jamk.fi

Employee Profiles in Automated Access Management

Harri Säkkinen

Master's thesis
May 2020
Technology
Degree Programme in Cybersecurity

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Säkkinen, Harri	Opinnäytetyö, ylempi AMK	Toukokuu 2020
		Julkaisun kieli Suomi
	Number of pages 68	Verkkojulkaisulupa myönnetty: x

Työn nimi
Työntekijäryhmien profilointi automaattista pääsynhallintaa varten

Tutkinto-ohjelma
Kyberturvallisuuden koulutusohjelma

Työn ohjaaja(t)
Kotikoski, Sampo
Hautamäki, Jari

Toimeksiantaja(t)
Jyväskylän kaupunki, tietohallinto, Jalkanen Arto

Tiivistelmä

Kaupunkien teknisessä tuessa myönnetään, poistetaan ja muokataan eri käyttäjien käyttöoikeuksia. Tämä on prosessi, josta helposti muodostuu aikaavievä ja samanlaisena toistuva tehtävä. Siksi tarpeeksi nousee tarve suorittaa prosessi koneellisesti tunnistamalla jo etukäteen ketkä tarvitsevat mitä käyttöoikeuksia ja milloin. Tunnistaminen edellyttää työntekijöiden järjestelmiin ja käyttöoikeuksiin liittyvien tarpeiden profilointia.

Profilointi tapahtuu haastatteluiden avulla, joissa kysytään ja dokumentoidaan kyseisen työntekijän käyttöoikeustarpeet. Tarpeet perustuvat aina johonkin tehtävään jolla on tärkeys ja toistuvuus. Näistä saadut dokumentit toimivat automatisoinnin perustana ja apuna päätöksenteossa, koska kaikki tehtävät eivät tuo merkittäviä työaikasäästöjä.

Lopputuloksena syntyi 10 työntekijäprofiilia joiden perusteella kaupungin on mahdollista tunnistaa missä automaatiosta on eniten hyötyä, miten, kenelle ja tarvittaessa myös luoda pohja käyttöoikeushallinnan laskutukselle. Varsinainen automatisointi edellyttää kuitenkin erillistä käyttöönottoprojektia ja järjestelmäintegraatioita. Siksi työntekijäprofiilien selvityksen tulisi edetä asteittain ja tuottaen jatkuvia, selkeästi mitattavissa olevia tuloksia.

Työn viitekehyksenä toimi ITIL ja erityisesti sen pääsynhallintaan ja kysynnän hallintaan liittyvät osa-alueet. Pääsynhallinnassa kyse on ajantasaisten käyttöoikeuksien myöntämisestä oikeaan aikaan oikeille henkilöille. Kysynnänhallinnassa kyse on loppukäyttäjien tarpeiden tunnistamisesta ja ennakoimisesta.

Työntekijöiden tarpeiden profilointi avustaa kummassakin ja automatisointi sallii tietohallinnon vastata näihin tarpeisiin huomattavasti tehokkaammin. Lopputuotoksena syntyi 10 työntekijäprofiilin taulukko, josta on mahdollista päätellä missä tarve on suurin.

Avainsanat (asiasanat)
ITIL, IDM, profilointi, pääsynhallinta, automatisointi

Muut tiedot (salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Säkkinen, Harri	Master's thesis	May 2020
		Language of publication: English
	Number of pages 68	Permission for web publication: Yes

Title of publication
Employee Profiles in Automated Access Management

Degree programme
Degree Programme in Cybersecurity

Supervisor(s)
Kotikoski, Sampo
Hautamäki, Jari

Assigned by
Jyväskylän kaupunki, tietohallinto, Jalkanen Arto

Abstract

Employee profiles in automated access management is an interesting topic because it is about defining what access rights a group of employees needs to do their work. Then letting a script grant or remove the rights. Unlike humans, machines cannot interpret or assume, so the instructions need to be precise, which are not readily available in a multi-system, multi-department organization. As the number of systems increases, so do the users.

Consequently, the task of maintaining the access rights becomes more complex and repetitive. In the case city, the process was carried out manually by technical support personnel and considered mundane, so the need to automate was readily acknowledged. The primary objective of the study was to learn how the employee profiles could be defined in such a way that the profiles could be used as a starting point for access automation. Without this information, the department of IT has no comprehensive picture of who or what needs access rights or why they are needed, making automation efforts difficult.

