steps that they have taken to protect the confidentiality, integrity and availability of the organization's data. The existence of a risk-based information security management policy which is for example implemented into the organization's Incident Management tool, gives evidence that the organization has taken the necessary steps. (Calder & Watkins 2012, 20).

Automated controls should be considered in the system and organization should also consider the need for any supporting controls, manual or automated. The controls implemented should reflect the business value of the information that is being monitored. ISO27002 is suggesting appropriate controls and audit trails should be designed into applications. Application systems are vulnerable to the accidental or intentional input of incorrect or corrupted data and this can lead to system failure, fraud or corruption of existing data. Transaction inputs should be validated and ISO27002 recommends a number of controls depending on the outcome of a risk assessment. (Calder & Watkins 2012, 268-269.)

Good controls create more business value. When IT and business units operate on the basis of a well-defined and well-understood control model, it can make IT more efficient, more productive and even defect free. It establishes process between IT and business and enables leadership to have flexibility within well-defined variables. (Worstell 2013, 120.) An increasing number of companies have started to focus on the implementation of effective controls in their systems while simultaneously providing management and external auditors a suitable framework within which to assess the ERP system's internal controls. (Chang & al. 2014.)

The above sources indicate that the benefits for integration monitoring would be enhanced information security, more efficient way of controlling, increase in business value and better internal controls.

3.3 Case study: Company O's implementation model for integration monitoring

In order to implement integration error messages in Dell Boomi, it would require a project in Company O to go through existing integrations and evaluating whether continuous monitoring is required. A risk assessment should be conducted for integrations to evaluate criticality levels and then implement monitoring messages on those integrations where it's actually needed. Monitoring and integration evaluation model is developed based on internal control theories. Figure 15's process of implementing the integration controls is adapted from COSO's Implementation process which was introduced in chapter 2.6 and figure 10. Implementation of error monitoring can be conducted with the following model to evaluate the integrations, control points and data indicating effective performance.

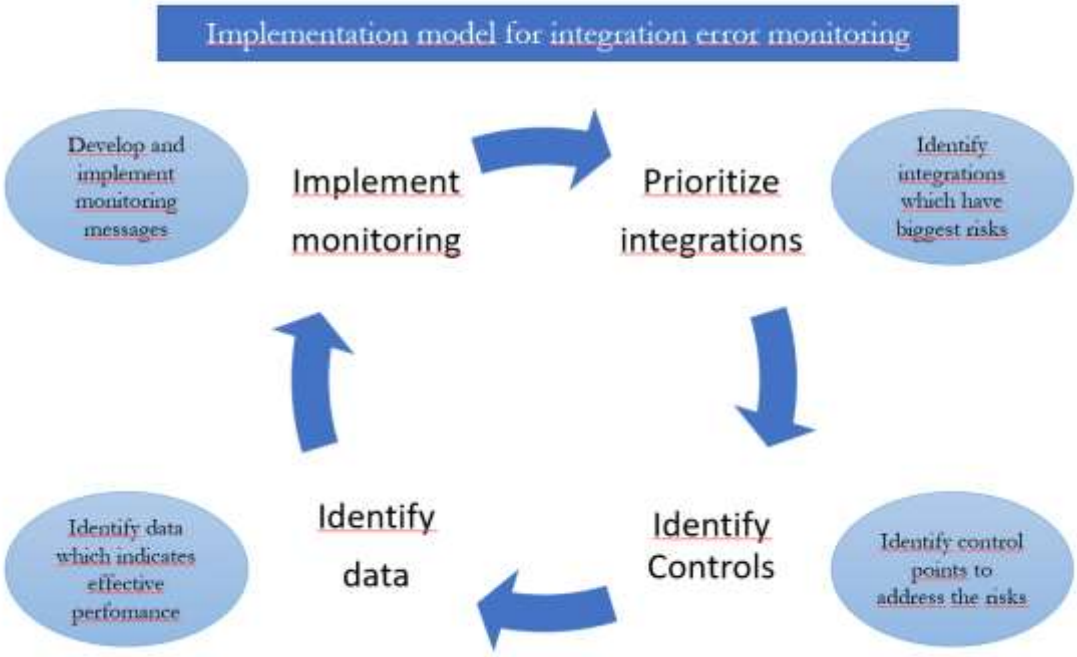


Figure 15. Company O's implementation model for error monitoring. (COSO's process model adapted, Metso 2019)

The process for integration monitoring should be aligned with Company O's IT Management and also with internal audit to ensure management's commitment and support to the model and also to validate that the model fits to Company O's risk assessment model. This model was chosen for the implementation because the company has four-step criticality level evaluation in use for applications and also because COSO model has been suggested in the internal control literature to be combined to other frameworks such as ITIL and Scrum. COSO process model was slightly just adapted to fit to integrations. The steps of the implementation are introduced in the next sub chapters.

3.3.1 Prioritize integrations

The prioritization should be done disregarding the effects of control activities, meaning that the risks should be considered without the presence of the internal control. This way it is guaranteed that the monitoring efforts are directed to those controls that mitigate the most important risks. (COSO 2009, 20.) Company O has already an Application Management Tool (APM) -tool in use so the best solution would be that this tool is used on integration criticality level analysis to enable quick implementation without new tools. This way IT owners could have all the necessary information in one place and there isn't another tool or questionnaire to be filled. The respective application IT Product Owner should do the risk evaluation. APM tool could have the same criticality levels defined as

the application and if the integration has criticality level High or Critical, the monitoring process should be implemented to necessary control points.

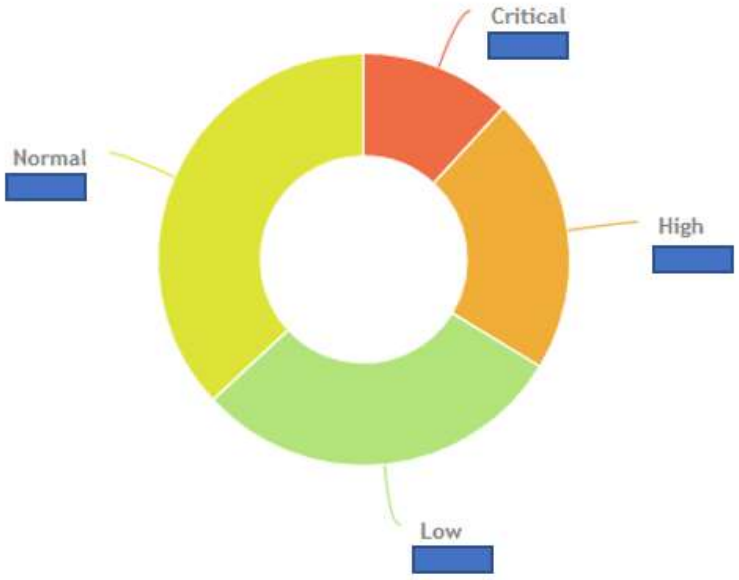


Figure 16. Company O Application Criticality levels (Metso 2019)

Company O is using four-step criticality assessment on the applications as illustrated in figure 16. The figure is showing current split between different application criticality levels. The highest criticality level is Critical which is given to applications which have a serious impact on the company revenue and/or operations. The other criticality levels are High, Normal and Low. Currently the criticality evaluation is done by IT Service Management, the assessment is illustrated in appendix 1. Since the applications are evaluated with these categories, it is suggested to be used also on integrations so that the levels are the same. Figure 17 is a sample application integration information from APM and it could have an extra box for Monitoring as well.

