Risk management in corporates

Can digitalization help improve risk management in cash management?

Jenni
Verno

Degree Thesis
International Business Management
2019

DEGREE THESIS	
Arcada	
Degree Programme:	International Business Management, MBA
Identification number:	20520
Author:	Jenni Verno
Title:	Risk management in corporates – can digitalization help improve risk management in cash management?
Supervisor (Arcada):	Andreas Stenius

Abstract:

The purpose of this study was to investigate if digital solutions help reducing risks related to cash management. The main theories included cash management, risk management and digitalization in finance. The study was conducted as case study. The results show that the companies have different solutions in cash management and all help in reducing operational and financial risk. The most important is to have a risk management plan that is actively conducted. The importance of monitoring the end users in financial actions was highlighted. The automation of digital solutions was also risk reducing factor. Many of the companies were already adapting Fintech 3 (Zheng et al. 2018, p. 1) that included smart finance that combines internet finance, Big Data to achieve accurate calculation and includes blockchain, cloud or other emerging technologies. Still it would be interesting to see if the companies are adopting more solutions like AI for reducing financial risks.

Keywords:	Digitalization, Cash Management, AI, RPA, Information Security, Risk Management, Financial risks, Operational risks
Number of pages:	62 + 7
Language:	English
Date of acceptance:	

OPINNÄYTE	
Arcada	
Koulutusohjelma:	International Business Management, MBA
Tunnistenumero:	20520
Tekijä:	Jenni Verno
Otsikko:	Risk management in corporates – can digitalization help improve risk management in cash management?
Ohjaaja (Arcada):	Andreas Stenius

Tiivistelmä:

Tutkimuksen tarkoitus on selvittää, auttavatko digitaaliset ratkaisut vähentämään riskejä kassanhallinnassa. Teoriaosa käsittelee kassanhallinta-termiä, riskienhallintaa sekä rahoituksen digitalisoitumista. Tutkimus on toteutettu tapaustutkimuksena.

Tulokset osoittavat, että yrityksillä on erilaisia ratkaisuja kassanhallinnan osalta ja kaikki nämä ratkaisut osaltaan vähentävät sekä operatiivisia- että rahoitusriskejä. Tärkeintä on, että yrityksellä on riskienhallintasuunnitelma, jota aktiivisesti noudatetaan. Tutkimuksessa nousee esiin myös se, että kassanhallinnan loppukäyttäjien toimintaa käydään läpi riskienhallinnan näkökulmasta. Digitaalisten ratkaisujen automaatio pienentää kassanhallinnan riskejä. Monet yritykset olivat jo tutkimuksen mukaan omaksuneet uudempia Fintech 3 (Zheng et al. 2018, s. 1) -ratkaisuja, jotka yhdistelevät internetrahoitusta ja Big Dataa suorittaakseen tarkkaa laskentaa ja jotka sisältävät lohkoketjuteknologiaa, pilvipalveluita tai muita nousevia teknologioita. Olisi mielenkiintoista nähdä, hyödyntävätkö tutkitut yritykset muutaman vuoden kuluessa enemmän tekoälyä vähentääkseen kassanhallinnan riskejä.

Avainsanat:	Digitalisaatio, Kassanhallinta, AI, Riskienhallinta, Rahoitusriskit, Operatiiviset riskit, Tekoäly.
Sivumäärä:	62 + 7
Kieli:	Englanti
Hyväksymispäivä:	

MASTERARBETE	
Arcada	
Utbildning:	International Business Management, MBA
Identifikationsnummer:	20520
Författare:	Jenni Verno
Arbetets namn:	Risk management in corporates – can digitalization help improve risk management in cash management?
Handledare	Andreas Stenius

Sammandrag:

Syftet med forskningen är att utreda hur digitala lösningar hjälper minska risker inom kassahantering (cash management). Teorin inkluderar kassahantering, riskhantering och digitalisering inom finansieringen. Resultatet visar att företag har olika lösningar i kassahantering och alla lösningar bidrar till riskreducering, i hänsyn till båda operativa och finansiella risker. Det är viktigt att man har en ordentlig riskhanteringsplan som man följer. Det är också viktigt att ha kontroll på användare i kassahantering. Automatiseringen är en faktor som minskar risker. Enligt forskningen hade många företag redan adopterat Fintech 3 (Zheng et al. 2018, s. 1) modell som inkluderar smart finans som kombinerar internetfinans samt Big Data för att nå noggrann kalkylering och som kombinerar blockchain, molntjänst och andra teknologier. Det skulle vara intressant att se om några av dessa företag som har undersökts kommer att använda mera av artificiell intelligens (AI) för att minska risker i kassahantering inom närmaste framtid.

Nyckelord:	Digitalisering, Kassahantering, AI, Riskhantering, Finansiella risker, Operationella risker
Sidantal:	62 + 7
Språk:	Engelska
Datum för godkännande:	

Contents

1 INTRODUCTION TO TOPIC

Companies have different kind of risks in financing, economy, IT and organization structure. Cash management can mean different things in different companies and in different countries, depending on their Financial Department or legislation. The overall term "Cash Management" covers the cash flow optimization and managing liquidity. (Agoston 2016, p. 1074) Digital finance includes all products, services, technology and infrastructure that enable companies to have access to payments, savings and credit facilities via online without the need to visit a bank or without dealing directly with the financial service provider. (Peterson 2018, p.2)

In recent years the risk management, organization culture and ethics have been emphasized in business. The standards for example in internal auditing have changed in 20th century. Companies need to describe their most significant risks and uncertainties and risks' impacts on the result of operations and financial position in the annual report. (Accounting Act 3:1.5§). Jarmo Leppiniemi has divided companies' risks into strategic, operative, financial and hazard risks. (Leppiniemi 2012, p. 48)

The Report to the Nations on Occupational Fraud and Abuse 2018 shows that the more active the company is in preventing frauds the more it mitigates losses. The active methods that companies can run are IT controls, surveillance and monitoring, account reconciliation, internal audit, management review and document examination. The process of management review means organizational control, processes, accounts or transactions for adherence to company policies and expectations. (Report to the Nations on Occupational Fraud and Abuse 2018, p. 18).

1.1 Purpose of the thesis

It is presently unclear whether the digitalization help to reduce risks relating to cash management. Digitalization in finance has been criticized of developing too fast so that regulatory environment is not enabling full-scale digital finance. Data security risks and systemic risks that nobody hasn't recognized before are lowering consumers' trust in digital finance. (Ozili 2018, p. 239) Still the digitalization continues, and we are experiencing Fintech 3.0 phase, which means smart finance which combines internet finance and big data to achieve accurate calculation and there includes blockchain, cloud computing and other emerging technologies. (Zheng et al. 2018, p. 1-2)

The aim of the present thesis is to investigate whether digital solutions can reduce risks related to cash management. The author is writing the thesis for Arcada University of Applied sciences. The idea for the thesis came up from OpusCapita Solutions Oy where the author is working as a Lead Consultant in Cash Management Department. The company is a software company focusing in purchase to pay solutions.

It is obvious that every company has nowadays some kind of digital solutions that they use in cash management and the automation has helped companies to optimize its business processes. In cash management there are related a lot of different kind of risks: data security, access policies, payment processes, book keeping and frauds. The author wants to investigate if the digital application or system help companies to minimize or manage their risks. Perhaps it is the opposite that fast-developing technology increase risk factors in cash management.

1.2 Statement of the problem and research questions

The specific research questions are:

1. What kind of risks the companies deal with in cash management?
2. Can digitalization help reduce these risks?

The thesis is structured as follows. The literature review is handling cash management, digitalization in finance and risks. The method is discussed in chapter three and the result of the study is discussed in chapter four. The empirical part is a case study focused in five Finnish companies, all listed (four in OMX Helsinki and one in NYSE). The author chose the companies because they had lot of global transactions. One of the chosen companies did not have much of global transactions but their cash management was globally concentrated and managed.

In literature review the author has gone through cash management, digitalization in finance and risks. In the empirical part the author has identified companies' risks related to cash management from annual reports (2017, 2018) and then performed interview to get deeper understanding of the digital solutions used by these companies.

The author of this thesis did not find directly a research that would fit in the exact same niche. Lot of research was found related to cash management as well as research related to digital finance and risks. Separately there were also research of ERP, SaaS, AI, RPA etc. Since digitalization is developing fast, the author tried to find lot of current references and articles from recent years.

2 LITERATURE REVIEW

2.1 Cash Management

From bank's perspective cash management means mainly financial transactions and systems that are built around financial transactions for example, online payments, account statements, cash pools and channels for delivering solutions for customers. (Bragg 2010, p. 4)

From company's perspective cash management can cover different things: optimization of cash in help of cash pools, netting, factoring and in-house bank, incoming and outgoing payments including due dates and payment collection, trade finance in terms of letter of credit and bank guarantees, also the risk controlling related to access and operational roles, bank accounts, and credit limits. (Bragg 2010, p. 5)

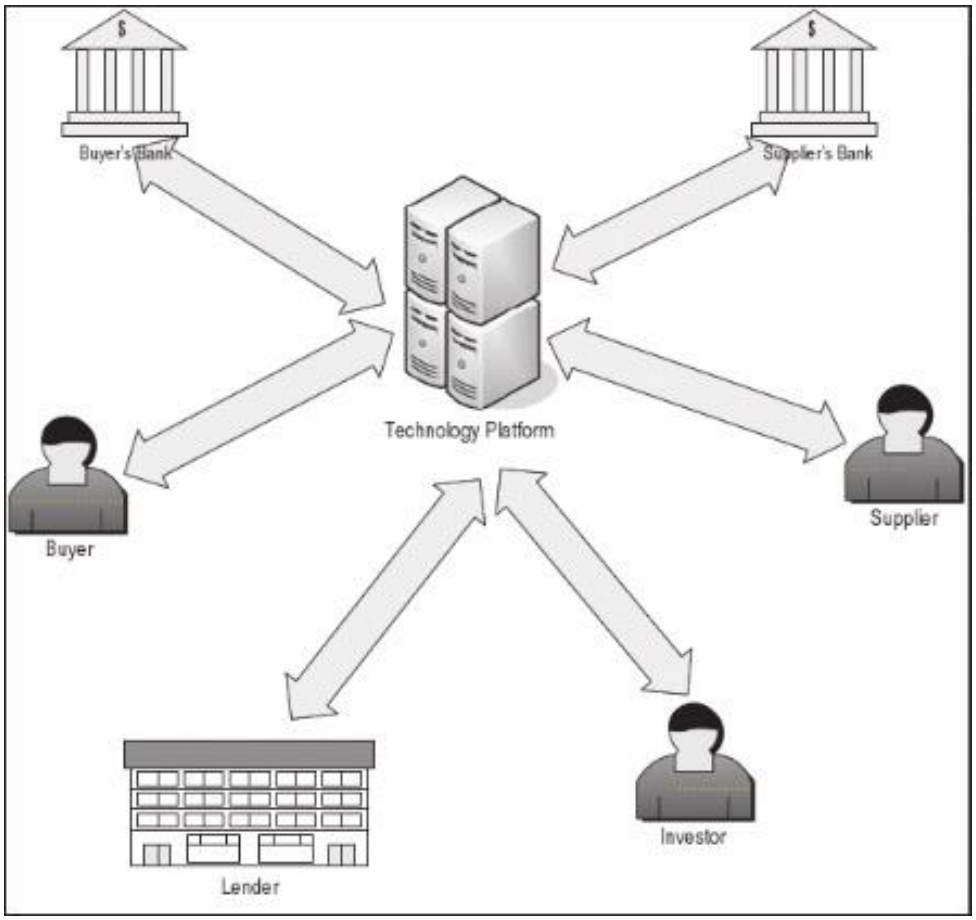
From treasury perspective the term cash management means using cash forecasting and working capital management activities to ensure that enough cash is available for operational needs. The efficiency of cash management can be for example, the use of cash pooling systems, which relates more to cash concentration. (Bragg 2010, p.4) "*Cash Management is concentrating on minimizing cash balance by collecting and disbursing cash effectively*." (Ross et al. 2008, p.771)

According to Leppiniemi: "*managing finance in companies can be divided into running tasks like cash management and credit trade (e.g. limits and interests) and then into the planning of how to optimize and increase the effect of sales and purchasing*". (Leppiniemi 2012, p. 165). The goal of the solution payment and account management is efficiency for example, payment flow and accurate reporting. (Leppiniemi 2012, p. 173). Efficiency can be reached by the help of cash pool accounts or the companies can minimize their need of banking services by using electronic banking, e-invoicing or direct debits. (Leppiniemi 2012, p. 181). Today direct debits in Finland are direct payments, e-invoices and SEPA direct debits. (FKL Sepa Services 2019)

Niskanen defines cash management as: "*running current assets as well as short term liabilities."* Current assets mean account receivables and inventory. Short-term liabilities mean account payables. (Niskanen 2016, p. 376) Liquidity refers to company's ability to manage daily liabilities like covering outgoing cash flows. (Niskanen 2016, p. 235) Technology has had a huge effect on payment traffic and the information (reporting) services have been developed during the 20th century. Cash can be considered as a risk since depositing cash is costly and nowadays the companies won't benefit the low interest rates. (Leppiniemi 2012, p. 182)

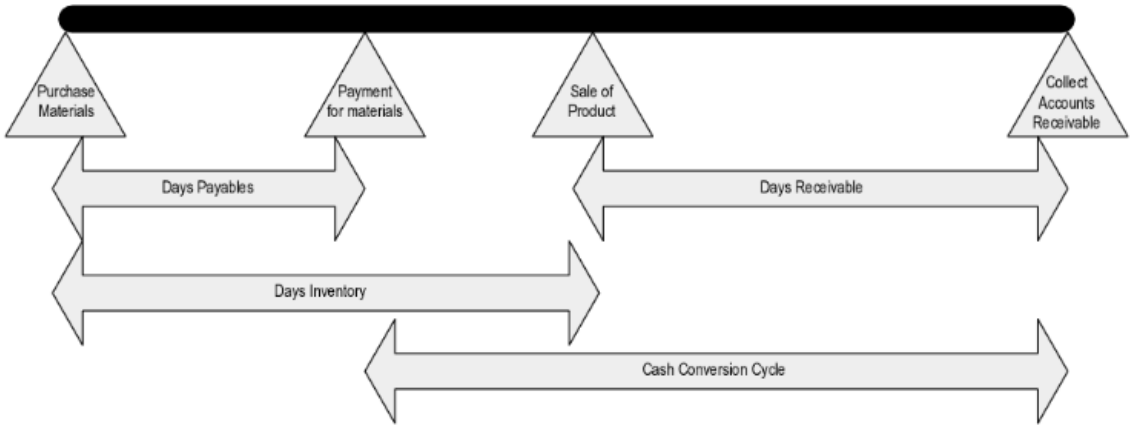
Cash management can also be defined as financial processes. Khalid calls financial processes as financial supply chain. From financial supply chain we can separate cash flow and working capital processes. It is critical that the processes run efficiently since companies need working capital to meet its short-term obligations, suppliers and for example tax authorities. (Khalid 2010, p. 51)

Figure 1Financial Supply Chain (Khalid 2010, p. 49)



The working capital processes are the elements of the financial back office. All cash inflows and outflows take place through them as does the management of the financial structure and procurement of goods and services. (Khalid 2010, p. 56) When looking at working capital process we can separate Cash Management to concern payment inflows and outflows and controlling liquidity.