The necessary information can be gained by interviewing super users in 1-to-1 interviews, each roughly 45 minutes long. The resulting employee profile tables gave insight to the tasks the profiles carry out and which systems they access. The conclusion was that these profiles give the necessary insight to understanding the employee groups and their value, but to automate the access related tasks further details are needed.

Thus, future automation projects should carry out integrations hand-in-hand with employee profiling, where the profiling identifies which employee groups would benefit from automation and give the benefits an understandable value proposition. Based on this information, a city can then decide which profiles are moved into the automation pipeline.

Keywords/tags (subjects)
ITIL, IDM, profiling, access management, automation

Miscellaneous (Confidential information)

Contents

1 Introduction

Information technology (IT) has a growing role in the heart of business, often managed by independent IT departments. What used to be just a phone number for receiving computer related support calls is now catering a number of different departments and their various needs, such as the upkeep of student registries and rent collection. (Farenden 2012, Chapter 4 - Thinking It Through: Service Strategy.)

Within IT administration, this may entail system troubleshooting and installations, supplier management and contracts, the technical aspects of databases and servers, and the political aspects of highspeed Internet connection distribution, as well as automation and access management. In business, it is about technology helping the business to achieve more with less (Farenden 2012, Chapter 4 - Thinking It Through: Service Strategy).

Common to all these needs is that the end-users expect the IT, as a department, to provide technological solutions and outcomes while bearing the burden of work and related risks. This is a service: generating desired outcomes to the users while keeping the risks, complexity, and costs (ITIL Service Strategy 2007, 16). A service could be the provision of new computers, where the end-user usually requests a new computer by filling a form and then receives it within a set number of days, ready for use at the place of their choice. No work or knowhow required from the end-user, the service provisioner taking the responsibility.

In the same vein come the Windows user accounts, which are an important part of a network. Every employee is a user and each user has a personal user account that allows them to use the resources of the network, such as a computer and the software of that computer. Each account can have a separate collection of media, documents, and settings. (Tidrow, Boyce & Shapiro 2015, chapter 4.) The user accounts are usually created as a service, where the user receives the account ID, password, email, and the correct access rights without knowing how they were granted.

Over time the creation of user accounts leads to differences between them. User John may be an accountant and needs access to accounting software. User Mike

might be an IT administrator, who needs to access helpdesk software. Their tasks and responsibilities translate to different kinds of routines they carry out during their employment (ITIL Service Strategy 2007, 131-132). Often different users manage different parts of the same process, which leads to their accounts having different collections of access rights. These collections are called *employee profiles*.

The goal of this study is to map 10 employee profiles within a medium-sized Finnish city and examine what their tasks require for automated access management. Automated access management involves granting the required access rights at request from, for example, a self-service portal. The value of this lies in understanding why the case city's employees need access rights and when they need them, thus improving security and enabling the IT to automate the authorization process. As a secondary goal, the critical success factors and challenges met during the study will be noted so that repeat studies can avoid them. ITIL Lifecycle is used as the framework of the study.

The study begins by explaining the background of the example city and how ITIL Lifecycle describes demand management. The readily known challenges, the meaning of patterns of business activity, activity-based demand management, and the role of a demand manager are explained. This section is based on ITIL's practices, but excludes sections that are more relevant to creating services. The scope of the study is limited to the creation, modification, and deletion of employee profiles as well as their access rights. Note that the term 'employee profiles' was chosen over 'user profiles' because only the employees are targeted. A city may have other user groups, such as outside consultants and anonymous, public users.

Later the study carries out empirical research by interviewing a number of super users within the city, who are in a central role in the upkeep of the software. The purpose is to learn about their tasks, record them to a written form, and compare the findings to the guidance given by ITIL demand management. The information given by the managers is expected to be reliable, because they are the ones most closely affected by the changes in user profiles. Often they are the ones to grant the access rights, although the task may be divided between multiple super users. This reliability assumption, however, is re-evaluated during the analysis. Will there be a trend of emphasizing the importance of their own work?