Integrations

	Direction	Application	Type	Criticality	Description
Test system	Receives	System 1	Sche	Critical	
Test system	Delivers	System 2	Sche	Normal	
Test system					

Figure 17. Company O's APM tool Integration information and criticality levels (Metso 2019)

APM tool could even have an alert or notification message if integration has criticality level High or Critical and state to the IT Owner: "Integration monitoring process needs to be implemented". This notification would be sent until the "Monitoring" box is ticked. On Integrations there would be added additional information regarding the criticality levels and the

risk analysis evaluations evaluation. Questions shown in figure 18 are adapted from four-step model that was introduced in chapter 2.6, risk question matrix is also as appendix 2.

Target risks		
LEVEL	**Description**	**Present level**
2	Integration error target is only the system itself or scheduled	
1	Integration error target is the system itself or its scheduled tasks and other internal or external system.	
0	Integration error impacts several systems and scheduled jobs.	

Probability risks		
LEVEL	**Description**	**Present level**
2	Integration error happens once in six months or once a year/very seldomly.	
1	Integration error occurs at least monthly.	
0	Integration error can occur weekly or even daily.	

Severeness risks		
LEVEL	**Description**	**Present level**
2	Integration error doesn't have impact to company's revenue or operations.	
1	Integration error can have an impact to company's revenue or operations OR the actual impact is not known.	
0	Integration error has severe impact to company's revenue and/or operations.	

Consequence risks		
LEVEL	**Description**	**Present level**
2	Integration error doesn't have impact to business continuity or other business processes. Estimate also how long business can tolarate if integration doesn't work: less than 1 day or more.	
1	Integration error can have an impact to business continuity or other business processes. Estimate also how long business can tolarate if integration doesn't work: less than >=5 hours.	
0	Integration error has a severe impact to business continuity and processes and effects operations. Estimate also how long business can tolarate if integration doesn't work: <=5 hours	

Figure 18. Risk evaluation questionnaire for Company O APM tool (Metso, 2019)

If risk analysis gives a result of 50 or more, there should be monitoring implemented to the middleware or to the sending/receiving system, see figure 19 showing risk level. It is not currently possible to obtain reports of integrations from the APM tool but it should be possible to improve this functionality and then the integrations could be prioritized with a report which would have monitoring implemented first.

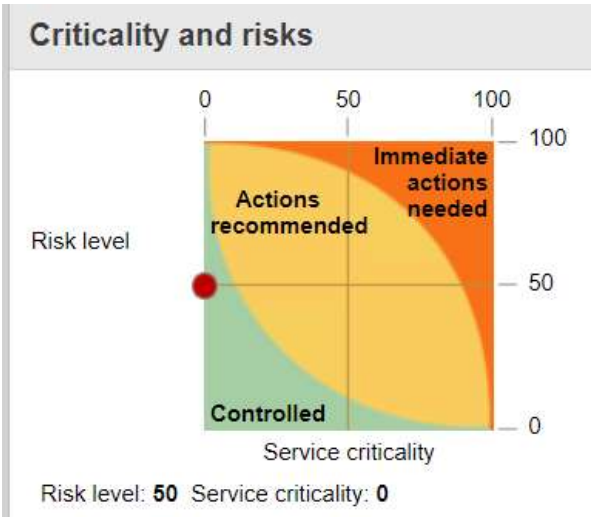


Figure 19. Company O APM tool Integration criticality level matrix

Since the integrations risk analysis questionnaire is not in the system yet, it is suggested that the application criticality level is used to prioritize integrations at first stage. There should be a project manager assigned to this project so that the monitoring would be implemented in an organized way and documented as well.

3.3.2 Identify Controls

In order to execute effective monitoring there needs to build an understanding of how the control system is designed to work and how the failure of the system will affect the organization's objectives if not detected on time. Therefore, the identification of the key controls needs to succeed the risk assessment with the target to identify the controls that best support the management conclusions of the control efficiency. This does not mean that some controls would be considered as less important than others, but the focus is to find the most meaningful controls to be exposed for monitoring. (COSO 2009, 22.)

As the second step it is important to identify the control points in monitoring. This step is heavily linked also to the first step when the integrations would be prioritized, then it would be worthwhile to check also the necessary controls per integration. The purpose of integration solution is to effectively govern the solution. It is important to understand the units and processes from which the integration is built from. (Tähtinen 2005, 59.) Control point identifying will be done so that there will be centralized monitoring solution in place. Dell Boomi will be used as a sample in this thesis to illustrate control points, sample document in figure 20.

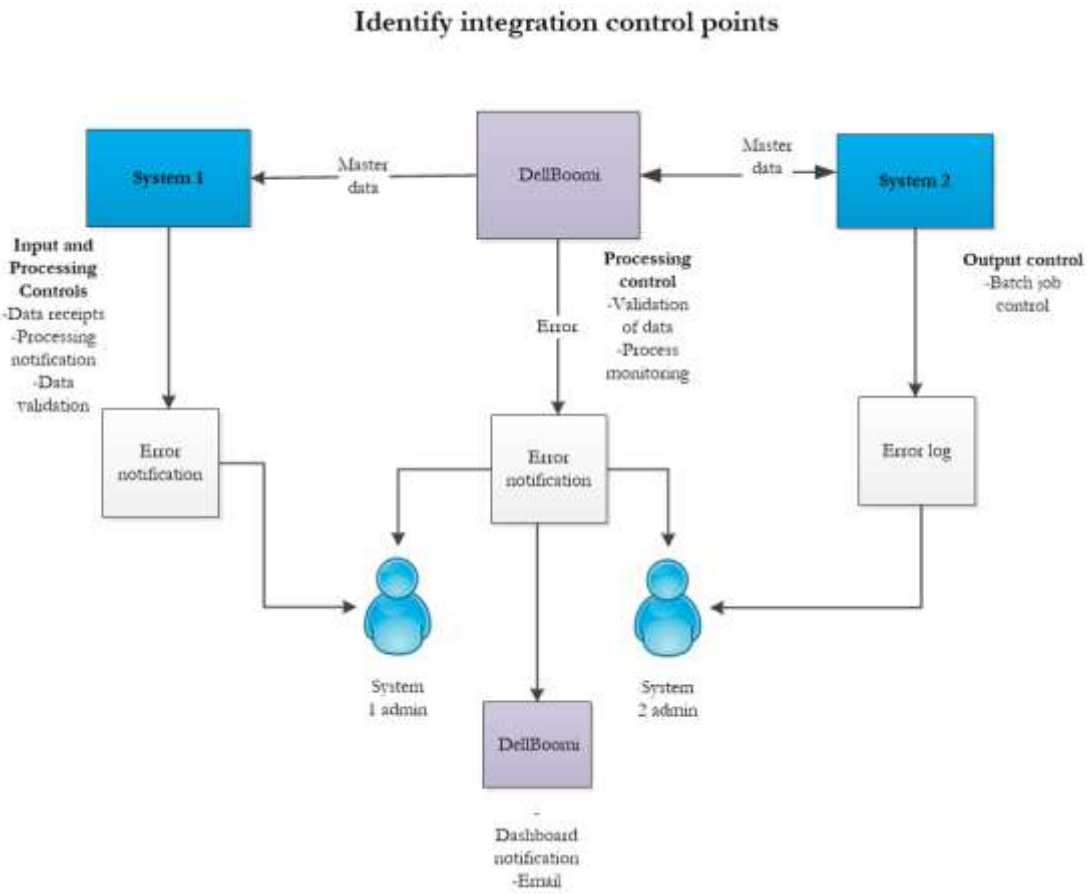


Figure 20. Identifying integration control points. (Metso 2019)

When identifying the control points, the nature and criticality of the data plays an important part. And also the business process where the data relates to and what is the impact if the data transfer fails. Thesis therefore suggests that the control points are in the sending and in receiving system and also in the Dell Boomi platform. According to COSO model illustrated in figure 10, it is important to identify the risks which relate to the processes and communicate it to stakeholders. Also it is important to have adequate controls and monitoring to avoid ineffective processes (Moeller 2013, 65.) It has also been identified in P2P integration errors that quick and comprehensive communication of processing and validation errors have resulted also quick corrections, the errors are noticed within minutes instead of days. Especially Master data errors have impact on end user experience if an invoice has to be handled more than once due to incorrect Master data in the system.