Figure 2 Working capital process (Khalid 2010, p. 59)



Cash flow automation relates strongly to cash management. The automation of cash flow means automation of incoming and outgoing payments and liquidity management. (OpusCapita 2011, p.12) It is important to focus on cash flow automation since the number of non-cash transactions is growing fast and the automation makes processes fast, secure and visible (World Payment Report 2017, p. 10). The optimization of cash flows is important in terms of account payable payment terms, accurate timing and readiness to get short-term financing. (Niskanen 2016, p. 379)

Cash management is concerned with optimizing costs of short-term cash policies of a company. By calculating the cost and the risks of different cash management models and computing the data, the case study provided a new tool that helped cash managers to choose the correct cash management model (Molina et Al. 2018, p. 282)

2.1.1 The Future of Cash Management

In the future new payment ecosystems are emerging what means open API's (Application Programming Interface), instant payments, blockchain technology (with virtual currencies) and new payment and transaction types – however this also requires harmonization and regulation from governments. The automation of repetitive tasks is enabling treasuries to take over more strategic roles and focusing on cash forecasting and fraud prevention. The cyber threat and multiple payment ecosystem participants need to be monitored and evaluated more carefully. (World Payment Report 2018, p. 35)

New regulations in finance, development in information technology and global business operations are important aspects in the near future. (Polak et al. 2018, p. 189) Global financial crisis affected for example, to change of role of the corporate treasurers and cash managers. The crisis shifted the focus from earnings to easy availability to cash and liquidity. Managing of risks like securing liquidity got more focus. (Polak et al. 2018, p. 190)

2.1.2 SEPA

The Single Euro Payments Area (SEPA) was a project to harmonize the way of making and processing retail payments in euros. The goal was to make payments in euro and across Europe fast, safe and efficient. SEPA enabled customers to make cashless euro payments to anyone located anywhere in Europe, for example by credit transfer, direct debit or debit card. The SEPA territory consist of 34 European countries and includes countries which are not part of the euro area and the European Union. SEPA sets same standards and rules in payment transactions and this applies e.g. ISO20022 XML messages, IBAN bank account number and bank identifier code BIC. (ECB SEPA key facts 2019, p. 2) Furthermore, SEPA has transformed the digital financing in Europe when many treasuries have been able to centralize their ERP's because of standardization and common currency between EURO countries. (Palva 2015, p. 12)

Along with SEPA came also PSD (Payment Services Directive and its second phase PSD2). The purpose of PSD2 is in payments to increase pan-European competition with participation also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users. On October 8, 2015, the European Parliament adopted the European Commission proposal to create safer and more innovative European payments (PSD2, Directive (EU) 2015/2366). The new rules aim to protect better consumers when they pay online, promote the development and use of innovative online and mobile payments such as through open banking (API), and make cross-border European payment services safer. (PSD2, Directive EU 2015/2366

2.2 Technology in financial processes

2.2.1 Digitalization in finance

The first technology phase in finance was the Internet in 1995. Today we are experiencing the second phase of revolution in finance and it is the digitalization in finance. (Dandapani 2015, p. 3) The new marketplace on the internet differs from the traditional market environment. The firms that build up their businesses in the digital market are internet-based companies (IBCs). Their value creation and delivery are based on the internet, which means that if the servers would stop working, these companies would be unable to create and deliver the value that they offer to their customers. (Wittkopp 2018, p.194)

Corporate treasury management is aiming full automation and straight-through processing (STP) for systems integration. Use of inhouse-bank cover finance activities and serve as a center of expertise and control. The automation can include features like payment on behalf (POBO) and collection on behalf (COBO). Corporates are using more and more online banking, e-billing, e-procurement, XML standards, cash pooling solutions and instant payments. (Polak et al. 2018, p. 193) Taking advantage of business intelligence the corporates get more reliable reports for decision making and analyzing.

Digitalization is disruptive and it has an impact on almost any sector of the global economy and profoundly changes business practices and creates new innovations. (Wittkopp 2018, p. 194-195) Smart, connected products are completely changing the value chain and therefore companies need to rethink what they are doing (Porter & Heppelmann, 2014)

Peterson puts digital finance into consensus that digital finance encompasses all products, services, technology and infrastructure that enable individuals and companies to have access to payments, savings and credit facilities via online without the need to visit a bank or without dealing directly with the financial service provider. (Peterson 2018, p.2)

Almost all the productivity gains of the last 50 years have not come from better management and financial controls. These productivity gains have come from better automation and control of the processes. The same advances in integrated circuits and electronics that brought us the PC and the smartphone also brought us intelligent sensors, networked devices, and database-driven control systems. (Boyes 2014, p.xxiii)

In the article of Digital Finance and FinTech: Current research and future research directions by Gomber et al. 2017, p. 537 has been stated that: *"financial industry has experienced for decades a continuous evolution in service delivery due to digitalization"*. This means expanded connectivity and enhanced speed of information processing both at the customer interface and in back-office processes. Digital financing is defined as for example "new innovations" like digital banking, mobile solutions and delivery platforms, micro finance, payment solutions, peer-to-peer lending and delivery platforms. New technologies and services are not only reserved for start-ups but also for established service providers.

Term FinTech (Fintech) is a neologism which originates from the words "financial" and "technology" and describes in general the connection of modern and, mainly, Internet-related technologies (e.g., cloud computing, mobile Internet)

with established business activities of the financial services industry (e.g., money lending, transaction banking). (Gomber et al. 2017, p. 538-539)

Since there have been lot of research in 2015 related to digitalization of financial processes, Maresova et al. 2018 uses the term Industry 4 (Fourth Industrial Revolution) and concludes that individual countries can prepare for the social and economic impacts involved in the current trend of digitization and automation. In the future, an increasing interconnection of industry, science, research, and innovative new technologies can be expected. (Maresova et al. 2018, p. 11)

According to Dandapani (2015, p. 3) the digital finance processes include payment systems, cloud computing in financial services, valuation metrics for multi-sided platforms (MSPs), quantum trading; and cyber security – costs, benefits and protection. Electronic finance is a dominating force changing business models and systems in financial services. New developments are creating newer valuation metrics and reinforcing the costs and benefits of security systems. (Dandapani, p.1)

Today when talking about digitalization in finance it is more about technological enablers that have important facilitating functions in financial processes, operations, and business models. Important facilitators are for example, fast and mobile Internet, artificial intelligence (AI), worldwide connectivity, mobile devices, intuitive user interfaces and security technologies. (Gomber et al. 2017, p. 537)

2.2.2 SWIFT

Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a core part of the financial services infrastructure and is widely regarded as the most secure trusted third-party network in the world serving 200 countries with over 8000 users. SWIFT was founded in 1973 based on the vision of creating a global financial messaging service and a common language for financial messaging (Scott 2012, p.462)

2.2.3 Electronic banking

Electronic banking is a high-order construct, which consist of several distribution channels. It should be noted that electronic banking is a bigger platform than just banking via the Internet. (Pikkarainen et al. 2004, p. 261) In Finland electronic banking has been developed already from the 1980's when banks started to use technology in banking and especially in clearing. After 1995 when internet came along the internet banking started to develop.

Shaikh et al. continues: "*Mobile banking (m-banking) has emerged as an important distribution channel. Electronic commerce (e-commerce) continues to have an impact on the global business environment, but technologies and applications also have begun to focus more on mobile computing, the wireless Web, and mobile commerce.* "(Shaikh et al. 2015, p. 129)

Electronic banking is not only about internet banking. It can be related to banking software that includes several functions like money withdrawal, accounts inquiry, deposit, bank counter transactions, customer account information, message monitoring and SWIFT. So electronic banking can be performed with different kind of banking software tools. (Altin Gumussoy 2016, p. 277)

2.2.4 ERP

ERP (Enterprise Resource Planning) systems were already developed at the 1960's when modern factory production increased and computing was born, there was a need to manage and balance production and customer demand. These early computing programs helped plan manufacturing, purchasing and delivery. They helped companies to keep their stock levels low, which in turn reduced the amount of money tied up in inventory. At the 1990's the term ERP got more common and more wide system when it became more generally for the companies' back office tool. (Rashid 2002, p. 2-5).

In 2000 it was the internet-enabled software that gave real-time access to the ERP solution. It also described software that went beyond a company, to provide management and functionality that helped a company to integrate with systems outside of the business. This involved the integration of supply chain management, customer relationship management (CRM) and business intelligence. (Rashid 2002, p. 12-13)

Figure 3 ERP System concept 1990's (Rashid 2002, p. 3)

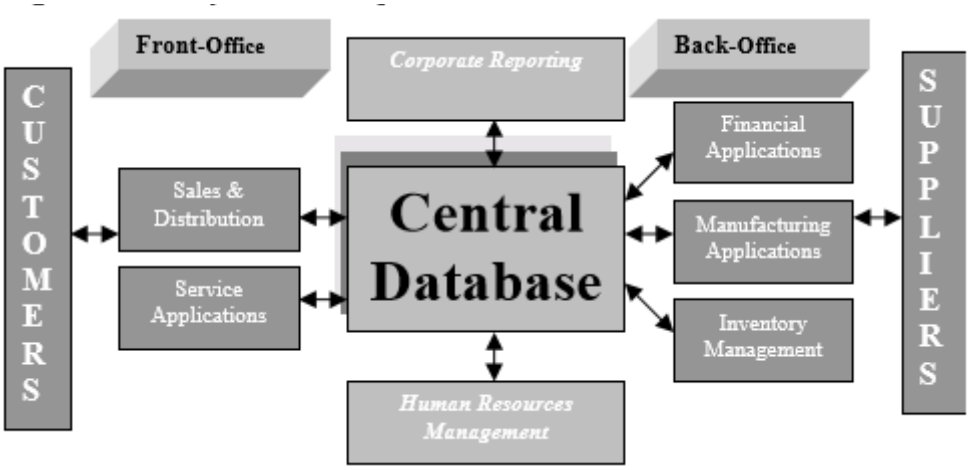
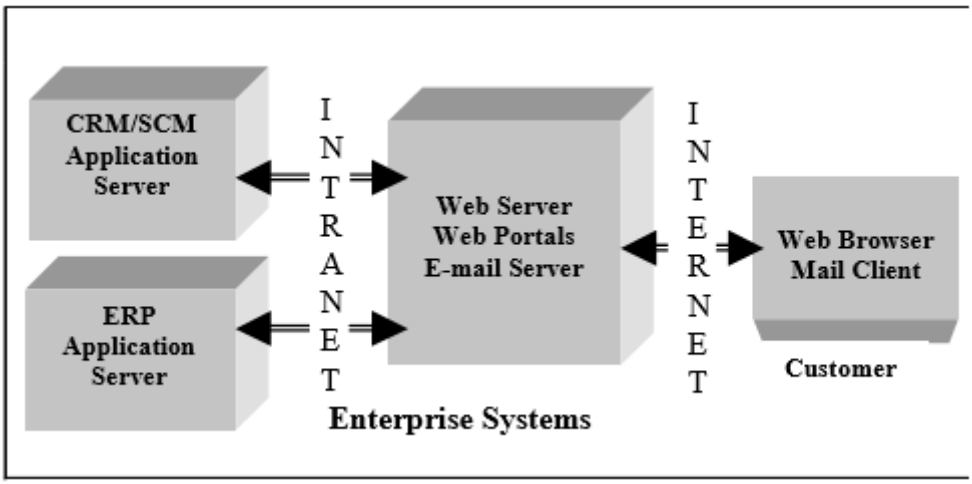


Figure 4 Web-enabled extended ERP system (Rashid 2002, p. 14)



2.2.5 SaaS technology

Cloud computing is an elastic execution environment of resources involving multiple stakeholders and providing a metered service and multiple granularities for specified level of quality. SaaS (Software as A Service) provides ready-to-consume software applications which address the needs of specific business functions and processes. Cloud providers manage the software applications and the hosting environment completely. Cloud customers might need to manage their specific configurations within the supported software application. (Abbadi 2018, p. 46)
The base of cloud banking is a pay-per-use or subscription-based service that extends the capabilities of information technology in real time over the internet. The principle behind this is based on the optimization of supply chains that translates into higher efficiency and lower costs.