Qualitative research acquires data through interviews, documents, and observation data (Khan & Huma 2015, Chapter 3 - Research Methodology), which is important in today's shift towards more service oriented IT, where IT strives to provide outcomes rather than technological applications (ITIL Service Strategy 2007, 16-17). These methods were found to be a valid way of acquiring the data from department representatives, so it was chosen for this study.

The results are analyzed using case-oriented approach to interviews. The collected data is processed and written to a clearer form, where the field notes are opened and possible dictations are transcribed. The processed results can be read by anyone and function as a valid source for commenting and analysis. (Miles & Huberman 1994, Data Processing and Preparation.) In a case-oriented approach all results are analyzed comparatively instead of individually. The goal is to find similarities, simplify, and compare different outcomes to form more general explanations. (Miles & Huberman 1994, Case-Oriented Strategies.) With the employee profiles, the similarities lie in the tasks. If the study was to be extended to involve more roles, the similarities could be shared between many roles regardless of the company.

2 Research Framework

In this chapter the research question will be defined together with the context, the case city, where the research was executed. Understanding these may give insight for repeating the study in a different organization. The ITIL framework is explained and results from similar studies examined. Finally, a framework for access automation is presented, which presents the situation the organization should strive for.

2.1 The Research Questions and Goals

Science seeks to answers questions whereas engineering seeks to develop solutions. In cybersecurity, it is important to realize these two work in tandem, where solutions follow design. One of the first steps is to understand the research question before the development of new can begin. The research question should not be answered ambiguously. (Edgar & Manz 2017, Chapter 3: Starting Your Research.) In other words, science first answers a question, makes a design, and from there engineering develops a solution.

In this study the questions arise from daily helpdesk routines, where city employees request changes to system access rights on a regular basis. The systems can be anything and anywhere, but the expectation is that the change is carried out promptly, securely, and by the protocol. This leads to at least three kinds of issues: (1) the protocol varies by system and department, (2) granting access is a standard priority task among higher priority tasks, and (3) helpdesk does not grant all access rights, instead referring them to other parties. All which cause delay and a chance for an employee to err.

While skilled employees can memorize and solve these requests easily enough, any changes in the staffing are prone to causing issues. Since the changes usually follow the same pattern, the idea of automating these access related tasks arose. What if the admission and removal of access rights was centralized and handled by machine, removing the need to process them by hand altogether? Leading to three research questions:

1. Who are the employees that process or need access rights?
    - Can they be profiled?
2. What kind of tasks require access rights?
    - Which systems are involved in these tasks?
3. How important are these profiles to the business?

The research question is answered by creating a number of goals, which in turn are tied to metrics. Before any implementation, a baseline of performance metrics should be created. Without metrics it is difficult to measure business impact and trends. The metrics can be either business or customer metrics. (ITIL Service Strategy 2011, 125.) Employee profiles are tied to access management and the efficiency of IT's business process efficiency, so business metrics were chosen:

1. Who are the employees that process or need access rights?
    - Goal 1: Interview super users to define employee profiles
        - Metric: 10 employee profiles defined
2. What kind of tasks require access rights?
    - Goal 2: Define what kind of tasks are involved
        - Metric: 100% of access related tasks stated
        - Metric: 100% of access related systems stated
3. How important are these profiles to access management?
    - Goal 3: Define how important each employee profile is
        - Metric: Importance rating per employee profile

Once these goals have been achieved, final action recommendations can be given and considered for access automation. Note that the results are not definite, since the person interviewed may not be aware of every nuance of the system or if there are other ways to operate it. Having a complete and accurate list could be formed over a longer period of time as an on-going process, so this study is but a starting point for a city wishing to improve its access management capabilities. Managing employee profiles is not a project with a clear ending date, but a continuous process that takes regular maintenance, time, and manpower to function.

During the next chapters, the research questions will be answered progressively by explaining the context, the methods, how the research was carried out, and finally by analysing the results. The process of creating employee profile should be beneficial to access management and repeatable in any city. Note that other end-users, such as visitors and outside consultants, are not in the scope of the study because in the case city they often do not gain access to systems. However, if they receive access rights the same way as employees, they could be defined just the same.

2.2 Case Jyväskylä: An Example City of 7000 Employees

Finland is a country of 5.5M people, where 88% of the population have access to Internet, 72% use it regularly, and 91% have a personal computer at home (Tilastokeskus 2017, 2-32). The population has a widespread, common, and inexpensive access to Internet services and computers. These statistics might be closely comparable to those found in other Scandinavian and Central European countries.