3.3.3 Identify data

The third step in the monitoring design process is related to the quality of the data used in monitoring. COSO clarifies the concept of persuasive information, which should be brought out by the monitoring procedures. The persuasive information is something that is

both suitable and sufficient in order to give adequate support for making the management conclusions of the effectiveness of the control system. The suitable information is explained by three more concepts: relevance, reliability and timeliness. The relevance of the information gathered through monitoring can be judged by how closely the information connected to the control in question. (COSO 2009, 27.)

The third step in the implementation process would be made so that the nature of data needs to be analysed with the respective IT application owner. If for example there are ten integrations of Master data from System 1 to System 2, all of this data is not necessarily critical and necessary to monitor 24/7. Dell Boomi team doesn't know what data needs to be controlled or how so this step is crucial to go through with the correct stakeholders and analyse the data which indicates the integration is performing correctly. The identification of data would need to answer questions to data relevance, how reliable is the data and timeliness of the data.

Thesis suggests that in this step the integration Criticality level is considered as well. If integration criticality is Critical or High, the data should be considered to have monitoring. In order to build and develop monitoring of the integration, there should be good knowledge of the system design, identify these controls, test those controls and the develop necessary control on the data. COSO internal controls also highlight the importance of control documentation. (Moeller 2013, 175.) The final decision of the monitoring would be made by the IT Application Owner and architecture design would be done with the help of IT architect to illustrate and document the monitoring. Figure 20 is illustrating a sample architecture document with minimum information, in addition to this there would be an Excel documentation of the interfaces with risk evaluation, control points, data which is controlled and what is indicating that the data is in error.

3.3.4 Implement monitoring

The monitoring procedures may be executed through ongoing monitoring or separate evaluations. The advantage of the ongoing monitoring is that it is often implemented in real time, thus providing information by which the control deficiencies may be identified and corrected at early stage. (COSO 2009, 38.) In the last step the agreed monitoring model would be implemented with the Dell Boomi Product Owner, development team and with the relevant application's IT owner. Company O has Agile way of working in use so implementation would be done according to the Scrum framework. That means that imple-

mentation would be done in Sprints. All go-lives would follow Company O's Project methodology and necessary approvals would need to be obtained as with other projects. Risks are minimal in the go-lives since the monitoring is mitigating business risks.

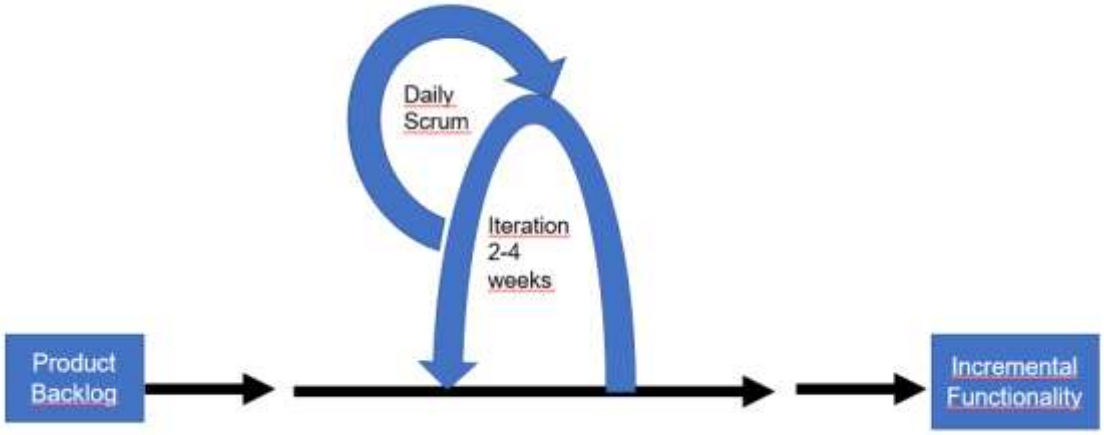


Figure 21. Skeleton and Heart of Scrum (Digital Media Hunt 2019, adapted)

Figure 21 is illustrating the skeleton of Srum and the implementation process. The Scrum process is adapted to fit into integrations. At the start of an iteration, the development team reviews what it must do during the sprint. It then selects an integration process which can be provided as an Increment of functionality by the end of the iteration. The heart of the process is the iteration. The team takes a look at the requirements, considers the available technology, and evaluates the best way to monitor the integration most efficiently and what is best fit for it. Development team collectively determines how to build the functionality and keeps Daily Scrum meetings to modify approach as there can be new complexities, difficulties, and surprises. The team figures out what needs to be done and selects the best way to do it. At the end of the iteration, the team presents the increment of functionality it built so that the stakeholders can check the integration functionality and timely adaptations to the project can be made. Scrum is a creative method for development and its enables also productivity. (Digital Media Hunt 2019.)

Implementation phase can be adjusted so that it fits to the team and the integration. The roles for the Scrum Development team will need to be clearly defined so that there is Dell Boomi Product Owner (PO), Scrum Master and the necessary Dell Boomi developers participating the Daily Scrums. Project Manager will be kept updated by the Dell Boomi PO. Dell Boomi PO would also maintain the product backlog so that the highest priority integrations would be implemented first. Sprint Backlog would have to be adjusted if there would be new applications coming, usually implementation projects have tight schedules.

There would be a risk board and sticky notes in the Scrum board indicating the risk level of the integration. Ylimannela's (2011, 2-4) model had only two risk categories so this would be adjusted to fit into the four-level risk categorization at Company O. The sticky notes would illustrate the risk level and the risk owner. The risk level owner would be the sending system IT Application Owner. Sticky notes samples are illustrated in figure 22.

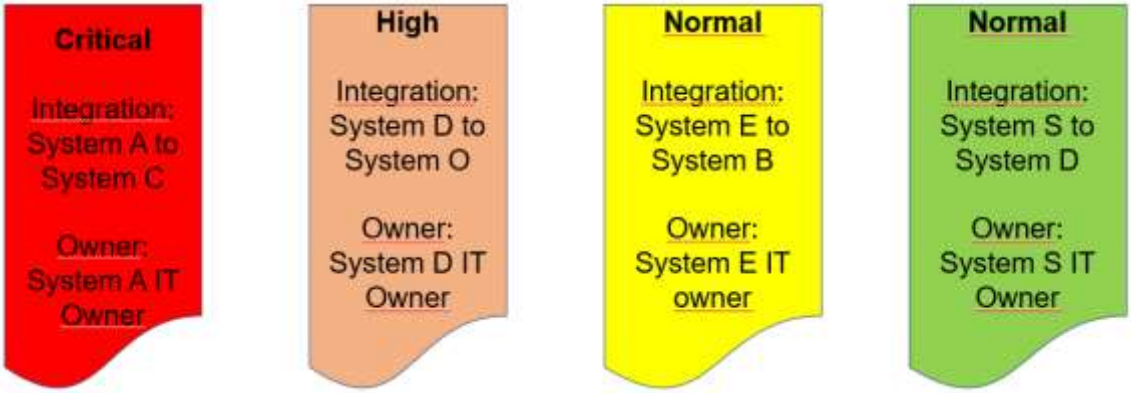


Figure 22. Integration risk level sticky notes in Scrum board (Ylimannela 2011, 2 adapted)

Risk communication between Scrum team is important. The Scrum master and Product Owner should handle communication between the Scrum team and business decision makers. One of the key principles in Scrum is that the scrum master should handle problems and communication with people who aren't part of the team. Security risks which are often technical shouldn't really be part of business decision makers risk management activities, except in a case where a large security risk could affect long-term business decisions. (Ahola & al. 2014, 42.) Communication would be kept open within the Development Team and Company O's usual channels would be used to broadcast Sprint Backlog, meeting notes, risk board, risk register roadmaps, technical documentation and other relevant documents. Since implementation would be executed also in Project mode, the communication would be done also to the Company O's IT Management team about the progress, targets and go-lives. Project would be followed up as well in IT info sessions.