Cloud computing is advantageous to both users and service providers in terms of cost savings and flexibility due to usage-based billing. An increase in flexibility leads to an increase in capacity, which helps financial institutions shift their expenditures elsewhere instead of investing in infrastructure, personnel education or software licensing. Security asset of the SaaS is that service providers are under constant scrutiny, going through background checks, certifications and external monitoring. Encryption also plays an important role when providers are protecting the data entrusted to them. (Dandapani 2015, p.3)

An academic article of Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis tells about the research where North Carolina State University achieved a substantially decreasing of expenses with software licensing and at the same time reduced the campus IT staff from 15 to 3 employees with full working schedule. The university was experiencing continuous increased IT costs and they had to start finding ways to get savings without weakening the quality of studies. Biggest risks related to data protection, and to the sensitive data like research, results, students' scholastic records and employees' accounts. Many of the risks specific to cloud environment were transferred to cloud providers and special attention was in data security. (Mircea et al. 2011, p. 2-4)

When choosing the data protection and security solution, the risks and costs on/non-implementation must be considered, as well as the benefits of using the respective solution. Data encryption is the simplest solution of data protection against the unauthorized access in the cloud environment. Data may be encrypted now of their collection or before their transfer in the cloud environment. Other protection methods were firewalls and federated identity management (Mircea et al. 2011, p. 2-4)

Though cloud computing provides appealing benefits in terms of cost reductions and increasing productivity it introduces security issues. It makes authentication important in terms of the need to build stronger mechanisms like Multi-Factor Authentication (MFA) and Single Sign-On (SSO) models. MFA is based on Two-Factor Authentication that means a one-time password as a second factor after standard password authentication. SSO in other hand is used to eliminate password management complexity. For web-based sessions using cookies, perhaps the most promising solution is to cryptographically bound them to the underlying Transport Layer Security (TLS) channel. This avoids cookie theft and can be extended for bounding SSO security assertions. (Soares 2013, p. 1)

2.2.6 API (Application Programming Interface)

API is a software intermediary that allows two applications to talk to each other. In open banking API is a system that provides a user with a network of financial institutions' data through the use of APIs. The Open Banking Standard defines how financial data should be created, shared and accessed. By relying on networks instead of centralization, open banking helps financial services customers to securely share their financial data with other financial institutions. Benefits include more easily transferring funds and comparing product offerings to create a banking experience that best meets each user's needs in the most cost-effective way. Real-time data allows more effective planning and helps companies to make invoice-factoring decisions. Open banking can help financial-risk oversight by

providing reporting of counterparty exposures, automatically calculating liquidity positions, forecasting scenarios and supporting foreign exchange. (Wright 2018, p. 41)

2.2.7 AI (Artificial Intelligence)

AI is usually a broader term for machine learning, deep learning and neural networks. AI can be used to render new insights, transform decision making and drive improved business outcomes. It includes many areas of study and technologies behind capabilities like voice recognition, NLP, image processing and others that benefit from advances in algorithms, abundant computation power and advanced analytical methods like machine learning and deep learning. (Jones 2003, p.5).

Machine learning is a branch of AI that aims to give machines the ability to learn a task without pre-existing code. In the simplest terms, machines are given a large amount of trial examples for a certain task. As they go through these trials, machines learn and adapt their strategy to achieve those goals. Deep learning is often made possible by artificial neural networks, which imitate neurons, or brain cells. (Jones 2003, p. 9)

For example, combinations of AI, big data, and blockchain technologies could make it possible to do real-time verification of business transactions and audits of full financial data sets, reducing and perhaps eliminating the need for sampling. (Tysiac et al. 2018, p. 28) Xin and Yan have concluded that using AI increases in accounting information quality and that cause systematic risk to decrease (Xin and Yan 2019, p. 102)

According to Zheng et al. their research has shown that recent progress of AI technology can improve service efficiency and reduce costs in different financial areas like in risk management and financial security. AI is the core technology of new technological revolution and industrial transformation. In finance there has been three phases of AI. The first was Fintech 1.0 where computers could be used for replacing manual calculation and accounting books for more effective

financial operations. The second Fintech 2.0 was called Internet finance and the third phase is now ongoing and it is called Fintech 3.0 smart finance which combines internet finance and big data to achieve accurate calculation and there includes blockchain, cloud computing and other emerging technologies. (Zheng et al. 2018, p. 1-2)

AI together with Big Data can for example, help in assessing risks, build credit systems and achieve anti-fraud functions. Khandani et al. 2010, p. 47 constructed machine-learning forecasting model to estimate consumer credit risks. In fraud detection Bolton et al. 2002, p. 235-249 presented a method based on anomaly detection process.

2.2.8 RPA

RPA (Robotic Process Automation) is tailored for repetitive back office jobs that typically are not client facing, for example accounting data entry, communication between different systems, monitoring, reporting, payment processing etc. Adopting RPA makes sense for any organization looking to improve the efficiency, but many companies are choosing low-cost labor in cheaper regions than robotic automation. RPA is not prone to human error and no training is required which reduces the operational risks. What comes to global companies – robotic automation diminishes disadvantages created by time zone restrictions. (Seasongood 2016, p. 31-32)

2.2.9 Blockchain

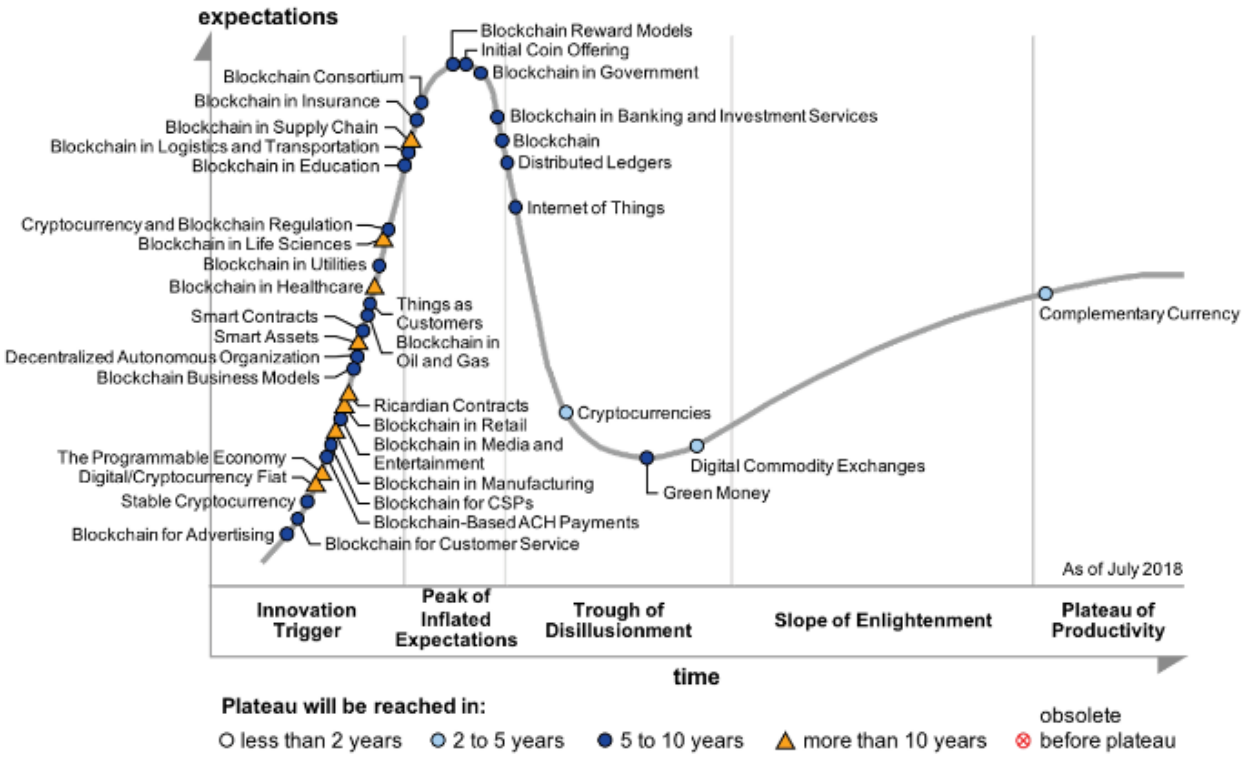
Blockchain is a secure transaction ledger database that is shared by all parties participating in an established, distributed network of computers. It records and stores every transaction or exchange of data that occurs in the network, essentially eliminating the need for "trusted" and centralized third parties. A transaction is a transfer of information between two or more nodes within the network: this information can be virtual currencies (e.g. bitcoins), sensor data, property information, or any other type of structured data. (Bashir 2017, p. 16)

Blockchain is often described as a "transfer of trust in a trustless world," referring to the fact that the entities participating in a transaction are not necessarily known to each other, yet they exchange information with surety and no third-party validation. The blockchain enables entities (companies, individuals, sensors) to exchange and share data and information in a distributed and secure way, enabling anonymity of these entities (if required). (Bashir 2017, p. 17)

Data ownership and data security can be hinder to data sharing. In finance the blockchain technology can solve the problem of information decentralization in terms of digital currency, payment and settlement, intelligent contracts and financial transactions with consensus mechanism and security in the center. (Zheng et al. 2018, p. 6)

Bitcoin is one of the numerous virtual currencies based on blockchain technology. It was developed in 2008 by Satoshi Nakamoto. A Peer-to-Peer Electronic Cash System was written on the topic of peer-to-peer electronic cash and introduced the term chain of blocks. This term over the years has now evolved into the word blockchain. (Bashir 2017, p. 9) In order to achieve this goal of a “trusted record within an untrusted environment,” the Bitcoin ledger relies on significant computational power and interested parties or “miners” to validate and confirm transactions, using a structured process for adding transaction records to the blockchain in return for monetary reward. By trusted record Nakamoto was referring that Bitcoin is an electronic payment system based on cryptographic
proof instead of trust. (Nelms et al. 2018, p. 21)

Figure 5 Gartner hype cycle of blockchain 2018 (Gartner 2018)



Gartner's hype cycle of blockchain predicts that in 5 to 10 years banking and investment services have taken blockchain into use. (Gartner 2018) For example, the Swedish Central Bank (Riks Bank) has already started to investigate the possibility to replace cash by digital currency "e-krona" because the amount of cash is decreasing all the time. (Sverige's Riks Bank 2018)

2.3 Risk Management

Chapman and Cooper (1983) define the risks as an exposure to the possibility of economic of financial loss or gains, physical damage, injury, or delay because of the uncertainty associated with pursuing a course of action. (see Jie 2002, p. 91) Risk management is a systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk. (Jie 2002, p. 91)

According to McKinsey survey 2017: Digitalization consists of Data management (data governance, data quality, consistency processes, and operating models), Process and work-flow automation (streamline, standardize, and efficiently execute routine tasks), Advanced analytics and decision automation (statistical techniques and algorithms, together with artificial intelligence like machine learning and robots), Cohesive, timely, and flexible infrastructure (data architecture and the use of techniques such as data lakes, virtualization, and the hybrid cloud), Smart visualization and interfaces (tools and applications present users with data like interactive dashboards, and even augmented reality), External ecosystem (digital capabilities developed with established peers and utilities), Talent and culture (traditional business and technology knowledge and experience with modern data, analytics, and digital expertise). (McKinsey 2017, p. 8)

While digitalization in finance has developed aid for companies to monitor their financial risks it is still important to underline that the main responsibility belongs to management. It includes the risks like political and country risks, hedging and currency risks, funding, interest rate and legal risks as well as documentation risks and it is management's responsibility to make sure that adequate systems and controls are put in place. (Dickson, 1998, p. 298)

2.3.1 Risk categorization

The first step in creating an effective risk-management system is to understand the qualitative distinctions among the types of risks that organizations face. According to Harward Business review – Managing Risks, a new framework 2012: *"Risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them."* This won't help if the company is facing external risks, like natural catastrophe. The article categorizes risks into three different categories: preventable risks, strategy risks and external risks. (Kaplan & Mikes, 2012)

Preventable risks are inside the organization and are controllable and can be prevented for example by monitoring operational processes. Examples are the risks from employees' and managers' unauthorized, illegal, unethical, incorrect, or inappropriate actions and the risks from breakdowns in routine operational processes. Strategy risks are different than preventable risks because they cannot be managed through a rules-based control model. Instead they need a risk-management system designed to reduce the probability that the assumed risks materialize and to improve the company's ability to manage the occurred risk events. Many companies take risks through their research and development activities. Some risks arise outside the company and are beyond control like natural and political disasters. Companies cannot prevent such events from occurring, their management must focus on identification and mitigation of their impact. (Kaplan & Mikes 2012)

Enterprise Risk Management (ERM) plays a corporate governance role in the holistic management of all risks to aid in decision-making and increasing the likelihood of achieving operational and strategic objectives. Risks are typically classified as hazard, financial, operational and strategic risks by CAS 2009 and ISO3001. (McShane 2017, p.137)