2017 Finland had 311 municipalities with an independent governance(The Ministry of Finance 2017). One of them is the city of Jyväskylä: the seventh largest city in Finland with approximately 137 000 residents, two universities (Jyväskylä Facts 2018), 7000 employees, 400 different job titles, and at least 17 departments (Jyväskylä Organization Chart 2019). Jyväskylä is a Finnish city officially founded in March 1837 in Central Finland (Tommila 1972, 15). A year later the city had 189 residents and from the beginning the fledgling city was planned to act as an independent and self-sufficient hub of Central Finland. Jyväskylä was known for the first Finnish secondary high school, founded in 1857 (Tommila 1972, 126), which still exists in the city center. At the time, city planning, lot auctions, and building played a critical role.

The employees and the governance have been divided into four main departments and 23 sub-divisions. The departments have their own leaders and service areas, such as city administration, education, culture, and urban planning:

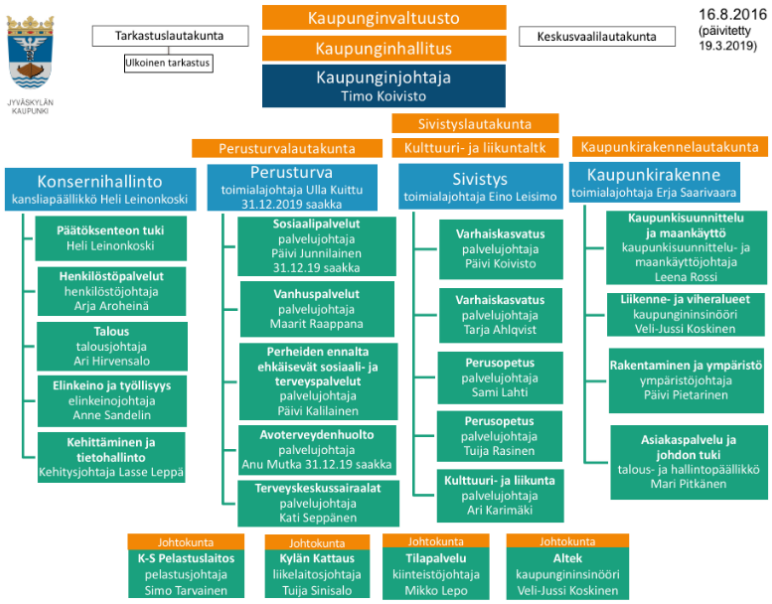

Figure 1. Jyväskylä's organization (Jyväskylän kaupunki 2019, organisaatio)

As seen in the figure, IT has been grouped with financial services, but in practice operates as an independent unit with a CIO of its own, bringing the total number of sub-divisions to 20. Other statistics that can be concluded from the chart are:

- 4 top-level departments (blue)
- 4 top-level chiefs
- 24 lower level departments (green)
- 24 department chiefs
- 10 decision-making boards (orange)
- 1 city leader (dark blue)
- 3 outside boards (white)

In contrast, the city board has 13 members from various political groups and the mayor, who presents the cases to the board. The board signs and approves the legal contracts of the city. The board is also responsible for the day-to-day decision making and the preparation of the matters presented to the city council. (Jyväskylän kaupunki 2019, City Board)

The council consists of 67 elected councellors and decides for the most important matters of the city, such as taxes and budget. The council also appoints the 13 members of the city board. The current members and the up-to-date structure is publicly available at Jyväskylä's website. The chart appears similar to other city organizations regardless of country, such as City of the Brisbane (City of Brisbane 2019, Organisational Chart) and Perth (City of Perth 2018, Organisational Structure),

as seen in figure 2. Both charts share the same characteristics: a tree view, a number of individual departments specializing on an area of expertise, and a smaller count of supervising bodies. They are hierarchial and focus on function, product, market space, geography, or process (Morris & Gallacher 2016, Chapter 6: Organizational Departmentalization).