Once integration error monitoring implementation for Critical and High applications would be finished, the Development team would continue the work as Business as Usual and Daily Scrum would be evaluated if those are continued.

3.4 How to improve further the integration monitoring

When interviewing Dell Boomi developer it was evident that the current way of integration monitoring is not working as efficiently as it could (Dell Boomi developer 31st Aug and 21st Oct). Most important reason is identified to be the lack of knowledge of iPaaS platform

and Dell Boomi's capabilities in the Company O's organization and the second is missing ownership of the platform. Active monitoring of integrations is currently in use for appr. 25 processes and there are over 500 integration processes in Dell Boomi. The error messages for P2P integrations is now done via email and this communication method could also be improved. Thesis lists few improvement ideas for both integration monitoring and also how to grow the awareness of Dell Boomi within Company O. Improvement ideas have been gathered from literature reviews, scientific articles, interviews and with observation.

3.4.1 Enhanced responsibility and communication

Firstly there should be an IT Product Owner for the Dell Boomi platform who drives the vision of integration architecture within the company. Secondly there should be info sessions arranged of the Dell Boomi capabilities across the organization in different kind of info sessions. Communication is an important part of COSO's internal control framework. It is not a horizontal layer but a component that is almost like a bridge across all other components. Appropriate information must be communicated up and down in a manner and due course that allows people to carry out their responsibilities. There should also be a good understanding of the information and communication flows or processes in the organization. (Moeller 2013, 168.) In an outsourced or cloud-based environment, it is essential that a clear definition of roles and responsibilities are identified (Worstell 2013, 53). There could be a survey conducted in Company O about the Dell Boomi platform to get the present state and awareness clarified. This would have to be conducted on a detailed level asking awareness about iPaaS capabilities such as JIRA ticketing, SMS possibility and so on.

As part of efficient communication, it is important to align the data transfer schedules between the systems and on system breaks. Sometimes system outage has been scheduled at a time when currency exchange rates are transferred to the system and this is noticed next day when the damage has already happened. Technical errors can be avoided by scheduling a fixed time for a service break per system, time can be agreed both with business, data integration staff and application support teams. Proper communication to all stakeholders of the service break is also a vital aspect in well-planned service breaks. Dell Boomi team should also be involved in the service break notifications. Dell Boomi should also have a process in place to re-send messages again to ERP system if there's a connectivity error. This process of course needs to be agreed beforehand.

Both sending and receiving systems should have error messages triggered on failed integrations either in system transfer or run logs or via e-mail to administrators. Error monitoring emails should contain a direct link to the error in the inbound or outbound system if possible to ensure quicker error fixing. E-mail error messaging is very quick way to inform different stakeholders of the issue but it is important that it contains the error message and all possible information available of the error. There can also be a direct link to the error, for example the link to the invoice in the P2P system. This kind of link is currently missing from the error e-mails and it can be easily added, see figure 23.

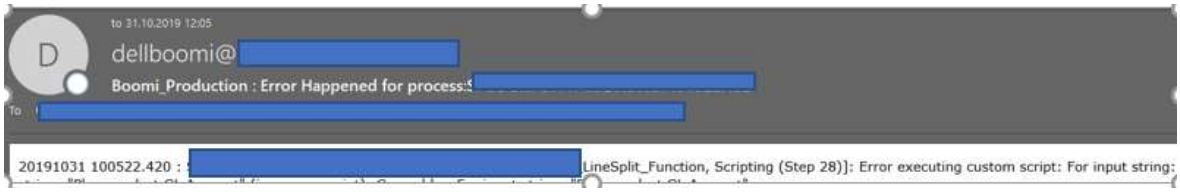


Figure 23: Dell Boomi sample error e-mail (Dell Boomi 31st Oct 2019)

3.4.2 More automation

Dell Boomi could make a connection with HTTP client to Company O's incident management tool on critical error types and a problem ticket gets created automatically to correct party. Many integration errors and other topics are handled via e-mail and this takes much time from actual development work which could be avoided via tickets. Integration into for example JIRA can be done also via API which would be a modern way of integration, there is specific Informatica® Cloud JIRA Connector that can be used. If tickets would be opened automatically it could reduce the number of the incident tickets created by the end users or by Dell Boomi team. (Dell Boomi developer 21st Oct 2019 & Boomi 2019.)

Dell Boomi developer (21st Oct 2019) also mentioned that tickets would help also the team's monitoring how many issues they are working on a daily basis. Automated ticket creation therefore enhances communication and quicker problem resolution enhance end user experience since it's possible that the system end user doesn't even notice failure in some cases. This kind of improvement could then enhance also end user satisfaction. IT owners could also follow Service Level Agreement (SLAs) of the integration errors as there would be tickets open of Critical and High errors. IT must be able to measure uptime, performance, and response time of business critical applications and the infrastructure they run on.

RPA brings more automation potential on integrations as well. RPA often offers a more inexpensive and quicker solution to the same problem that an integration aims to solve. RPA's competitive advantage comes from the solution's light structure, that allows implementing the technology without changes to the organizations existing IT systems. A software robot can be taught a simple process in just a few days, which means that also the impact of the technology is quickly realized. On the other hand, the same technology can be configured for new purposes as the needs of the organization change (Luukka 2019). In Gartner's (2018) report it was stated that global spending on RPA software reached $680 million in 2018, an increase of 57 percent year over year. Gartner's Senior Research Director has said (Gartner 2019d) that organizations are adopting RPA when there are a lot of manual data integration tasks between applications and are looking for cost-effective integration methods.

According to Atlassian (2019), there's over 200 apps and web services to sync alert data and streamline workflows. Few samples of these apps are Jira, ServiceNow, slack, Microsoft Teams, HipChat and Amazon CloudWatch (Atlassian 2019). In Dell Boomi there are also several HTTP clients available but those are not used to full potential. The same case concerns also database connectors. There are un-used capabilities in Dell Boomi that could be harnessed to integrations. The Dell Boomi developer doesn't necessarily suggest the use of these capabilities because some of them can require a lot of work and perhaps the developers haven't done it before. (Dell Boomi developer 21st Oct 2019.)

An interesting capability in Dell Boomi is also that it can send an SMS messages, this could be used in fatal and critical integration errors. Or Dell Boomi can send a message to slack, Teams or chat bots on certain integration errors with HTTP client based REST call or with an existing connector (Boomi 2019 & Dell Boomi Developer 21st Oct 2019). This makes real-time reaction to integration errors possible and very quick communication to stakeholders across the organization.

Further topics on automation are automated integration testing, Artificial Intelligence, Machine learning, IoT possibilities, Event-Driven data flow also known as Microservices architecture, Service-Oriented-Architecture (SOA), Interoperability... There's a lot happening in the technology side and these should be investigated further what would be possible to do in Company O's platform and for integration management. The business world requires not just integration but integration at level of the organization. Part of the applications and programs have evolved and commercialized at many individual level but a more centralized approach is needed to cover up whole organization. (Abbasi & al. 2014, 74.)