CAS defines that there are two dimensions in ERM: *risk type* and *risk management processes.* Risk types are hazard, financial, operational and strategic. Risk management processes include understanding of the current conditions, identifying risks, analyzing, prioritizing and monitoring risks. (Louisot et al. 2014, p. 104). In Finland the Finnish Risk Management Association (FinnRima) has used the same categorization. (www.riskikompassi.fi)

Strategic risks relate to developing business and executing its strategy plan. The organizations need to be able to adopt changing economies and keep up in the changing technology environment. When companies are seeking growth potential from abroad, they need to prepare for different kind of legal requirements and culture. Strategy risks can also relate to organization structure or outsourcing processes. (Louisot et al. 2014, p. 4)

Financial risks are related to the companies' liquidity planning, interest and currency risks, credit risks and changes in taxation. (Niskanen 2016, p. 398) Liquidity risk means that company does not have enough cash to cover outgoing cash flows (short-term debt, account payables etc.). To liquidity risk the company can affect by optimizing account payables e.g. using cash discount or paying on the last due date and with cash forecasting. (Niskanen 2016, p. 399, 327) Credit risk is a risk where customers are not able to pay their invoices (account receivables). This is preventable by monitoring customer payment behavior. (Niskanen 2016, p. 390)

Currency risk is highlighted when company is doing global business. Currency risk can expose in a single transaction related to purchases and sales or it can be seen when a subsidiary is abroad, and the balance sheet are shown in domestic currency or the company's market value can depend on currency rate of exchange. Companies can cover from currency risks by using solutions like netting or making derivatives. (Niskanen 2016, p. 431-432)

Hazard risks are unexpected external risks (natural catastrophe or personnel lost etc.) that can harm the company when they happen. It is important to analyze and recognize these kinds of risks. Often the companies have insurance for this kind of risks but then it is important to follow insurance company's policy how to prevent the risks. Many companies have a crisis plan in case of hazard risk. The operational risks include technology, information and quality management, processes, personnel's knowhow, contracts and responsibilities and frauds. (Niskanen 2016, p. 250)

European Banking Authority monitors the risks within following framework (EBA Risks Assessment Report 2017, p. 18-19):

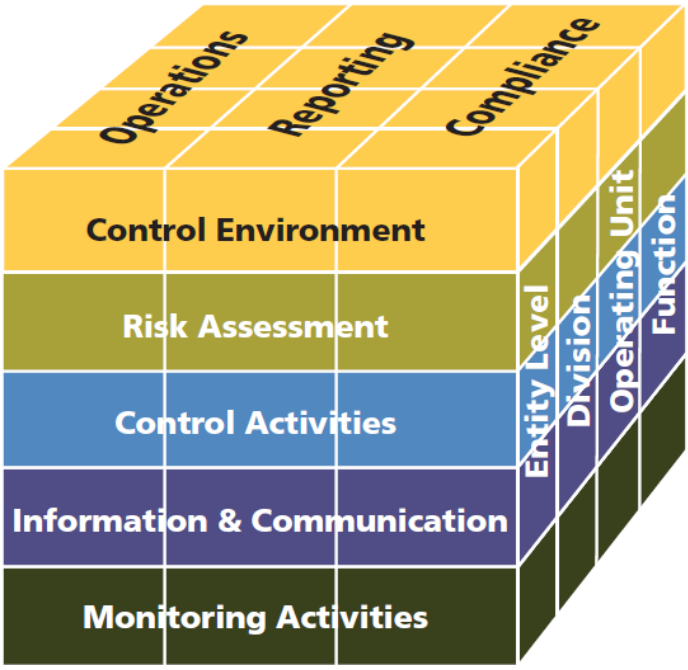
Table 1 Risk framework (EBA 2017, p. 18-19)

Business model analysis	Credit risk	Operational risk
- A description of how a company intends to generate revenues and earn a profit - the assumptions used might turn out to be wrong. - e.g. the limited adaptability of IT infrastructures	- A risk of not getting the account receivables that leads disruption to cash flows, and increased collection costs - internal credit controls, in data quality and in reporting	- A prospect of loss resulting from inadequate procedures, systems or policies. Systems failures or Fraud - IT risk due to large and complex IT environments and aging IT systems
Market risk	**Liquidity risk**	**Interest rate risk**
- the possibility of an investor experiencing losses due to factors that affect the overall performance of the financial markets	- A risk that a company or bank may be unable to meet short term financial demands. - Improved internal tools needed to measure and monitor liquidity risk	- An investment's value will change due to a change in the absolute level of interest rates (maturity) - internal behavioral models and quality of data

Market risk relates to product pricing and to currencies and interest. For example, if company operates in transporting business the change in oil price effects directly on the transporting costs. And if the company won't manage to transfer this cost in their prices this will immediate impact on the company's profitability. It is possible to minimize risks by derivatives and transferring part of the risk to banks. (Niskanen 2016, p. 235)

COSO (the National Commission on Fraudulent Financial Reporting established in 1985) is an independent private-sector initiative that studies the causal factors that can lead to fraudulent financial reporting. The organization has developed a framework for internal control, enterprise risk management and fraud deterrence. In 2013 the organization updated its framework into cube and many listed companies globally use the cube as a basis for company's own risk framework. (www.coso.org)

Figure 6 COSO Cube (Coso Framework, p. 4)



2.3.2 Operational risks

Since this study is focusing on the risks in cash management and digital solutions it is important to focus on the operational risks rather than e.g. hazard risks. Operational risk is identified and related to international standards on the seven types of events: internal fraud, external fraud, clients, products and business practices, losses incurred tangible assets, business disruption and system failures, delivery and execution and management processes, and employment practices and workplace safety. (Angelache 2011, p. 66)

Organizations might invest to technology that is obsolete or the integration architecture is not supporting new technical solutions. Information and quality management relates to thoroughly planned reporting and transferring data from system to another. It needs to be secured and controlled and considering the cyber risks as well as educating its personnel to protect from those risks. (CAS 2019)

In the organization there can be several units that are responsible for operational risks mentioned above like Accounting Department, Internal Audit, IT, Risk Management, Operations Department etc. (Angelache 2011, p. 66) Angelache suggests measurement of operational risk and creating a methodology to identify, plan and avoid operational risks. (Angelache 2011, p. 71)

Weeserik points out that globalization, global internet connectivity, and value chain dependencies, have made operational risks more significant than ever before. The risk exists in every organizational activity. (Weeserik 2018, p. 1-2) Operational risk management includes 4 categories: risk identification, risk analyzing, risk reducing measures and risk monitoring. (Jie 2002, p. 93)

Operational Risk Management (ORM) includes human actions, internal processes, systems, and external events. Information systems provide benefits for integrating risk management activities and optimizing performance due to increasing requirements, complexity and a growing volume of risks. Business Performance Management (BPM) technologies are believed to provide a solution for effective Operational Risk Management by offering several combined technologies including work flow, data warehousing, advanced analytics, reporting and dashboards. (Weeserik 2018, p. 1)

2.3.3 Internal Audit

According to the Finnish Limited Liability Companies Act 21.7.2006/624: "*the company's management must ensure that proper books of account are kept*". IIA (the Institute of Internal Audit) says that the definition of internal audit is: "*Internal auditing is an independent, objective assurance and consulting activity*

designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." (IIA 2018)

Internal audit in Finnish companies are based in COSO framework that defines internal control as *"a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations."* Internal control system includes five components work to support the business objectives: Control Environment, Risk Assessment, Control Activities, Information & Communication and Monitoring Activities. (COSO, Integrated Frameworks 2013)

2.3.4 Code of conduct

A code of conduct has value as both an internal guideline and an external statement of corporate values and commitments. It clarifies an organization's mission, values and principles. A code of conduct encourages discussions of ethics and compliance, empowering employees to handle ethical dilemmas they encounter in everyday work. It can also serve as a valuable reference, helping employees locate relevant documents, services and other resources related to ethics within the organization. Externally, a code of conduct serves several important purposes: compliance, marketing and risk mitigation like preventing illegal acts. (Mamic 2014, p. 10)

2.3.5 AML (Anti-Money Laundering)

Since business is more global and engaging with e-commerce it will enhance the risks of identity-related financial crime. The money launders try to use the weakness of financial regulation and the possibility of being monitored and detected. The online payments make the effective AML regulation hard to meet. Anonymity, non-face-to-face contacts, the speed of transactions and globalization with

cross-border activity attracts criminals. (Yan 2011, p. 94) Companies have today their compliance policies as well as banks have their own policies to reduce the AML risk. Yan (2011) states that there has been too much focus on "front-end" of customer identification than on the "back-end" which controls online money laundering activities. (Yan 2011, p. 99).

Know your customer (KYC) is essentially the work conducted by a firm or bank to undertake background checks on clients and customers to enable them to both obtain and confirm additional information regarding their customers. KYC is designed to understand the customer's circumstances and business. So, it is not performed only for in terms of the risk of money laundering or terrorist financing, but also in terms of their profitability to the firm. (Cox 2014, p. 169)

AI could be a solution for suspicious transactions. When banks are flagged of suspicious transactions the compliance team start to investigate the reason. This can often take time. With help of AI the compliance team could automate the desktop research process by scanning Internet search engines, news sites and internal and external database to put together the suspicious individual's "dossier" within a minute. AI would help the system to filter out irrelevant information such as individuals with identical names. (Enterprise Innovation 2017) The same solution could be used also in companies to avoid frauds. (Bolton et al. 2002, p. 235-249)

2.3.6 Frauds

The important factor in operational risks is frauds. European Community Council Regulation 2899/95 defines irregularity as follows: "*Irregularity shall mean any infringement of a provision of Community law resulting from an act or omission by an economic operator, which has, or would have, the effect of prejudicing the general budget of the Communities or budgets managed by them, either by reducing or losing revenue accruing from own resources collected directly on behalf of the Communities, or by an unjustified item of expenditure*." In this regulation the term irregularity means economic abuse or misappropriation and the author uses

term fraud further on with the Thesis. It is almost impossible to include misappropriation to the Act of Criminal Code of Finland (39/1889) because it is very difficult to define the line between deliberate or gross negligence.

When the punishment is not always defined because the term misappropriation or economic abuse are wide, and the punishment are always strictly related to the law text, it is important for companies to prevent misappropriation and economic abuse. The impact of gray economy for the communities is huge: it has been estimated that in Finland the number is approximately five billion euros every year and only a small fraction reveals or lead to criminal or administrative measures. Economic crime means act in company or in community or abusing those and is aiming for illegal financial gain. (Koivu et al. 2010, p. 15-16).

The Report to the Nations on Occupational Fraud and Abuse 2018 reveals that globally there are millions of business and public organizations vulnerable or potentially vulnerable to fraud committed by their employees. Occupational fraud means fraud committed against the organization by its own officers, directors, or employees who were entrusted to protect its assets and resources. According to this survey there were 2690 real cases of occupational fraud in different industry categories from 125 countries. These losses were estimated to be more than seven billion dollars. The most common frauds were asset misappropriation schemes with amount of 89% of the cases. (Report to the Nations on Occupational Fraud and Abuse 2018, p. 5-6).

2.3.7 How to cover from frauds

There are several ways how companies and organizations can cover from irregularities and frauds. The positive way is to update company policies and instructions and control that they are being followed. Also, a thorough risk analyses help organizations to cover the targets. If management takes care that internal audit is working properly the risk for irregularities decreases. The rejecting misappropriations can be divided in different levels: structural basis, socializing basis,

motivation and circumstances, decision making process and the misappropriation itself. (Koivu et al. 2010, p. 71).

Important actor in covering from frauds is the organization culture. The management has the final control in building the structure, norms, internal instructions and the organization chart and the norms must be updated and clear for everyone in the organization. It is difficult to recognize motivated irregularity actors, but organizations can see that internal audit acts as a preventing actor for irregularities as well as it can analyze the abuse targets and cover those carefully. (Koivu et al. 2010, p. 26-28).