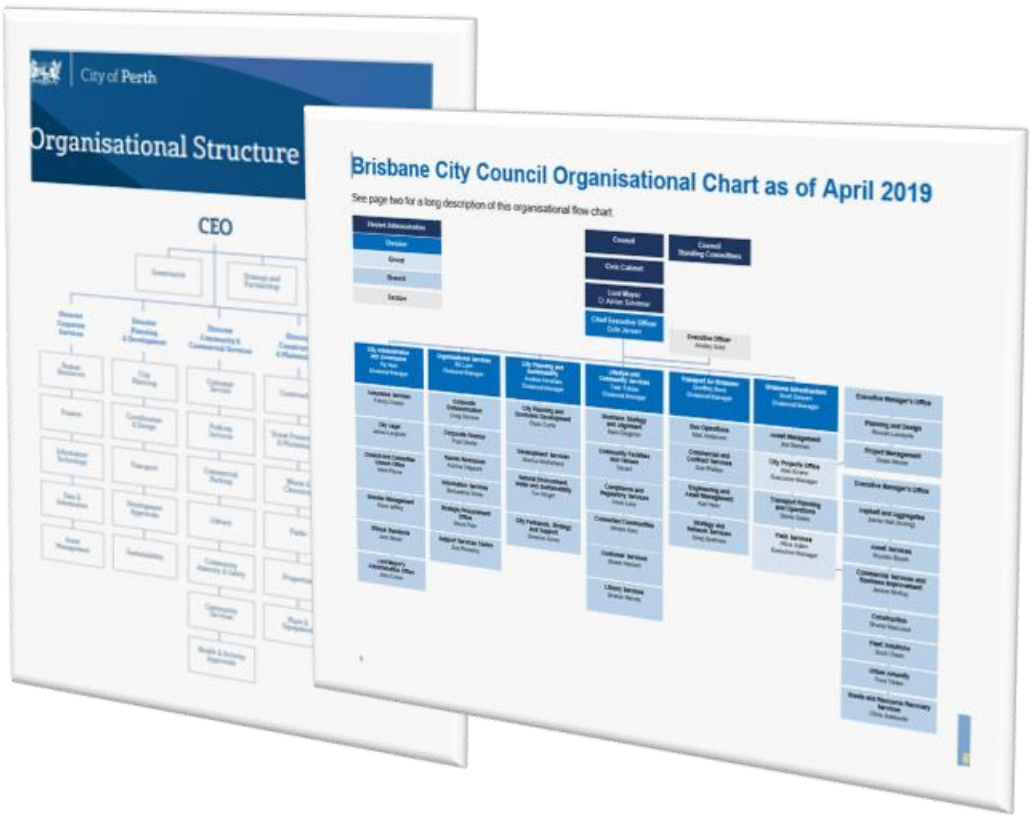

Figure 2. Other examples of departmentalization

In the case city, the infrastructure is based on Microsoft Windows server and workstation technology. The user accounts are created to *Active Directory (AD)* with the default tools, although an unknown number of other systems have accounts and profiles of their own. AD is an umbrella term for domain, certificate, federation, and rights management services, which have become an important part of Windows based environments (Clines & Loughry 2008, chapter 1: Understanding Active Directory). AD is used as an information store that is integrated to Microsoft Exchange email service and SAP contracts. As an information store, AD may include information such as last name, first name, middle name, job title, foreman, department, and the ending date of the account or contract. The information plays a critical role in access management, or the lack of, which in turn generates service requests to helpdesk.

Similar choices in similar cities may lead to the same issues in city management and IT infrastructure; therefore the results of this study might be worth considering if a city wishes to develop its employee profiling. Employee profiling is important for the automation of system account creation and integrations, which ultimately shifts workload from helpdesk to a machine.

For example: by enabling the creation of user accounts through an intranet self-service website, a city can speed up the processing times, implement automated authentication methods, and move the associated workhours from granting the rights to monitoring them. These aspects are outside the scope of the study, but nevertheless they are a part of Jyväskylä's goal to improve its identity management systems.

2.3 ITIL and the Service Lifecycle as a Process Framework

ITIL stands for Information Technology Information Library, which is a collection of practices common to successful companies. It is a non-proprietary, non-prescriptive, and tested framework that gives value by giving insight to managing services, processes, people, and the underlying components. Not only as a reaction to growing needs, but through prediction and the ability to consistently produce what is needed by the end-users and customers. (The Official Introduction to the ITIL Service Lifecycle 2007, 4.) Without a consistent management framemwork or strong leadership, an organization grows by developing what is immediately necessary.