3.4.3 Master data management

The concept of Master Data Management (MDM) is a complex and dynamic due to the segmentation of data across the business functions. The cross-functional roles and responsibilities, particularly in relation to data steward functions, needs to be clearly defined. MDM is about people, process, and technology. The proper combination of these three elements is what makes MDM successful. MDM is constantly fine-tuning these elements for maximum benefits. Figure 24 represents people, process and technology and MDM as a pair of gears. As one is adjusted, the other is impacted. (Cervo & Allen 2011.) Data governance is becoming vital to handling changes (Gartner 2019b, 18).

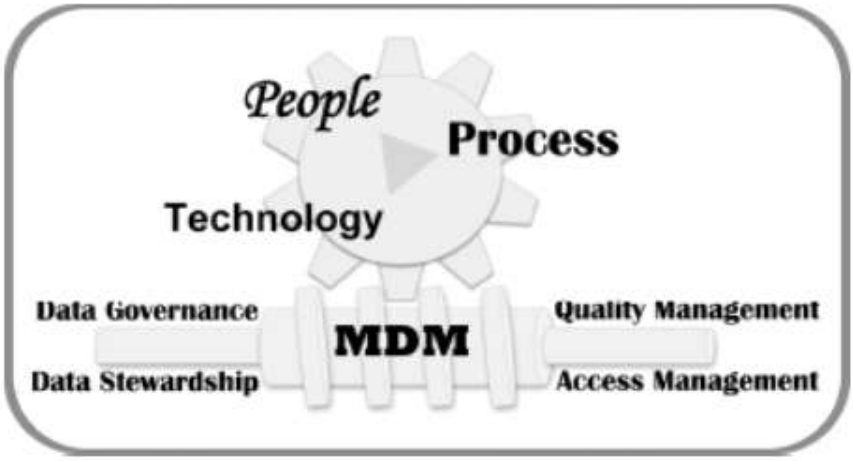


Figure 24. Reliance between MDM and People, Process, and Technology (Cervo & Allen 2011)

The first step should be to profile the data and identify what needs to be migrated. Cervo & Allen (2011) suggest that in data migrations the data should be classified with four categories:

A. Data to be migrated
B. Data to be cleansed
C. Data to be consolidated
D. Data to be cleansed and consolidated

It is important to have a clear understanding of the data elements to be converted as well as the type of transformation required to convert them. It may be necessary to break down the classification even further. (Cervo & Allen 2011.)

Gartner (2019b, 18) mentions few good practices for data governance:

- certify data quality of individual data sources to encourage more usage of quality data and accountability of data ownership
- proactively manage technical metadata and the shared business glossary

- refresh your MDM program and architecture to leverage more SaaS and external data
- identify key data governance areas with Big data to prioritize compliance, risk, business value and reusability

Many organizations have realized that segregation of data and application integration leads to escalating costs due to overlapping effort, redundant tooling and conflicting approaches. (Gartner 2019b, 18). Data governance policies and standards need to be well documented, communicated and enforced. P2P application error monitoring indicates that majority of errors are due to incorrect Master data between the systems. Dell Boomi developer confirms that Master data errors occur frequently in the integrations but usually the error is noticed in either sending or in receiving system (Dell Boomi developer 31st Aug 2019).

Thesis suggests better ownership to the Master data across whole organization and a separate cleanup project and data validation checks for the systems. Also architecture diagram should also be more up-to-date according to Master data and the data transfer schedules. The Master data is scattered in several systems so the governance will be difficult in the future as well.

3.4.4 Other improvement suggestions

There are few SAP based applications in Company O's IT landscape and along with the package there's also separate module called Solution Manager (Solman). There are possibilities to utilize the Solman more, it is possible to monitor the business process performance related to the SAP workflows, background jobs and overall system performance as well as have better control over changes and recurring incidents.

There are also available some monitoring solutions which provide more sophisticated tools for holistic monitoring, such as splunk. These kind of monitoring tools use predictive algorithms, advance analytics and Machine Learning to quickly notice and even prevent incidents and system failures (splunk 2019). There are also tools which monitor servers and the whole network, such as Datadog, LogicMonitor, ManageEngine OpManager, Passler PRTG and others. Server monitoring tools are the best way for enterprises to ensure that their servers, both physical and virtual, are operational and functioning at a manageable level. (Hein 2019.)

New monitoring tools will perhaps improve the reporting and monitoring process but those are also adding complexity to architecture and costs as well when a new tool needs to be

implemented. iPaaS vendors are already providing features powered by AI or Machine Learning techniques. This trend will continue as each iPaaS vendor finds new ways to leverage the knowledge base of iPaaS pipelines created by their customers. AI can be used to detect patterns and best practices among the solutions created by their customers. (Gartner 2019a, 16.) This would be a centralized solution since in Company O Dell Boomi has already connectivity to several systems and servers.

Also lot can be achieved by first optimizing the processes. Optimizing the process should always be the first step regardless of the fact will it be eventually automated or outsourced. It is a balancing act between the effort required to improve a process and the value that it will bring to the organization, prioritization activity needs to take place whether benefit is worth the cost. (Rutaganda, Bergstrom, Jayashekhar, Jayasinghe & Ahmed 2017, 40.) Business process improvement should also be done continuously along with the integration work. It has turned out in several projects in Company O that some integration is not needed anymore, the other system has been sunset or business is handling the work in another way like with RPA. But this information hasn't been updated into integration documents or blueprints so those are out of date.

3.5 Summary of empirical chapter

In the empirical chapter the researcher has provided answers to the research questions and to the original research problem about integration errors. There's also presented the possible implementation model how the integration error monitoring could be further integrated into Dell Boomi processes and in the Company O's organization.

The P2P error emails were analyzed in the beginning of this chapter. It was identified that there are several errors related to Master data and data validation. From these findings and from literature there are improvement suggestions listed in the empirical chapter. The P2P error messages were analyzed and categorized because the Dell Boomi reports were only available for 35 days and recent reports haven't been stored by anyone in the organization. As in the P2P integrations there are over 3500 error messages generated from nineteen integrations in four months, it indicates that there must be several errors on a daily basis for other integrations too. Therefore there is a justification for an improvement in the integration error monitoring but this would have to be further investigated with the Dell Boomi team to understand the magnitude of error count and then go forward with improvements and implementation. It was not possible for the researcher to obtain data for

the all integrations in Dell Boomi so this leaves room for further study inside the organization. Platform that would work for all the different data systems and getting the processes and transactions aligned is vital to the organization (Abbasi & al. 2015, 76.)

The implementation model in chapter 3.3 is a hybrid model adapted from COSO's Implementation process and from Ylimannela's (2011 2-5) Risk Management on Agile development model. The created model is practical and simple enough to enable integration error monitoring in an Agile way and Company O's existing tools and applications can be used. The model also considers the internal control and risk management which was a requirement for the implementation model. Since a suitable model was able to be provided by the thesis, all the needed requirements were fulfilled in this research. The implementation model has not been tested in the organization nor has the COSO model been discussed with Company O's Management or internal audit so these would be the first steps before implementation could be taken forward.

Although fast and cheap solutions are often desirable, it might be worth spending some additional money to know that if something breaks, you're notified immediately and that there is a backup system already running (Luukka 2019).

4 Discussion

The goal of the thesis was to investigate the errors on P2P integrations and based on this analysis, literature review and other research findings to suggest improvement actions for integration error monitoring. The purpose of the thesis was also to introduce an implementation process model for integration error monitoring for Company O and find benefits of error monitoring.

The purpose of the thesis was to answer the following research questions:

- What kind of integration errors there has been in P2P -integrations?
- How the error monitoring process could be improved?
- What kind of implementation model there could be for integration monitoring?
- What benefits integration error monitoring brings to the organization?