By organizing thorough accounting the company can reveal accounting manipulation. Internal auditing is independent and objective control and assessment and it is not only looking for frauds, but it also consults company management to avoid risks. The field for the misappropriations is so wide that none of the theories can cover the total prevent of misappropriations. (Koivu et al. 2010, p. 67-71)

2.3.8 Cyber threats

Cyber threat consists a myriad of advanced attack scenarios. Adversary behavior is no longer primarily focused on widespread, disruptive activity. It is characterized by targeted, multi-stage attacks that aim to achieve specific tactical objectives and establish a persistent foothold into vulnerable enterprises. (Gore 2017, p. 233)

Cyber threat can be defined as the threats and risks that come from firms' activity online, trading on the internet, the use of electronic systems such as credit cards and ATM cards, networks of technology as well as storage of personal data in computers or computer networks. Cyber security can be breached by a growing number of potential parties, including internal employees, disgruntled customers, rogue hackers, competitors and global activist groups. (Dandapani 2015, p.622)

2.3.9 Managing Information Security

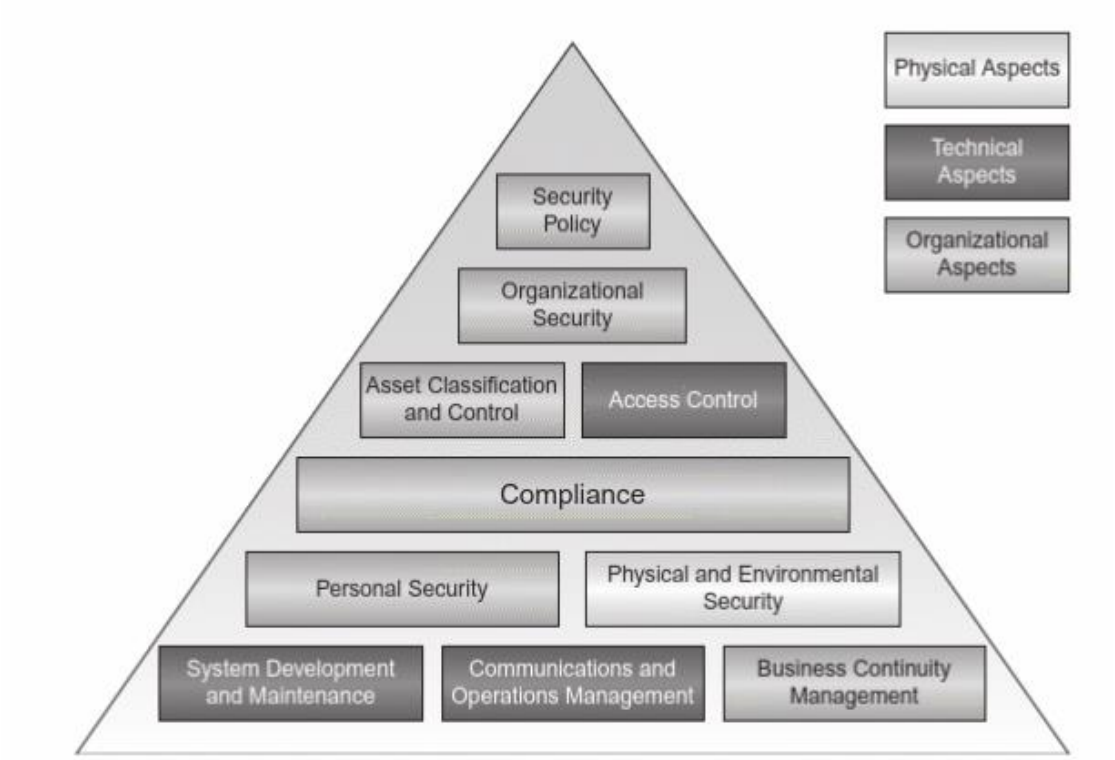
Information technology is a great help in cash management, but it is also dangerous if it is not kept secure. (Polak et al. 2018, p. 191) Though information is critical for companies' success of their business operations, very few companies have managed to keep their information secure and avoid unauthorized access or stop intrusions or prevent disclosure of secret information. In every computer related environment, security can be considered the most important. (Blanco 2014, p. 687)

Polak et al. suggest that for protecting treasury systems the company should encrypt messages, protect data against cyber-attacks, obtain ISO and other certifications, improve bank connectivity (get the most use out of SEPA standards and cash pool systems), remove all the paper documentation from the process, adopt standardized XML formats to secure systems access and provide 100% automation.

Information security management is important for organizations as the trend grows in many enterprises of moving all IT operations to cloud. The exponential growth of a global information economy means that an ever-increasing amount of personal data is collected, used, exchanged, analyzed, and retained in a global footprint of IT resources including databases, and cloud, virtualization, and big data sites. (Vacca et al. 2013, p. 1)

For information security managers, it is important to keep clear perspective of all the areas of business that require protection. Information security managers must collaborate with business units from employee training to research and development. One example of active cover is to protect data and files with different user rights and passwords. Also, a control of user rights and user administration with certain criteria helps companies to cover their data. Security model below describes guidelines and principles for initiating, implementing, maintaining, and improving information security management in an organization (Vacca et al. 2013, p.1 -2)

Figure 7 Security model (Vacca et al. 2013, p.79)



The user should be aware of the risk of device's or software's security, for example, not to hide written passwords under the keyboard. The difficulty to manage many identities discourages the use of identity management system. Weak passwords used by users on many web sites keep the number of successful attacks high. (Vacca et al. 2013, p. 79)

Single Sign-On (SSO) is the name given to the requirements of eliminating multiple password issues and dangerous password. When we use multiple user IDs and passwords just to use the e-mail systems and file servers at work, we feel the inconvenience that comes from having multiple identities. The second problem is the scattering of identity data which causes problems for the integration of IT systems. Moreover, it simplifies the end-user experience and enhances security via identity-based access technology. (Vacca et al. 2013, p. 79) The identity authentication is developing fast and techniques developed are image recognition, voice print recognition and biometric solutions like face recognition or EyePrint ID technology. (Zheng 2018, p. 6)

3 METHOD

The method is a case study based on five companies operating in Finland and globally. The purpose is to solve if digitalized solutions in companies' cash management help minimizing the risks identified in cash management.

3.1 Case study method

Case study is a research methodology, typically seen in social and life sciences. It can be defined as "a strategy for doing research which involves empirical investigation of particular phenomenon in real life context using multiple source of evidence". A case study allows the researcher to take a complex and broad topic, or phenomenon, and narrow it down into a manageable research question (why and how). (Saunders et al. 2007, p. 145-146). Myers specifies that *'The purpose of the case study research is to use empirical evidence from real people in real organizations to make an original contribution to knowledge'* (Myers 2009, p. 76)

The strength of the face-to-face interview is the richness of the communication that is possible. Questionnaire data can appear thin, abstract and superficial. A face-to-face interview should be used when most of the questions are mainly open and require an extended response with prompts and probes from interviewer to clarify the answers or if the material is sensitive in character so that trust is involved e.g. people disclose things in face-to-face interview that they don't disclose in anonymous. (Gilham 2000, p. 62)

In case study it is useful to have chain of evidence and maintain a case study database. The examples of different kind of evidence are documents, records, interviews, observations etc. It is also important that in case study it has been used multiple sources of evidence. (Gillham 2000, p. 20-21). That is why the author has used annual reports and company interviews in data collection.

Case study research has often been criticized on the grounds that its findings are not generalizable compared to survey research. If generalization is done in case

study, the following steps need to be taken: criteria is the necessity to demonstrate that the relevant phenomenon is identified and described in the collected data. This data must be presented in support of the relationship between phenomenon in line with the predictions of the theory. (Troman et al. 2005, p. 74)

3.1.1 Case study in chosen topic

Technology, automation and digitalization have helped companies to improve their efficiency and costs. It is obvious that there is no turning back on time before digitalization and that digitalization is changing continuously. There are different risks in companies and in cash management. Companies use technology to control the cash management: incoming and outgoing payments as well as forecasting liquidity. It is not only operational risk but also risks in the whole IT architecture and financial risks.

The literature part of the thesis has provided information related to cash management, digitalization of finance as well as risks. The study focuses to investigate five companies A, B, C, D and E that are listed companies and have global business or otherwise global cash management structure. Global business is relevant in cash management's perspective since there are more risks both financial and operative risks. The chosen companies are listed and therefore obliged by law that they need to describe their risks in the annual report it is obvious that the information is very general.

This case study collects data from annual reports (2017 and 2018) as well as companies' code of conduct and qualifies the risks and risk management by using qualitative method. The author has performed an open interview for deepening the understanding if digital solutions can help minimizing the risks in companies. The interview covers deeper information on how the processes work in risk management from cash management's perspective. It is problematic to show if the technology increase or minimize the risks in companies since the companies need to consider the risks from different perspectives. The study is conducted

anonymous since the risk management is a sensitive topic and it aims to protect companies from risks.

Reliability is a concept used for testing or evaluating quantitative research, the idea is most often used in all kinds of research. The most important test of any qualitative study is its quality. A good qualitative study can help us "understand a situation that would otherwise be enigmatic or confusing". This relates to the concept of a good quality research when reliability is a concept to evaluate quality in quantitative study with a "purpose of explaining" while quality concept in qualitative study has the purpose of "generating understanding".

Validity is described by a wide range of terms in qualitative studies. This concept is not a single, fixed or universal concept, but "rather a contingent construct, inescapably grounded in the processes and intentions of particular research methodologies and projects". Although some qualitative researchers have argued that the term validity is not applicable to qualitative research, but at the same time, they have realized the need for qualifying check or measure for their research. (Golafshani 2003, p. 602-603)

The ability to generalize findings to wider groups and circumstances is one of the most common tests of validity for quantitative research. Generalizability is one of the criteria for quality case studies depending on the case selected and studied. The way to achieve validity and reliability of a research get affected from the qualitative researchers' perspectives which are to eliminate bias and increase the researcher's truthfulness of a proposition about some social phenomenon using triangulation. Triangulation is defined to be "a validity procedure where researchers search for convergence among multiple and different sources of information to form themes or categories in a study". (Golafshani 2003, p. 601-604) In this Thesis the generalization is made of based on the data collected and interviewed of the five chosen case companies.

3.2 Companies interviewed for the study

3.2.1 Company A

Company A is a Finnish company in industrial business. In 2017 company's group net sales was approximately 384 million euros, with operations in more than 20 countries in Europe, Asia and USA. Company has almost 1,800 people employed globally and is one of the leading suppliers of industrial coatings. Company A has recently created a code of conduct for its employees which includes general company policies and guidelines for employees related to working conditions and recognizing corruption and fraud attempts. Every employee must take the code of conduct course, which is carried out in a digital format.

Though part of the risks is trusted outside the company – the company A also pointed out that not all auditors require for example that companies would show how are they setting the user rights or what kind of access policy the company has towards financial systems. Though there haven't appeared any frauds in the company this risk should not be transferred to auditors because the management is ultimately responsible of any misappropriations. (Interview A, January 2019)

3.2.2 Company B

Company B is Finnish listed company and a global leader in smart technologies for the marine and energy markets. In 2018, company B's net sales were 5.2 billion euros and it has approximately 19000 employees. The company has operations in more than 80 countries around the world. The company B has structured risk management process based on ISO31000 guidelines. (Company B annual report 2018, p. 157)

3.2.3 Company C

Company C is forest based industrial company listed in Finland and it has global business operations in 12 countries. The company's net sales in 2018 was 10.5 billion euros and the company have 19000 employees. Together with internal

control and risk management, the company makes sure that its operations are effective, that financial and other information are reliable, and that the company complies with the relevant regulations and operating principles. The internal control's risk frame is based on COSO model and the risk management operates in yearly cycle from planning to evaluation. Risk factors are classified as strategic risks, operational risks, financial risks and hazard risks. (Company C annual report 2018, p. 4, 22)

3.2.4 Company D

This is an IT company focusing on computer hardware, software, hosting and consulting fields as well as it has its own research and analysis activities. In Finland this is a subsidiary that has a parent company in US (listed in NYSE). Company's net sales in 2017 was 79.139 billion dollars. The number of employees was 366000 and the company operates in 170 countries. Management conducted an evaluation of the effectiveness of internal control over financial reporting based on the COSO model. (Company D annual report 2018, p. 2, 68) The company in Finland experiences the internal audit process so that it is basically business control that contains lot of proactivity and testing. First there are peer review and friendly audit and if something appears the internal audit steps in. (Interview D, February 2019)

3.2.5 Company E

Company E is a North European construction company listed on Nasdaq Helsinki. It has more than 10000 employees and the company operates in 11 countries. The revenue for 2017 was 3.8 billion euros. The Group's President and CEO retains overall responsibility for risk management. The heads of business segments and support functions identify, assess and monitor the major risks facing their respective areas of responsibility, draw up contingency plans for those risks and attend to the implementation and supervision of risk management. Financial management is responsible for the financial risks. The Group's internal audit organization

supports management in ensuring the effectiveness of risk management and internal control. (Company E annual report 2017, p. 5)

4 ANALYSIS AND RESULTS

As a result of the literature review and comparing the collected information from case companies, i.e. data from annual reports and interviews, the author presents the results related to research questions. The first question was: *"What kind of risks the companies need to deal with in cash management?".* Under this question the author has presented results with subtitle Risks in cash management that contains operational risks and financial risks related to the companies' liquidity planning, interest and currency risks and credit risks. Then under the second research question: "*Can digitalization help minimize these risks?"* the author has gathered the results under the subtitle Digitalization in cash management.

The author categorizes digital solutions in finance into traditional ones that are already settled to listed companies operating globally and to new ones that many companies are looking as an option but not yet taking into a wide use. Traditional digital solutions are ERP, electronic banking, banking software and cash pool solution. The new ones are more added services that can of course be integrated to the existing solutions like AI and block chain and functioning in SaaS. The new ones are presented under the chapter Future cash management though many of the new solutions have been in use in companies many years.

4.1 Risks in cash management

The companies in the study had identified risks in the annual reports. Almost all the companies told that their risk identification was based on the risk management frame (e.g. COSO or ISO31000 model). The companies also had defined their own code of conduct for supporting their risk management.