ITIL v3 Lifecycle consists of five books, which detail the service strategy, design, transition, operation, and improvement. These five parts form a cycle that drives service production as a working whole. (The Official Introduction to the ITIL Service Lifecycle 2007, 3.) ITIL is not the only way to manage and lead service production; however it is a proven collection of methods that can be adapted to city administration at a level that the organiation is comfortable with, allowing the organization to either cherry pick the best or seek a more thorough advice. Because of these factors, ITIL was chosen for this study.

In figure 3, the service lifecycle has been arranged to a more visual form. At the center is the strategy, particularly service portfolio, around which the service design,

transition from plans to operation, and daily operations revolve. They return feedback which each turn, which drives continual improvement to all aspects of the cycle. The cycle, as a whole, does not remain static as people, processes, products, and partners change over time.

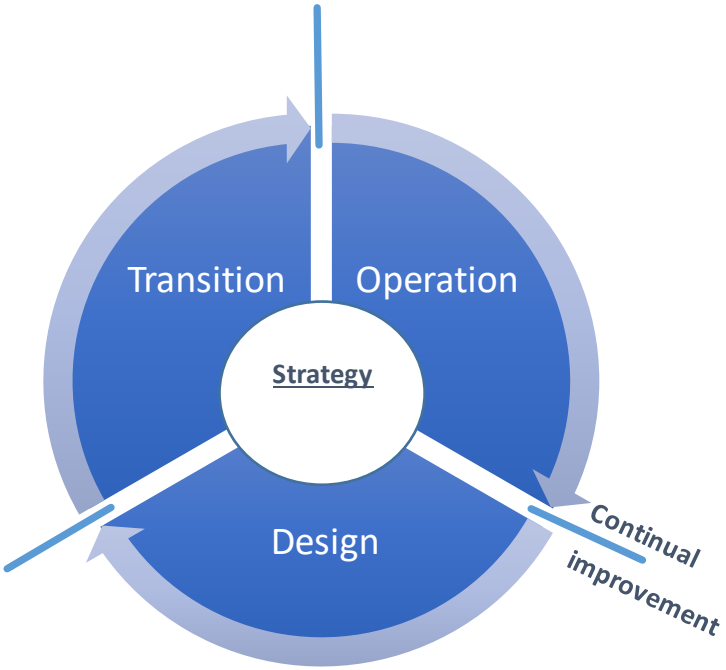

Figure 3. ITIL v3 Lifecycle, divided to five sections

ITIL and other best practice frameworks, such as M_o_R for the management of risk and PRINCE2 for the management of projects, were originally founded by *the Office of Government Commerce* (OGC) in the late 1980s due to the need to find how the most succesful organizations handled their service management in the United Kingdom (The Official Introduction to the ITIL Service Lifecycle 2007, 3). For IT, other well-known service management frameworks are COBIT5 and USMBOK, but also standards such as ISO/IEC27001. All these aim to provide guidance on the enterprise governance and IT management (COBIT5 2012, chapter 1), hopefully leading to better services for everyone.

In Finnish city administration ITIL can provide tools for improving service quality through the same methods that have already made a number of companies succesful. The scope of the study is limited to the employee profiles, which are introduced for the first time in ITIL Service Strategy under the section of demand management. Demand management is concerned in forecasting user capacity

needs, usage patterns, and understanding what drives the use (ITIL Service Strategy 2007, 129). Demand management links people, processes, and applications to patterns of business activity, which include interactions with suppliers, IT administration, and any other stakeholders. These business activities change over time and maintaining accurate profiles requires maintenance. (ITIL Service Strategy 2007, 131). In a later edition this is also stated more clearly: the purpose of demand management is to define and analyse employee profiles to undestand the typical needs of various users (ITIL Service Strategy 2013, 245).

Employee profiles are linked to business patterns. Therefore a change in this business pattern should notify a change authority and other stakeholders, including AD administration. In a city, this requires the departments to officially acknowledge which services they provide to each other and how they depend on them. For example: if secretary Mary, among twenty others, requires access to confidential documents on a network drive, available only to the secretaries of city management, she will call helpdesk and request access. Helpdesk and an AD administrator then grant access as a service.