When discussing the thesis subject in Company O, it was found out that the integration monitoring is very low level in the organization and there isn't any risk evaluation as such done in Dell Boomi for integrations. Furthermore, the integration risk levels are not maintained in the Company O's Application Management tool. Researcher had open discussion with several IT Application owners and Digital team about Dell Boomi platform and it turned out that is not very widely known in the organization nor are its capabilities. Therefore the thesis subject was identified to be the integration error monitoring, further improvement suggestions and also developing an implementation process for integration monitoring.

When the thesis subject was chosen it was not crystal clear that the theory would be based largely on internal and application controls. When doing the theoretical framework studies, internal control theories provided a lot of answers and arguments why it is good to improve and develop more the current way of integration monitoring. According to internal control theories and recent research, the internal control system of an organization is a highly related process with implications to the organizations culture, business environment, operations and structure (eg. COSO 2009, Moeller 2013).

4.1 Consideration of results

During the thesis work it was discovered that the Dell Boomi dashboard is containing integration error monitoring data basically only for one day. And the csv reports from Dell are

only for the last 35 days. Due to these reasons it was not possible to obtain reliable data from Dell Boomi how often there really occurs integration errors in other processes than P2P integrations. This was a setback for the research, the data gathering and grounds for the development of integration error monitoring were not thoroughly possible to obtain. But since researcher has been observing integration errors for many years for all the Finance applications in Company O, it is evident that that those happen very frequently and further improvement is justified. Dell Boomi developer interviews confirmed researcher's observation. Several researcher's IT colleagues in Company O stated that they have the same situation and a lot of time is spent on the integration error fixing either in IT, business or by external vendors.

Due to this data collection limitation, the case study is now mostly about how to implement the integration error monitoring and it lists also improvement suggestions for further development. Luckily P2P system integration error monitoring has been live for over five months so those results were able to be used to demonstrate most common integration error types. The improvement suggestions are not based solely on these findings but are general development ideas and future trends for integration error monitoring gathered from literature, scientific reviews, interviews and with observation. At least for P2P integration errors the results of these five months have been giving a lot of information how the integration error monitoring messages could enable quick error fixing and enhanced communication. Some errors have been fixed so that it doesn't happen again, so the messages have also improved root-cause analysis and problem solving. Several data collection methods were used on improvement suggestions and considered with analytical mindset so researcher considers these to be reliable results.

First research question was about the P2P integration errors and the answers to different error types were provided in the research by using statistical methods for data analysis. Although the improvement suggestions are not solely based on this data, nevertheless it was useful background data to investigate what kind of errors there has been in the recently activated error messages. There was data available for five months, from June to October 2019, which is quite comprehensive time to follow up on the errors. The purpose of the analysis was to find whether the integration errors listed in theory matched the ones in the P2P integration errors and also to find some improvement ideas at least for P2P integration errors. The collected data surprised the researcher since there were so many error messages every day especially on Master data and the count of email has increased, this raised questions is anyone checking the errors on a daily basis? This is something with special interest to the researcher and it will be discussed within the P2P development

team that who are responsible to check the error messages and what action has been taken to fix these errors from happening again.

The second research question was about the improvement suggestions. The results to this question was provided with the analysis of P2P error messages, literature and scientific articles and with observation. There was a wide range of data collected to showcase improvement suggestions which enhances the credibility. Improvement suggestions are not collected from the researcher's own opinions but from different data sources and supported by literature and with future trends on integrations. Thesis was able to find few suggestions that can be investigated further in Company O and in other organizations as well who are using iPaaS platforms. A lot of new technology is available, it is subject to the relevant organization to find the best and efficient ways to improvement integration monitoring.

The third research question was about the implementation model and this was the essence of the case study. During the research process there wasn't articles or other studies found how to actually implement internal controls or monitoring. Internal control theories didn't have much help on this either. Although a lot of time was spent on literature review and scientific articles, researcher suspects that integration monitoring is not a widely researched subject when it comes to iPaaS platforms. However the selected implementation process from COSO was largely supported by the literature, particularly the COSO Monitoring Guidance, and it contains the necessary steps that were required for risk evaluation as well. The implementation process is simple, can use existing tools and can be implemented with Scrum. Therefore the third research question was answered although the support from literature and scientific articles was rather weak.

The implementation process wasn't tested during the thesis so it can be considered as an option for Company O whether integration error monitoring will be implemented. The thesis empirical part is based on internal control theories and other data collection methods were used also to get the process credible and reliable. The implementation process is adapted from COSO's monitoring and process model and it has been adapted to fit into integrations and to Company O's architecture and IT frameworks. This model adapted by the researcher is general and can be used in other organizations as well if it fits their internal control policies and practices. Most of the organizations have an Application Management tool in use and are also using Agile development methods so in this perspective the model can fit to other organizations as well.

Fourth research question was about the benefits of integration monitoring. Answers to this research questions were collected from literature, scientific articles and with observation. Literature provided necessary information on this subject and the benefits were possible to be linked into the P2P integration error messages. And thesis also found the benefits for centralized monitoring which indicates that it is beneficial to do monitoring in Dell Boomi or in another centralized platform. The answers to this research question helped also in finding answers to research question on improvement suggestions. The answers on integration error monitoring benefits are general and can provide assistance to other organizations or studies as well.

Although case studies have been discussed extensively in the literature, little has been written about the specific steps one may use to conduct case study research effectively. There is a lot of theory and different frameworks available especially on internal controls but very little has been written about how to actually implement and adjust these so that it fits to the organization. Scientific articles stated the same and also that one framework is not usually enough for the organization, but a good solution is a combination of several frameworks and best practices. This information strengthened the researcher's vision not to use another complex framework in the implementation process but to combine it to fit into Company O's culture and ensure that Agile way is used in the implementation. Researcher has been careful that the thesis results are not biased with personal judgements or opinions and tried to base the findings, suggestions and new implementation model with several data collection methods. But of course the risk of personal opinions is possible.

As a conclusion of the thesis is that the research questions were answered with the theory and other data collection methods and also an implementation process model was created in case study based on the research data. The variety of data collection methods makes the thesis credible and the new implementation model reliable, the results can be used in Company O and also in other organizations as well. Thesis nevertheless emphasizes the importance that the integration errors need to be investigated more in Company O in order to analyze whether it is worthwhile to implement monitoring e-mails further in the organization and also evaluate that Dell Boomi platform has necessary memory, resources and other necessary tools available. The implementation process model is simple enough to enable quick results and it could bring enhancement to the integration error monitoring which is currently not done efficiently.

The biggest dilemma that the businesses today face is the ever increasing demand and expectation from the consumers. This has in turn led business to rely more and more on

the IT industry to develop advanced support tools that would help companies respond to the change. The IT industry on the other hand is constantly evolving based on the foundation of technology and applications established. Centralized integrations bring the existing platforms and systems together. (Abbasi & al, 2019, 76.)

4.2 Further development work

Would be beneficial to research the integration errors so that there is enough and valid data available how much of the integrations are in error on a daily or monthly basis. Data should be gathered at least for six months or more for thorough analysis and then really focus in the organization to the actual problems and how to improve the situation. This kind of research could be conducted in any of the iPaaS platforms or middleware used in other companies than in Company O.

It could also be a subject to research how the implementation model created in this thesis actually works in practice and follow results before and after the implementation. There should be start and end state analysed before and after the research to validate have the integration monitoring been successful and has the monitoring process improved the situation in the respective organization.

Another important research topic could be the iPaaS platforms technical capabilities and how to improve and automate different processes with the help of AI, RPA or with Machine Learning. iPaaS platforms are still relatively new in Finland and there wasn't a single thesis in Theseus on that topic at least with the ones that are available for public search. The Cloud platforms and Cloud computing are already here so would be a good thesis topic to investigate those topics further.