In general, the results show that there are similarities and differences between case companies. Though the author had identified the operational risks and financial

risks the closest to cash management risks – a comment from one case company was that none of the risks that are mentioned in for example in annual report cannot exclude, since all company risks are affecting the risks in cash management one way or another. (Interview B, February 2019) Other risks that were mentioned in addition to operational risks were political risk, accounting risk, manufacturing, supplier and sub-contractor risk, life cycle risk and contractual risk. Company E mentioned also the accounting risk among the risks in cash management since if the company has lot of receivables, it has a negative impact on company's balance and that can cause issues with ratings and investors. (Interview E, February 2019)

4.1.1 Operational risks

Company A focuses on group level control in cash management. The accounts are concentrated under the group's supervision by the help of cash pools. The control follows the four-eye principle which means nobody can alone create a payment, accept it and send it to the bank. There haven't been any major disturbances related to technology. Company A does not use any extra data protection like file encrypting or neither it uses extra security SSO or MFA in accessing to financial system. The company doesn't have any manual or specific instructions for user rights or access policy. (Interview A, January 2019)

The cyber risk instead is something that company needs to pay attention and company's IT is responsible for that. There haven't appeared any frauds in the company but Company A trusts that auditing people are looking after that risks effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations are being followed in the company. (Interview A, January 2019)

Operational risks play important role in Company B's cash management. The potential loss expectancy is highest with strategic and operational risks and lowest with hazard and financial risks. (Company B annual report 2017, p. 132) These risks can be manufacturing risk, supplier and sub-contractor risk, life cycle risk, contractual risk of the product, corruption and fraud, cyber and information

security risk as well as price risk. (Company B annual report 2017, p. 136) None of these risks can exclude when considering cash management. For example, if delivering a system for financial purposes and it doesn't work it is a big financial risk. Or considering that a bank would have a system disorder and in case of a big project where the purpose is to ship a big delivery but due to bank the shipper won't get the prepayment in time. This leads to situation where the supplier won't ship the product and this can cause the entire transaction to be discharged, which then causes the liquidity damages and the damage can be big. (Interview B, February 2019)

Centralizing payments to shared service center reduces also the number of users and helps to monitor user rights and user behavior. The company B can't comment their cyber risk related issues, but the company has a department managing and supervising cyber and information security risks as well as they communicate the risks in cooperation with Treasury Department. (Interview B, February 2019)

Company C has developed and implemented a comprehensive internal control system that covers business and financial reporting processes. Internal control is aimed at ensuring that the company's operations are efficient and reliable. (Company C annual report 2018, p. 107) Company C has included its operational risks e.g. supply chain management, project execution, partnerships, availability and security of information systems and non-compliance in operations and supply chain. (Company C annual report 2018, p. 107)

Company C's information security risk is monitored by the separate IT Security Department but of course the communication between finance and IT is at good level. The company hasn't experienced major disturbances in the information security. The most common problems have related to banks and the cash management processes are tightly scheduled and if something cause a delay, everything is then delayed. (Interview C, February 2019)

Part of the systems the customer is using SSO but not for all the systems. It is more important to focus that the channels where e.g. payment files are sent is secure. The access policy is outsourced into a separate system and the customer is following four eyes principle in payments. Also, all the financial roles related to ERP are thoroughly planned. The automation in cash management processes and between different programs minimizes the operational risks. (Interview C, February 2019)

Company D performs ongoing assessments regarding its technical controls and its methods for identifying emerging risks related to cybersecurity. The company also has a security monitoring program and a global incident response process to respond to cybersecurity threats and attacks. In addition, the company utilizes a combination of online training and other tools to foster a culture of security awareness and responsibility among its workforce. (Company D annual report 2018, p. 87) The security is in the company's business DNA. Everything is built inside the security layer. (Interview D, February 2019)

Company D follows concentration policy in cash management which means that European payment traffic is concentrated on one of the group's treasury centers. The company D has started to develop centralization (from 1990s) and purchase to pay solution has been in use ever since. That is integrated into ERP and starts from catalog where you can place an order and through acceptance process it finally is paid out from the external bank account through TARGET2. By concentrating global cash management to treasury has helped minimizing the hazard risks and the control of payments. (Interview D, February 2019) In payments there are always four-eyes principle and in manual payments six-eyes principle. Salary payments are also concentrated already 10 years ago. User rights and access rights are applicable in separate portal. When logging into financial system it requires authentication (e.g. SSO).

Company E assess operational risks monthly. Project management plays important role in minimizing the operational risks. (Company E annual report 2017, p. 56) Company E has transfer pricing policy which instructs employees how to

establish customer relationship, checking the credit reports history and background check from Reuters (KYC, political exposure or sanction list). Company E takes seriously that the bank account number should not be changed and if this needs to be changed it is behind strong authentication and access rights. (Interview E, February 2019)

The company hasn't experienced major disturbances in their IT systems. It has separate Security Department to maintain IT security but for cash management the risks are being followed mainly Treasury Department. Due to merger the company has different IT solutions and platforms, but critical systems are under control though there are some ongoing projects to concentrate and develop IT and financial systems. (Interview E, February 2019)

Company E has minimized operational risks of its subsidiaries by using inhouse bank solution and avoiding manual payments in subsidiaries. If there is a need for manual payments the treasury handles them concentrated. The company is following strict policy in payments and nobody can make single payments without somebody's approval. SSO is actively used in the financial systems. Also warehousing and project management have their own software systems. (Interview E, February 2019)

Access policy is concentrated to HR Department which forwards the requests to correct managers that then define the access rights for example to financial systems. These rights are monitored on yearly basis. Company E doesn't have concentrated financial systems like one ERP, but it has a goal to concentrate all the financials into core ERP system. Authentication is important and almost all financial systems are under SSO. If an employee leaves the company the access rights are right away deleted. (Interview E, February 2019)

4.1.2 Liquidity risk

Company A is well prepared for the liquidity. They know precisely their business cycles and can forecast the cash flows at one-year level. For example, in spring

company receives lot of orders, customers have long terms of payment and the company has production costs. To cover the shortage of liquidity the company uses their cash pools, or the company takes a short-term financing from bank through commercial paper solution. Company A does not experience a volatility at daily level and all outgoing payments fit inside the limits. (Interview A, January 2019)

Company B is managing the liquidity risk with making sure that the company's financing is at trusted level. Though the company hasn't any official rating, its customers are evaluating the company by its financial figures. The company B is having so called revolving finance to cover the negative cash flows. The cash flows are usually negative at the beginning of the year changing to positive towards end of the year. Any major financial decisions are not done based on short term receivables. In this since the company doesn't need a short-term liquidity forecasting except for subsidiary reporting purposes. (Interview B, February 2019) In annual report 2017 p. 226 the company states that: "*the company always ensures liquidity by efficient cash management and by maintaining sufficient committed and uncommitted credit lines available. Refinancing risk is managed by having a balanced and sufficiently long loan portfolio."*

Company C states that liquidity risk is managed by efficient cash management and restricting financial investments to investment types that can readily be converted into cash. (Company C annual report 2017, p. 152) Business units are doing cash forecasting for the group. This is partly automated (AP, AR from ERP) and rest is done manually. The reporting is also automated to a separate treasury system. (Interview C, February 2019)

Company D's liquidity risk is monitored continuously, and it may discontinue some of the hedging relationships by e-designating or terminating the derivative instrument in order to manage the liquidity risk. (Company D annual report 2017, p. 98) According to company D the treasury takes care that there is always enough funding on the accounts. The Treasury Department follows automated reports and

the liquidity is managed by efficient payment solution, i.e. inhouse cash solution and concentrated source to pay solution. (Interview D, February 2019)

The management of company E continuously evaluates and monitors the amount of funding required by the Group's business activities to ensure adequate liquid funds to finance its operations, repay its loans at maturity and to finance dividend. The Group Treasury is responsible for the adequacy of funding, the availability of different sources of funding and the controlled maturity profile of external loans. The funding requirements are evaluated based on financial budget prepared half yearly, monthly financial forecast and short-term, timely cash planning. (Company E annual report 2017, p. 149) There is a separate system for treasury and liquidity forecasts. Cash forecast is performed partly automatically, AP and AR reports can be fetched from ERP and e.g. salaries can be manually put into reports. None of the investments can be executed without management's approval. (Interview E, February 2019)

4.1.3 Credit risk

Company A's credit risk is being managed by strict credit policy and active debt collection. (Company A annual report 2018, p. 2) This happens also by the help of ERP system. The company monitors account receivables and customer behavior on a monthly and yearly basis. By taking out reports and setting alarms if due dates exceeds 15 days or 30 days and more the company can require prepayment from customer who haven't paid in time before. Company has considered factoring solution but hasn't taken it into use. Accounts payables are always paid on the due date. (Interview A, January 2019)

Company B's credit risk is managed by evaluating the vendors and doing business with highly rated banks. The working capital is optimized but, in this case, monitoring short term receivables and payables don't play that important role. More important is to agree with the payment terms and conditions and using trade finance products like reimburses. This reduce the counterparty risk. Making a reimburse happens so that a buyer makes a reimburse with its own bank and the

bank delivers the reimburse to vendor's bank. In this case the company B can get the reimburse by e-mail from its bank. In this case the company B evaluates that using e-mail for reimburse confirmation is a good thing from efficiency's perspective. For bank guarantees the company has a separate banking software system. Interest risk is managed by following the loan balance and by hedging. (Interview B, February 2019)

The company C has a credit risk policy and credit insurances to protect accounts receivables from significant credit losses. Outstanding trade receivables are monitored on monthly basis. Customer credit limits are established, and ongoing evaluations of their financial conditions are performed. (Company C annual report 2017, p.153) Purchase Department defines payment terms and Sales Department defines cash discounts, which is optimal in terms of working capital. (Interview C, February 2019)

Company D has a long-standing practice of taking mitigation actions, in certain circumstances, to transfer credit risk to third parties, including credit insurance, financial guarantees, nonrecourse borrowings, transfers of receivables recorded as true sales in accordance with accounting guidance or sales of equipment under operating lease. Company D is also following Moody's ratings for counterparties. (Company D annual report 2017, p. 38, 106) For the suppliers the company tries to set long payment terms and from customers the company wants to have cash in quickly. (Interview D, February 2019)

In company E credit risk management is carried out in the Finance Department. Accounts receivables are followed in ERP and reported to the group that manages credit risk related to operating items by holding the ownership of project constructions until payment is received, taking advance payments, accelerated payment programs of projects, guarantees, site-specific mortgages, credit risk insurance policies; and careful examination of clients' background information. In addition, selling of receivables to financial institutions is used in the management of the credit risk of operations. (Company E annual report 2017, p. 147)

4.1.4 Currency risk and interest rate risk

Company A protects the currency risk by the policy that all receivables in foreign currency must be covered by derivatives (forward contracts). The operative cash flows and own equity are not protected but cash pool accounts help in protecting from currency risk. Interest risk has been noticed in the company's policy and according to that 20-50% of all loans are tied to fixed interest loans. Rest of the loans are implemented by using interest swaps. (Interview A, January 2019)

The currency risk in the company B is at high level since the company operates in so many countries. Main protection against currency risk is covering with derivatives. The company is following currency risk and minimizing the risk by hedging. If hedging happens at subsidiary level the group treasury is acting as a counterparty. (Company B annual report 2018, p. 252) But there are countries involved where covering with derivatives might be useless because of regulation or political risk. In these cases, the company follows the currency fluctuation and delegates the risk to the business unit and by this procedure they can cumulate the risk into bigger units. The company B hasn't used virtual currencies because it would be too big risk to speculate with virtual currency value. Interest risk is managed by following the loan balance and by hedging. (Interview B, February 2019)

Company C's currency risk comes from future payment flows (transaction exposure) and from changes in value of recognized assets and liabilities in foreign currency and from changes in the value of assets and liabilities in foreign subsidiaries (translation exposure). The goal is to limit the uncertainty created by changes in foreign exchange rates on the future value of cash flows earnings and in the group's balance sheet. The group's policy is to hedge 50% of its estimated net risk currency cash flow. (Company C annual report 2017, p. 117) Business units are creating automated forecasts of their AR's and AP's and then the group can net the outgoing and incoming currencies and make FX trades in separate FX trade system. For the interest rate risk, the company maintain a certain profile with interest rate derivatives (swaps and futures) to change net debt duration. (Interview C, February 2019)

As a result, the company D does not anticipate any material losses from these risks. The company's debt, in support of the Global Financing business and the geographic breadth of the company's operations, contains an element of market risk from changes in interest and currency rates. The company uses financial hedging instruments to limit specific currency risks related to financing transactions and other foreign currency-based transactions. The company also maintains currency hedging programs for cash management purposes which temporarily mitigate, but do not eliminate, the volatility of currency impacts on the company's financial results. In addition to currency and interest rate risk the company recognizes a risk related to collectability of accounts receivables. To meet disclosure requirements, the company performs a sensitivity analysis to determine the effects that market risk exposures may have on the fair values of the company's debt and other financial instruments. (Company D annual report 2018, p. 66)

Interest risk arises mainly from the company E's current and non-current loans and related interest rate derivatives. (Company E annual report 2017, p. 146) Interest rate risk is hedged by interest rate derivatives (e.g. swaps). The currency risk is managed by hedging. The group treasury hedges the net position and takes care of all external hedging transactions and keeps only one position per currency. The company uses a separate FX deal system where they can make FX trade with different banks. (Interview E February 2019)

4.2 Digitalization in cash management

Company A had renewed their cash management process three years ago and it concentrated its accounts to two banks under the group's supervision by the help of cash pools. Company A has one ERP centralized for all units – only few units abroad don't use the same ERP and have their own book keeping. ERP is ten years old and the company has updating project ongoing. Company A uses also a banking software for sending payments to banks and settling payments with book keeping. Banking software is in SaaS. From treasury's perspective the best view of the

company's overall balance can be seen from internet bank's cash pool accounts (real-time, internal transactions and limits). (Interview A, January 2019)

The company A thinks that automation in financial processes helps their employees to focus on their relevant tasks. Cash pool structure plays important role in company's global business processes as well as ERP related to the receivables. ERP is soon to be updated so the company focuses to keep their systems practical and modern. Updating new systems have been painful projects but it has helped the company to perform their tasks better. (Interview A, January 2019)

Company B's cash management is centralized to share service center and they are highly dependent on using one ERP solution. The company is also having inhouse cash in ERP and cash pools from banks – though the inhouse cash is considered the most important. Only few accounts are outside inhouse cash because of political or regular reasons. Company B has invested in robotics and it uses in its routine tasks in financial operations. RPA helps in reducing human errors. Centralizing payments to shared service center reduces also the number of users and helps to monitor user rights and user behavior. (Interview B, February 2019)

Company C has different financial systems related to cash management (internet banks, ERPs, treasury system, cash forecasting system) but the main core system is ERP and SWIFT. Company's focus is in one core system and it aims to reduce the amount of manual payments. The company is using internet banks for monitoring incoming payments. Some of the company C's systems are in SaaS but not all. Same goes with accessing into systems – part of the systems the customer is using SSO but not for all the systems. It is more important to focus that the channels where e.g. payment files are sent is secure. (Interview C, February 2019)

In Finland Company C is executing group's policy in cash management which means that payments traffic is concentrated on one of the group's treasury center in Ireland. The company D has started to develop centralization (from 1990s) and purchase to pay solution has been in use ever since. That is integrated into ERP and starts from catalog where you can place an order and through acceptance

process it finally is paid out from the external bank account through TARGET2. (Interview C, February 2019)

The company E is having several ERP systems, but the goal is to concentrate everything into one system. In addition, the company is using a banking software for payments, internet banks for the cash pools and monitoring the incoming payments and separate treasury system. The company has focused in minimizing risks in subsidiaries by using inhouse bank solution and avoiding manual payments in subsidiaries. If there is a need for manual payments the treasury will do it concentrated. (Interview E, February 2019)

4.2.1 Future cash management

The company A believes in traditional cash management systems and to automation. Company's ERP is soon to be updated so the company focuses to keep their systems practical and modern. Company A does not use any extra data protection like file encrypting or neither it uses extra security SSO or MFA in accessing to financial system. Company A uses a separate banking software for payments that is in SaaS. Robotics and AI is not utilized unless automatic posting is counted as robotics and the company does not see these necessary. (Interview A, January 2019)

Company B has invested in robotics and it uses in its routine tasks in financial operations. RPA helps in reducing human errors. Centralizing payments to shared service center reduces also the number of users and helps to monitor user rights and user behavior. Company B has centralized ERP that is not yet in SaaS. (Interview B, February 2019)

The company C is neither using robotics nor AI in their cash management. The more important focus is in automation between different systems. When processes are automated like cash flows and payment transactions the risks are smaller (operational risks, financial risks) in cash management. (Interview C, February 2019)

Company D has automated their cash management many years ago. Its cash management is based on to purchase to pay solution that is fully automated. The company uses also inhouse cash solution to avoid too many bank accounts. The access into financial system is fully covered and requires authentication and access rights. Company D has used robotics for example in accounting already from the 90's and today it has reporting tool which uses also AI (Cognos) to be more accurate and efficient.

Company E is using AI already in salary related payments (e.g. calculating sales bonuses) but the company wants to have more focus in AI in the future. These types of AI could be automatic matching and payment anomalies. Robotic will be the future when talking about combining different systems like taking numbers from different reports for the budgeting tool etc. (Interview E, February 2019)

5 CONCLUSIONS

The research questions were:

1. What kind of risks the companies deal with in cash management?
2. Can digitalization help reduce these risks?

5.1 Risks that companies have in cash management

5.1.1 Operational risks

In the organization there can be several units that are responsible for operational risks mentioned above like Accounting Department, Internal Audit, IT, Risk Management, Operations Department etc. (Angelache 2011, p. 66) However this was run differently in many of the companies. The bigger the company was by its size the stricter the risks were managed from the top.

An example of active cover is to protect data and files with different user rights and passwords. Also, a control of user rights and user administration with certain criteria helps companies to cover their data. (Vacca et al. 2013, p.1 -2) User right

management was strictly thought through almost in all case companies. Three of the case companies told that the company had separate access management portal where employees could apply user rights to cash management systems. (Interviews C, D and E) Almost all the companies had processes in place for related to user rights. In every company they had so called four eyes principle at least that nobody could make payments without someone else acceptance. Three of the case companies were using some additional security services in cash management related to user right management like SSO. (Interviews C, D and E).

The information security risk was considered highly important among all the interviewees. All the companies had IT Information Department with security people involved. The cyber risk was listed as a growing risk, but it was also something that not all the interviewees were able or allowed to comment. None of the case companies had experienced major disturbances in their information systems but all considered the possible disturbances as big risk from cash management's perspective. For example, if a bank would have a system disorder and in case of a big project where the purpose is to ship a big delivery but due to bank the shipper won't get the prepayment in time. This leads to situation where the supplier won't ship the product and this can cause the entire transaction to be discharged, which then causes the liquidity damages and the damage can be big.

When talking about cash management related risks – half of the case companies were instructing risk management people in cash management risks as well as they were advising internal auditors. Four of the case companies had separate Risk Management Department that conducted and controlled regularly the risks at general level. In these case companies the internal auditor role was more to help and supportive. If something suspicious came out, then the internal role could emphasize.

What comes to internal or external frauds – this is a question that none of the case companies could comment. Since a listed company is obligated to announce if it has faced fraudulent action that affect to company's financial result

(Security Markets Act 746/2012 1/4§) – two case company reported of frauds in 2018 (none of the cases was related to corruption).

Three of the case companies told they were encrypting their payment files when sending those to banks but not all the case companies could answer to this question. One of the respondents told that this is a requirement from the SWIFT. Two companies wanted to specify that it is even more important to focus on the actual channels where the payment files are being sent and that the channel must be secure.

All the interviewees agreed that automation in cash management processes helped minimizing the operational risk. The concentration in cash management and payments transactions was the key word when considering minimizing and managing risks in cash management.

5.1.2 Liquidity risk

To liquidity risk the company can affect by optimizing account payables e.g. using cash discount or paying on the last due date and with cash forecasting. (Niskanen 2016, p. 399, 327) Three of the interviewees highlighted that it was also easy and cheap to get short-term financing from the bank and this was not a big risk if the account balance was negative. It was important to make sure that the company financing is at trusted level. The importance of cash flow optimization varied between the case companies. All case companies knew at general level the company's cash flow situation but two of the case companies commented that no investments could be done before checking the forecasts first. Three of the case companies had automated cash forecasting and two of the companies made forecasting at least half manually (putting numbers manually or using excel).

5.1.3 Credit risk

Account payables (AP's) and account receivables (AR's) optimization had different focus among the interviewed companies. The companies that have big transaction volumes are more dependent on the optimization of AR's and AP's than the companies that are selling less products but then the trade value is bigger. Still four of the case companies considered that the payment terms and AR and AP optimization were important in terms of working capital. All case companies were able to follow AR and AP from ERP system.

Trade finance products and guarantees for the bigger and valuable products and the optimization like negotiating payment terms or cash discount were more for the companies with bigger transaction volumes. Two of the case companies were using outsourced debt collection or factoring for their AR collection purposes.

5.1.4 Currency risk and interest rate risk

Companies can cover from currency risks by using solutions like netting or making derivatives. (Niskanen 2016, p. 431-432) To manage the interest rate risk all case companies were following closely their loan balances or using swaps or interest rates futures. In terms of currency risks all the case companies were monitoring their currency exposures regularly. The currency risk was minimized mainly with hedging. All the bigger trades were covered by derivatives. The method to make derivative trades was varying between companies. Some of them had online systems and there were ones that were calling or e-mailing directly to bank to their contact.

To avoid currency risk two of the case companies considered it is important to follow AP and AR cash forecasting by currencies so that that the company can react in time and make only one currency trade and then share the value to its units. Currency risk is mostly mentioned in GBP, USD and JPY. Transaction exposure and translation exposures are both mentioned in three of the case companies' annual reports. Cancellation of orders was mentioned as a risk factor that

could lead to ineffective currency hedges. A political risk is also mentioned when thinking about currency risks.

5.2 Can digitalization help minimize risks in cash management?

Based on the results of the study it can be stated that the digitalization in cash management helps companies to manage risks. Specially the operational risks related to human errors. In financial risks the cash forecasting, optimizing cash flows and using e.g. netting, cash pools, inhouse banks were helping to minimize the currency risks. Also, different online systems enabled quicker and cheaper FX deals (tenders between banks).

The companies can manage their risks both operational and financial risks also by thorough planning. By using risk models like COSO or ISO31000 frames and leading the risk management planning down to organization and doing active monitoring the companies can avoid big risks in cash management. The traditional ways of performing cash management by having ERP and using for example internet banks and making sure that for the financial systems there are clear user roles and access rights.

Concentrating financial transactions into one unit makes monitoring risks and user right management easier and more scalable. The automation is key word between different systems. The RPA already has influence in couple of companies and focusing on RPA in the future would help companies also to manage risks in cash management. When getting more reliable numbers to reports it will help companies to make decisions and react faster. The Author is convinced that RPA is going to be something that companies will be adapting more and more in the future.

By transferring financial systems to SaaS, it gives good protection to companies' information security. Also protecting data like payment files is important. Companies can outsource their information security for companies that are specialized to protect data security. The bigger risk is that the company must know

what kind of tasks their employees are doing with its systems. The employees that are not experts in cyber security or information security issues but are handling company's assets must have clear process and tasks to make sure that no operational or financial risk can expose.

There are several digital solutions that can help companies manage financial risks. In credit risk related issues companies can use for example a digital solution for KYC purposes when estimating customer's credit and trustworthy. For liquidity risk the companies can use different kind of automated cash forecasting systems or collecting automatic reports from different systems to a treasury system. AP and AR optimization can be done from ERP or taking AP and AR materials to a separate cash forecasting system. Factoring and debt collection can be automated or outsourced. For currency risk the companies can use online trading platforms as well as internally they can have inhouse bank solutions, netting and cash pools.

Though not all the case companies were yet using AI in their financial purposes this is going to be the future. If companies want to reduce manual work, get more accurate data for their reports and get alerts of the suspicious transactions (fraud detection), the AI would be the solution that would make this possible. According to Gartner's blockchain hype curve, the blockchain will be more stabilized in two to five years of time.

New ideas for the future studies could be taking advantages of AI in finance, how RPA reduces the risks in cash management or is using blockchain or virtual currencies a risk factor or an opportunity? Like all bigger companies, all case companies had ERP but few of the case companies had more than one ERP, still focus on one core system. Only one of the case companies had a pure purchase to pay solution where almost all the transactions flew automatically in the system from the purchase to a payment. All the companies had already some of the financial solutions (e.g. banking software) in SaaS and this is a trend where all the financial solutions are moving.

Two of the respondents had already plans to update their ERP and the author is assuming that all new ERP updates concern at least a hybrid SaaS model where part of the ERP stays on-premise and part of the data is moved to SaaS. Migrating ERP to SaaS is arguably more involved than migrating an edge system such as customer relationship management, which deals only with one aspect of how an enterprise function. While adopting the cloud, some organizations will prioritize by separating and migrating some modules or functions to the cloud first (such as human capital management), while the remainder continue to stay on-premise. (Accenture 2019 ERP trends, p. 12)

Online banks were also used though all the companies were trying to avoid manual payments via online banks. Some of the treasury people thought the online banks were necessary to follow real time balances. Especially when company used bank's cash pool, following balances via online bank was necessary, since banks won't even send the group account's balances anywhere. Though this might change when PSD2 will be fully applicable on 14th of September 2019. As the result of this research the author can say that internet bank is mainly kept for having bank accounts and following online balance. Cash pools are also for following group account balances and for the financial purposes (loans) but the actual payment traffic has been outsourced and concentrated already long time ago.

Three of the case companies told that they were using a separate treasury system where the company's balances were collected, and it was an important tool in managing financial risks. All case companies had also cash pools from banks and three case companies were using additionally inhouse banking solution. The benefit from inhouse bank was that the parent company was able to control that from which external bank account the payments should be paid (easier to control which bank account had enough balance).

All the interviewees were really thinking that the best risk management for cash management was automation and concentrating the payments into one place. Then also managing user rights were easier. Process planning in cash

management was considered valuable and if something was delayed during the day the whole process was delayed and this was a risk both from information security risk's side as well as financial risk.

AI was considered to be used mainly when talking about for example automatic posting rules (book keeping) among three of the case companies. This is basically not AI because the system is not learning anything – the user only sets certain criteria to the system that then recognizes where transactions need to be booked. As one example, it was mentioned a budgeting tool that makes the reporting data more trusted and reporting and analyzing can be done much faster. (Interview D, February 2019)

Three of the respondents thought that using AI in cash management will be increasing in the future. One of the case companies thought it could be helpful when recognizing payment anomalies and other gave an example that the AI could help in checking double invoices. Two of the case companies did not see that they could get advantage of using AI but instead they thought the automation is the key and straight through processes (STP) will bring more efficiency and less human errors. (Interviews A and C)

Three of the case companies were actively using robotics and in cash management processes for example, in reporting and paying salaries. One case company had developed robotic systems for their accounting purposes already at the 90's. (Interview D, February 2019) Limit goes mostly there that a robot is not allowed to execute payments. (Interview E, February 2019) Two of the respondents thought that they didn't need the robotics. Though automation can be partly considered as robotics like communication between different systems, monitoring and reporting, the interpretation of RPA and automation might be confusing. (Seasongood 2016, p. 32)

None of the case companies were using yet virtual currencies (like Bitcoin). One case company commented that this would be a big risk since the volatility is so high that the company cannot speculate with currencies. (Interview B, February

2019) One case company is developing and selling blockchain solutions related to supply chain and cross-border transactions, but the company can't comment if they are using these solutions to their own purposes as well. (Interview D, February 2019)

Like already stated the digitalization in cash management can reduce operational risks. Automation and different digital solutions minimize the number of human mistakes, frauds and misappropriations and give more accurate numbers for reporting. Digitalization also helps in minimizing financial risks like different solutions in liquidity forecasting, platforms for online FX trading, debt collection or customer evaluation or purchase to pay solutions. Risks in cash management can be still minimize also with thorough planning and monitoring.