For further study it would be also interesting to benchmark with other companies that are using iPaaS platforms, how the integration monitoring has been arranged. And also how internal controls have been successfully implemented in an organization. There was a lack of evidence around this are in the academic literature and therefore the topics related to different kind of monitoring procedures, internal controls KPI's, possible negative effects and such would be beneficial to other researchers as well to understand the phenomenon more thoroughly.

4.3 Evaluation of researcher's own learning

Researcher learnt that it is vital to do more thorough preliminary research how much literature and scientific articles there are available on the thesis topic. It was an unfortunate setback that the Dell Boomi dashboard details were only available for one day and nobody has stored the logs or reports of the integration errors. Researcher also underestimated how much time it takes to find the suitable theory and scientific articles which actually fit to the thesis subject. There are also always surprises along the way and that should have been estimated better in the thesis timeline.

The best decision along the process was to apply for a three months study leave from work. Since researcher had studied 3,5 years along with working full-time, the strengths were scarce and it was time to take a break and only focus on the thesis and the writing. Good planning of the timeline helped a lot along the process.

The thesis subject was especially interesting and motivated to write the thesis every day. In addition to different internal control theories and risk management, a lot was learnt on integrations, Dell Boomi and other iPaaS platforms capabilities and about future trends on integration monitoring. During the process analytical mindset developed as well, it is good to be cautious on which sources to use. Time is an essence and be always ready for surprises.

References

Abbasi E., Chawla, U.B.D & Hussain, L. Trends and Future for Enterprise Integration. International Journal of Innovation, Management and Technology, Vol. 6, No. 1, February 2015. http://www.ijimt.org/vol6/577-IS005.pdf [Accessed 7th Nov 2019]

Agrawal, R., Singh, D. & Sharma, A. 2016. Prioritizing and optimizing risk factors in agile software development.

Agile Alliance https://www.agilealliance.org/agile101/ [Accessed 7th Nov 2019]

Agile Manifesto https://agilemanifesto.org/principles.html [Accessed 7th Nov 2019]

Ahola, J., Frühwirth, C., Helenius, M., Kutvonen, L., Myllylahti J., Nyberg, T.,Pietikäinen, A., Pietikäinen, P., Röning, J., Ruohomaa, S., Särs, C., Siiskonen, T., Vähä-Sipilä & A., Ylimannela V. 2014. Handbook of the Secure Agile Software Development Life Cycle. University of Oulu. Juvenes Print. http://www.n4s.fi/2014magazine/article2/assets/guide-book_handbook.pdf [Accessed 7th Nov 2019]

Atlassian, OpsGenie integrations https://www.atlassian.com/software/opsgenie/integrations?&categories=featured [Accessed 11th Oct 2019]

Bamberger, J. 2006. Sound IT Governance Requires Breadth & Depth. Financial Executive, 22(2), pp. 54-56. https://search-proquest-com.ezproxy.haaga-helia.fi/docview/208882444/fulltextPDF/931547C164B747E7PQ/1?accountid=27436 [Accessed 31st Oct 2019]

Baxter, P., & Jack, S. 2008. Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), 544-559. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1573&context=tqr [Accessed 7th Nov 2019]

Boomi 2019. https://boomi.com/?utm_source=google&utm_medium=cpc&utm_content=dell%20boomi%20-%20exact&utm_campaign=G_Brand_EU_Search&src=web&gclid=CjwKCAjwtuLrBRAlEiwAPVcZB-prDCScx_LA3CIXrU6ktZJzArziesmKJl_82vL5HVm6Vl-q-xRXOMhoCyEIQAvD_BwE [Accessed 30th Sep 2019]

Boomi User Guide: Atoms, Molecules, and Atom Clouds. https://help.boomi.com/bundle/integration/page/int-Atoms_Molecules_and_Atom_Clouds_d8fe8ad8-3ba5-4eb1-967d-cd0fc9ffb062.html [Accessed 5th Oct 2019]

Cervo, D. & Allen, M. 2011. Master Data Management in Practice: Achieving True Customer MDM. Wiley.

Chang, S., Yen, D. C., Chang, I. & Jan, D. 2014. Internal control framework for a compliant ERP system. Information & Management, 51(2). https://www-sciencedirect-com.ezproxy.haaga-helia.fi/science/article/pii/S0378720613001158 [Accessed 24th Oct 2019]

Chorafas, D. N. 2007. Risk Management Technology in Financial Services : Risk Control, Stress Testing, Models, and IT Systems and Structures. Burlington Buttenworth-Heinemann.

COSO (2009) Internal Control – Integrated Framework, Guidance on Monitoring Internal Control Systems.

Data Integration Handbook. https://cdn2.hubspot.net/hubfs/48101/Rapidi%20Live/pdfs/eBooks/Rapidi%20eBook%20-%20Data%20Integration%20Handbook.pdf [Accessed 26th Sep 2019]

Digital Media Hunt 2019. Scrum Theory and Scrum Skeleton. https://digitalmedia-hunt.com/scrum-theory-and-scrum-skeleton/ Accessed 13th Nov 2019.

Gartner, Nov 2018. Gartner Says Worldwide Spending on Robotic Process Automation Software to Reach $680 Million in 2018. ttps://www.gartner.com/en/newsroom/press-releases/2018-11-13-gartner-says-worldwide-spending-on-robotic-process-automation-software-to-reach-680-million-in-2018 [Accessed 7th Nov 2019]

Gartner 2019a. Deploying Effective iPaaS Solutions for Data Integration: https://www.gartner.com/document/3913818?ref=solrAll&refval=228752241&qid=c5eb17bd74de58cf1d7 [Accessed 19th Sep 2019]

Gartner 2019b. Comparing Four iPaaS-Based Architectures for Data and App Integration in Public Cloud:

https://www.gartner.com/document/3226917?ref=solrAll&refval=228752349&qid=e47a30c888ae19d4b889c309 [Accessed 19th Sep 2019]

Gartner 2019c. Gartner Peer Insights 'Voice of the Customer': Enterprise Integration Platform as a Service
https://www.gartner.com/document/3956176?ref=solrAll&refval=228752146&qid=a97cf92ef5d788227d9b
http://www.uta.fi/sis/tie/tjsum/index/TJSUM_Luento5_2015_PirkkoNyk%C3%A4nen.pdf
[Accessed 20th Sep 2019]

Gartner, Mar 2019d. Gartner Predicts Up to Two-Thirds of iPaaS Vendors Will Not Survive By 2023. https://www.gartner.com/en/newsroom/press-releases/2019-03-07-gartner-predicts-up-to-two-thirds-of-ipaas-vendors-wi [Accessed 7th Nov 2019]

Groovy Apache. https://groovy-lang.org/ [Accessed: 20th Sep 2019]

Hein, D. 2019. The 9 Best Server Monitoring Tools To Use in 2019. Network Monitoring Solutions Review. https://solutionsreview.com/network-monitoring/the-9-best-server-monitoring-tools-to-use-in-2019/ [Accessed 7th Nov 2019]

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2013. Tutki ja kirjoita. 18. painos. Helsinki: Tammi.

Kananen, J. 2010. Opinnäytetyön kirjoittamisen käytännön opas. Jyväskylän ammattikorkeakoulu, Suomen Yliopistopaino Oy. Jyväskylä.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylän ammattikorkeakoulu, Tampereen Yliopistopaino Oy. Jyväskylä.

Kozlov, S. 2019. Best IT Infrastructure Monitoring Tools in 2019. https://dzone.com/articles/best-it-infrastructure-monitoring-tools-in-2019 [Accessed 1st Oct 2019]

Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere University Press. Tampere.