Referring to Zheng et al. 2018 many of the interviewed companies were already adopting at least part of Fintech 3.0 phase with smart finance that combines internet finance, Big Data to achieve accurate calculation and includes blockchain, cloud or other emerging technologies. Still it would be interesting to see if the companies are adopting in few years of time for example the Bolton's model of fraud detection (Bolton et al. 2002, p. 235-249) or AI together with Big Data to assess consumer credit risks (Khandani et al. 2010, p. 47).

REFERENCES

Abbadi, Imad M. Cloud Management and Security, John Wiley & Sons, Incorporated, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/arcada-ebooks/detail.action?docID=1701403. Created from arcada-ebooks on 2018-10-17 03:56:09.

Accenture. 2019 ERP trends. Available at: https://www.accenture.com/_acnmedia/PDF-90/Accenture-Unleashing-Exponential-Evolution-PDF.pdf Accessed 2.4.2019.

Accounting Act 1336/1997. (3:1.5§) http://www.finlex.fi/en/laki/kaannokset/1997/en19971336?search%5Btype%5D=pika&search%5Bpika%5D=Accounting. Accessed 3.11.2018.

Ágoston, K. C. 2016. Pareto improvement and joint cash management optimisation for banks and cash-in-transit firms. *European Journal of Operational Research, 254*(3), pp. 1074-1082.

Ahokas, N. 2012. Yrityksen sisäinen valvonta. Jyväskylä: Edita Oy.

Altin Gumussoy, C. 2016. Usability guideline for banking software design. *Computers in Human Behavior*, 62, pp. 277-285.

Anghelache, G. 2011. Operational Risk Modeling. Theoretical and Applied Economics, XVIII(6), pp. 63-72.

Association of Certified Fraud Examiners. *Report to the Nations on Occupational Fraud and Abuse.* https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf. Accessed 2.8.2018.

Bashir, I. 2017. Mastering blockchain: Distributed ledgers, decentralization and smart contracts explained. Birmingham, [England] ; Mumbai, [India]: Packt.

Blanco, C. 2014. Security in Information Systems: Advances and New Challenges. *Computer Standards & Interfaces,* 36(4), pp. 687-688

Bolton, Richard J., and David J. Hand. “Statistical Fraud Detection: A Review.” *Statistical Science*, vol. 17, no. 3, 2002, pp. 235–249. JSTOR, www.jstor.org/stable/3182781.

Bose/Gapgemini and Denis/BNB Paribas. 2018. World Payment Report. Accessed at: https://worldpaymentsreport.com/ 1.11.2018.

Bragg, Steven M. Treasury Management: The Practitioner's Guide, John Wiley & Sons, Incorporated, 2010. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/arcada-ebooks/detail.action?docID=487670.

Cox, D 2014, Handbook of Anti-Money Laundering, John Wiley & Sons, Incorporated, New York. Available from: ProQuest Ebook Central. [18 March 2019].

COSO 2013, Available: https://www.coso.org/Pages/ic.aspx. Accessed 2.8.2018.

Created from arcada-ebooks on 2018-10-12 06:54:04.

Dandapani, K. 2017. Electronic finance – recent developments. *Managerial Finance, 43*(5), pp. 614-626.

European Banking Authrority. EBA risk assessment report 2017. https://www.eba.europa.eu/risk-analysis-and-data/risk-assessment-reports. Accessed 11.10.2018.

European Central Bank. SEPA key facts 2019. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en. Accessed 11.4.2019.

European Community Council Regulation, No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995R2988:EN:HTML. Accessed 15.9.2018.

Farquhar, J 2012, What is case study research? SAGE Publications Ltd, London, pp. 3-14, [Accessed 23 January 2019], https://dx.doi.org.ezproxy.uef.fi:2048/10.4135/9781446287910.n2

Finnish Limited Liability Companies Act 21.7.2006/624. https://www.finlex.fi/fi/laki/ajantasa/2006/20060624?search%5Btype%5D=pika&search%5Bpika%5D=osakeyhti%C3%B6#L6P1. Accessed 3.8.2018.

Francisco Salas-Molina, Juan A. Rodriguez-Aguilar and Pablo Díaz-García. Selecting cash management models from a multiobjective perspective. Published online: 6 September 2017, Springer Science+Business Media, LLC 2017. Ann Oper Res (2018) 261:275–288 https://doi.org/10.1007/s10479-017-2634-9.

Gillham, B 2000, Case Study Research Methods, Bloomsbury Publishing PLC, London. Available from: ProQuest Ebook Central. [15 January 2019].

Golafshani Nahid, 2003. The Qualitative Report Volume 8 Number 4 December 2003 597-607 http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf.

Gomber, P. 2017. Digital Finance and FinTech: Current research and future research directions. Journal of Business Economics, 87(5), pp. 537-580.
Accessed at: https://doi-org.ezproxy.arcada.fi:2443/10.1007/s11573-017-0852-x. 18.11.2018

Gore, R. 2017. Markov Chain modeling of cyber threats. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 14*(3), pp. 233-244.

Harward Business Review, June 2012. Kaplan and Mikes. https://hbr.org/2012/06/managing-risks-a-new-framework. Accessed 23.9.2018.

Harward Business Review, November 2014. Porter & Heppelman, *How Smart Connected Products Are Transforming Competition*, pp.65-88.

Iivarinen, T. 2003. *Regulation and control of payment system risks: A Finnish perspective*. Helsinki: Bank of Finland.

Jie, F. 2002. How Can Every Organization Manage the Operational Risk? Journal the Winners: Economics, Business, Management, and Information System Journal, 3(1), pp. 88-103.

Jones, M. Tim. AI Application Programming, Charles River Media, 2003. ProQuest Ebook Central, https://ebookcentral-proquest-com.ezproxy.arcada.fi:2443/lib/arcada-ebooks/detail.action?docID=3135671.

Khalid, Zahid. Optimizing Back Office Operations: Best Practices to Maximize Profitability, John Wiley & Sons, Incorporated, 2010. ProQuest Ebook Central, https://ebookcentral-proquest-com.ezproxy.arcada.fi:2443/lib/arcada-ebooks/detail.action?docID=487690.

Khandani, Amir E., Adlar J. Kim, and Andrew W. Lo. “Consumer credit-risk models via machine-learning algorithms.” Journal of Banking & Finance 34 (2010): 2767-2787

Koivu, Ranta-Aho, Vuoti. 2010. Väärinkäytösriskit hallintaan. Tietosanoma Oy. ISBN 978-951-885-316-2.

Levy H.B. 2018. The Reality of Blockchain. Accessed at: https://blogs.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/. 20.11.2018.

Louisot, J, & Ketcham, CH 2014, ERM - Enterprise Risk Management: Issues and Cases, John Wiley & Sons, Incorporated, Somerset. Available from: ProQuest Ebook Central. [9 April 2019].

M.D. Myers, Qualitative Research in Business & Management. 2009. SAGE Publications Ltd.

Mamic, I 2004, Implementing Codes of Conduct: How Businesses Manage Social Performance in Global Supply Chains, Routledge, Sheffield. Available from: ProQuest Ebook Central. [1 February 2019].

Maresova, P., Soukal, I., Svobodova, L., Hedvicakova, M., Javanmardi, E., Selamat, A. & Krejcar, O. 2018, "Consequences of Industry 4.0 in Business and Economics", *Economies,* vol. 6, no. 3.

Marinela Mircea and Anca Ioana Andreescu, Article of Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. 2011. IBIMA Publishing Communications of the IBIMA http://www.ibimapublishing.com/journals/CIBIMA/cibima.html, Vol. 2011 (2011), Article ID 875547, 15 pages DOI: 10.5171/2011.875547. Accessed 16.10.2018.

Martin, Peter, and Walter Boyes. Real-Time Control of the Industrial Enterprise, Momentum Press, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/arcada-ebooks/detail.action?docID=1048450.

Mcshane, M. 2018. Enterprise risk management: History and a design science proposal. *The Journal of Risk Finance, 19*(2), pp. 137-153

Nelms, T. C. 2018. Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. *Theory, Culture & Society, 35*(3), pp. 13-33

Niskanen, J. 2016. *Yritysrahoitus.* 7. Painos. Helsinki: Edita.

OCBC Bank pilots AI-based AML solutions from Fintechs. *Enterprise Innovation.* 2017. https://www.enterpriseinnovation.net/article/ocbc-bank-pilots-ai-based-aml-solutions-fintechs-867567262. Accessed 24.4.2019.

Ozili, P. K. 2018. Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review. Accessed at: https://www.journals.elsevier.com/borsa-istanbul-review/. 18.11.2018.

Palva. 2015. Suomen Pankin rooli maksuliikkeen kehityksessä: kansallisista järjestelmistä yhteiseurooppalaisiin järjestelmiin. https://helda.helsinki.fi/bof/handle/123456789/13523. Accessed 15.10.2018.

Pikkarainen, T. 2004. Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research, 14*(3), pp. 224-235

Polak, P. 2018. Towards treasury 3.0/The evolving role of corporate treasury management for 2020. *Management: Journal of Contemporary Management Issues*, 23(2), pp. 189-197

Rashid, Hossain and Patrick. Article: The Evolution of ERP Systems: A Historical Perspectiv. 2002. https://faculty.biu.ac.il/~shnaidh/zooloo/nihul/evolution.pdf. Accessed 15.10.2018.

Ross S., Westerfield R,Jaffe J., Bradford J., Modern Financial Management, 2008. 8th ed. Mc Graw-Hill Irwin. ISBN 978-0-07-110088-5.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research methods for business students. 5th ed. Harlow: Prentice Hall.

Seasongood, S. 2016. Not just for the assembly line: A Case for Robotics in Accounting and Finance. *Financial Executive*, 32(1), pp. 31-39.

Shaikh, A. A. 2015. Mobile banking adoption: A literature review. *Telematics and Informatics, 32*(1), pp. 129-142

Sisäset tarkastajat ry. https://theiia.fi/sisainen-tarkastus/sisainen-valvonta-ja-riskien-hallinta-2. Accessed 2.8.2018.

Sverige's Riks Bank. 2018. Accessed at: https://www.riksbank.se/en-gb/payments--cash/e-krona/. 20.11.2018.

Soares, L.F.B.2013. Secure user authentication in cloud computing management interfaces. *Performance computing and Communications Conference (IPCCC), 2013 IEEE 32nd International*, pp. 1-2

Scott, Susan V. "Origins and Development of SWIFT, 1973-2009". *Business History* 54.3 (2012): 462-482.

The Automation Imperative. Article by McKinsey consulting: Edlich, Ip, Whiteman. 2018. https://www.mckinsey.com/business-functions/operations/our-insights/the-automation-imperative. Accessed 23.9.2108.

The Casualty Actuarial Society. 2018. https://www.casact.org. Accessed 23.9.2018.

The changing role of internal auditing. 2013. Deloitte by Pramesh Bana. https://www2.deloitte.com/.../ZA_RA_TheChangingRoleOfInternalA. Accessed 18.10.2018.

The Evolution of a Global Cash Management System Holland, Christopher P; Lockett, Geoff; Richard, Jean-Michel; Blackman, Ian Sloan Management Review; Fall 1994; 36, 1; ABI/INFORM Research

Tysiac, K. & Drew, J. 2018, "Accounting firms: The next generation", Journal of Accountancy, vol. 225, no. 6, pp. 26-32.

Troman, G., Jeffrey, B. and Waltford, G. (2005) Methodological Issues and Pactices in Ethnography. Amsterdam: JAI Press Inc (Studies in Educational Ethnography). Available at: https://search.ebscohost.com.exproxy.uef.fi:2048/login.aspx?direct=true&db=nlebk&AN=166784&site=ehost-live (Accessed: 1 February 2019)

Yan, L. 2011. Risk-based AML regulation on internet payment services in China. *Journal of Money Laundering Control*, 14(1), pp. 93-101.

Vacca, JR (ed.) 2013, Managing Information Security, William Andrew, Rockland, MA. Available from: ProQuest Ebook Central. [14 January 2019].

Wittkop, A. 2018. How Digitalization Changes the Internationalization of Entrepreneurial Firms: Theoretical Considerations and Empirical Evidence. *Management Dynamics in the Knowledge Economy, 6*(2), pp. 193-207

Weeserik, B. P. 2018. Improving Operational Risk Management Using Business Performance Management Technologies. *Sustainability, 10*(3), p. 640

Wright, G. (2018). Business benefits from open banking. Global Finance, 32(8), 40-41. Retrieved from https://search-proquest-com.ezproxy.arcada.fi:2443/docview/2112527033?accountid=27294

Zheng, X. 2018. *FinBrain: When Finance Meets AI 2.0.* http://arxiv.org/abs/1808.08497 Accessed 28.1.2019.

Xing, X. & Yan, S. Rev Quant Finan Acc (2019) 52: 85. https://doi-org.ezproxy.arcada.fi:2443/10.1007/s11156-018-0703-z. Springer US. Accessed 15.1.2019.