Lapan, S. D., Quartaroli, M. T. & Riemer, F. J. 2011. Qualitative Research: An Introduction to Methods and Designs. Hoboken: Wiley.

Linthicum, D S. 2003. Next Generation Application Integration: From Simple Information to Web Services. Safari Tech Books Online.

Loshin, D. 2010. Master data management. Morgan Kaufmann.

Luukka. E. Original article published Jan 20, 2017, edited Sep 9, 2019. Robotic Process Automation vs. Integration. https://digitalworkforce.com/rpa-news/robotic-process-automation-vs-integration-2/ [Accessed 27th Sep. 2019]

Magee, K. 2014. IT Auditing and Controls Part 10– A look at Application Controls. Infosec. https://resources.infosecinstitute.com/itac-application-controls/#gref [Accessed 30th Sep 2019]

Mendez, R. 2015. General Control vs. Application Control. https://prezi.com/iacknmfi6oxg/general-control-vs-application-control/ [Accessed 30th Sep 2019]

Moeller, R. R. 2007. COSO enterprise risk management: Understanding the new integrated ERM framework. Hoboken (N.J.): Wiley

Moeller. R. 2013. Executive's Guide to I Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. John Wiley & Sons publications. 2013.

Ojasalo, K., Moilanen, T. & Ritalahti J. 2014. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Sanoma Pro Oy. Helsinki.

Realyvásquez-Vargas, A., Arredondo-Soto, K., Carrillo-Gutiérrez, T. & Ravelo, G. 2018. Applying the Plan-Do-Check-Act (PDCA) Cycle to Reduce the Defects in the Manufacturing Industry. A Case Study. Applied Sciences, 8(11),. doi:10.3390/app8112181 https://search-proquest-com.ezproxy.haaga-helia.fi/docview/2250335376/fulltextPDF/EAFF858A686C4896PQ/1?accountid=27436 [Accessed 7th Nov 2019]

Reddy, S. 14th Feb 2019. 5 benefits of iPaaS. https://blog.axway.com/hybrid-integration/benefits-ipaas [Accessed 11th Oct 2019]

Russell, J.P. 2005. The ASQ Auditing Handbook. 3rd Edition. ASQ Quality Press, Milwaukee, Wisconsin. https://www.academia.edu/29334588/The_ASQ_Auditing_Handbook [Accessed 6th Nov 2019]

Rutaganda, L., Bergstrom, R., Jayashekhar, A., Jayasinghe, D., & Ahmed, J. (2017). Avoiding pitfalls and unlocking real business value with RPA. Journal of Financial Transformation, 46, 104-115. https://www.capco.com/-/media/CapcoMedia/Capco-Institute/Journal-46/JOURNAL46_full_web.ashx#page=104 [Accessed 6th Nov 2019]

Suominen, A. 2003. Riskienhallinta. 3. uud. p. Helsinki: WSOY

Siegel, C. 2019. iPaaS: Integration Plaform as a Service. https://blog.axway.com/hybrid-integration/whats-ipaas [Accessed 11th Oct 2019]

Singh, A. December 2018. Webinar Recap: Integration Platform as a Service (iPaaS) – Trends and Market Scenarios. https://www.appseconnect.com/webinar-ipaas-trends-and-market-scenario/ [Accessed 11th Oct 2019]

splunk. Modernize Your IT Monitoring with Predictive Analytics. 2019. https://www.splunk.com/pdfs/white-papers/modernize-your-legacy-it-with-predictive-analytics.pdf Accessed 22nd Oct 2019.

Tähtinen, Sami 2005. Järjestelmäintegraatio. Jyväskylä: Gummerus kirjanpaino Oy.

Worstell, K. F. 2013. Governance and Internal Controls for Cutting Edge IT. IT Governance Publishing.

Yin, R. K. (2009). Case study research: Design and methods (4 ed.). Los Angeles, CA: Sage.

Appendices

Appendix 1. Application Criticality level evaluation

Service Criticality

Defining service criticality

Rating is made by IT service management.

1: Critical

Applications having direct wide immediate impact to Company safety & operations, customer service, revenue, costs, whole organization efficiency or regulatory requirements

- Operations punctuality
- Sales and customer service sales portal

2: High

Applications highly critical some points of time

- Large number of regular internal users
- Customer Service applications having some tolerance to continuous availability
- Applications highly critical some points of time (e.g. Payroll, many Financial applications)

3: Normal

Applications used by many users and tolerating some hours of service breaks

4: Low

Applications tolerating long (~24 hours) service breaks

Appendix 2. Risk matrix questionnaire for integrations

Target risks		
LEVEL	**Description**	**Present level**
2	Integration error target is only the system itself or scheduled	
1	Integration error target is the system itself or its scheduled tasks and other internal or external system.	
0	Integration error impacts several systems and scheduled jobs.	

Probability risks		
LEVEL	**Description**	**Present level**
2	Integration error happens once in six months or once a year/very seldomly.	
1	Integration error occurs at least monthly.	
0	Integration error can occur weekly or even daily.	

Severeness risks		
LEVEL	**Description**	**Present level**
2	Integration error doesn't have impact to company's revenue or operations.	
1	Integration error can have an impact to company's revenue or operations OR the actual impact is not known.	
0	Integration error has severe impact to company's revenue and/or operations.	

Consequence risks		
LEVEL	**Description**	**Present level**
2	Integration error doesn't have impact to business continuity or other business processes. Estimate also how long business can tolarate if integration doesn't work: less than 1 day or more.	
1	Integration error can have an impact to business continuity or other business processes. Estimate also how long business can tolarate if integration doesn't work: less than >=5 hours.	
0	Integration error has a severe impact to business continuity and processes and effects operations. Estimate also how long business can tolarate if integration doesn't work: <=5 hours	

Appendix 3. Open interview questions with Dell Boomi developer

Interview held on 31st August 2019 and a follow-up meeting on 21st October 2019. In addition to these, there were also e-mail conversions.

31st Aug 2019

- Integration error handling, please explain the Try/Catch -process how it works in Dell Boomi
- What kind of coding is used in the Try/Catch -process?
- Can you share screen shots of the dashboard errors, Try/Catch -process and also on the Throw note?
- Is the process stopped completely if there's an error in one file or is it a continuing?
- Are different errors shown differently in the Dell Boomi dashboard?
- Are there any other options instead of e-mails for error messages?
- Are there log files stored in the Boomi server of errors?
- What kind of errors have you noticed in Dell Boomi, what are the most common error types?
- Please show the Dell Boomi dashboard and could you share a sample of P2P integration error how it's shown in the dashboard?
- Is it possible to retrigger a file in case of technical or connectivity issue?
- Can you provide View -access to Dell Boomi server?

21st Oct 2019

- In case of integration error, is it possible to trigger a message via API or other connector to JIRA or Company O's incident management tool?
- Are there other HTTP connectors available like Teams, slack or chat bots?
- Has there been any improvement actions for error handling so that tickets would be opened automatically?
- What kind of connectors you think would be benefical to be used?
- Do you see a reason why different connectors haven't been taken into use?

Appendix 4. Open interview questions with Company O's Head of Technology and Cyber Security

Interview held on July 2019 and a follow-up meeting in August 2019 on the Gartner reports.

- When and why Company O decided to implement Dell Boomi?
- Is there any other information that you could provide me on the Dell Boomi platform?
- What are the future plans for Dell Boomi in terms of automation and such?
- What do you know about the integration error monitoring and how widely it is used currently?
- Are there any Gartner reports that you could provide me on the Dell Boomi platform and iPaaS platforms?

Appendix 5. (confidential)

Attachment removed due to confidentiality.

Appendix 6. (confidential)

Attachment removed due to confidentiality.

Appendix 7. (confidential)

Attachment removed due to confidentiality.