The pattern is that Mary may have started as a new secretary and, due to her job, she immediately needs the access. Likewise, if her job title changes, she may not need the access anymore. Removing access rights is rarely as important to the user as gaining them, so it is likely that Mary would not notify helpdesk about the matter, creating a confidentiality vulnerability. To secure the documents, these kind of patterns and employee profiles need to be acknowledged, recorded, and acted upon in a timely manner.

ITIL demand management provides a method for creating employee profiles and matching them with business activity patterns. Employee profiles need to be defined -as well as the activities involved. The profiling model used in this study was modified from the original ITIL model to make the frequency of use more understandable. The original is shown in figure 4 below, which lists interactions with customers, processing sensitive information, and other tasks carried out by employee profile number 45F:

PBA No. 45F Activities	Activity Levels					
	Hi	3	2	1	Lo	NA
Interact with customers remotely (frequency)			x			
Interact with customers on-site (frequency)				x		
Archive or handle customer information			x			
Process sensitive information (privacy)						x
Generate confidential information						x
Provide technical support (frequency)		x				

Figure 4. Original ITIL model for understanding employee activities, patterns of business activity, and work routines (ITIL Service Strategy 2007, 131)

Figure 4 table displays a single role with six activities. The six columns, such as 'Hi' and numbers from 3 to 1, are the activity levels. The activities express the business the role carries out, which can be anything the role owner or his foreman consider central to the role. The listing may or may not be comprehensive, which is a valid point of review for later improvements, emphasizing the need for continuous development. The activity levels express how often the activities are carried out or if they are applicable to this role at all, should the owner wish to explicitly bar a specific activity from this role.

The modified tables 1 and 2, where the first one lists all the profiles and their primary purposes. It can be understood as a job title, although one employee can act in multiple profiles. In table 2, the actual activities are listed. It is somewhat equivalent to job description, although includes only the elements that involve system access. The final form of table 1 will also include columns for number of profile members and the importance rating, which are not part of ITIL's example:

Table 1. How to list employee profiles as a whole (ITIL Service Strategy 2007, 132)

ID	Employee profile name	Primary purpose
Table 2	User account administrator	Create and manage user accounts
Table 3	IT Department chief	Carry out credit card payments
Table 4	Financial accountant	Create financial statements
Table 5	Hospital nurse	Register and manage client status
Table 6	Kindergarden teacher	Register daily events

The usage patterns, or patterns of business activity (PBA), will be recorded using an adapted model from ITIL. In table 2, the activities of a user account administrator are recorded with their frequency and priority (Pri). The work can take place either

regularly, occasionally, or rarely. Priority is the super user's subjective evalution of the importance of the task, expressed by a number between 1-3:

- 1 is critical to the role, without which the business immediately stops, causing an incident or service unavailability. For example: interaction with customers over phone becoming unavailable to a remote support role
- 2 is important to the role, which can wait for a limited time before causing an incident. For example: helpdesk email ticketing not working while telephone support is still functional
- 3 is beneficial for carrying out the work, but can wait without causing an incident. For example: once a month archiving of support tickets

The number is not an absolute truth and relies on the expertise of the person interviewed, but it gives an indication where the emphasis of the work lies and if the management views the priorities the same way, possibly indicating a communication gap. This can be used to direct the automation efforts to areas of importance once a larger selection of employee profiles has been created and approved.

Table 2. Example user account administrator	**Pri**	**Reg**	**Occ**	**Rare**
Interact with end-users remotely	3		x	
Interact with end-users in person	3			x
Access non-sensitive end-user information	1		x	
Generate confidential information	1			x
Provide technical support	3	x		
Seek technical assistance	3		x	
Process SAP profiles	1	x		
Process AD profiles	1	x		
Process Exchange profiles	1	x		
Process helpdesk tickets	1	x		
Use an email service	2	x		
Use a telephony service	3	x		
Generate technical reports	3		x	
Maintain an IDM system	2		x	
MEMBERS: **5**		IMPORTANCE: **21**		

Demand management needs to cooperate with other service management areas, such as information security management (ISM), which functions within the overall city governance framework and ensures the services conform to the IT security policies, directing the security efforts (ITIL Service Strategy 2011, 331). The policies and responsibilities are set by the city governance, agreed by the executive management or the city board (ITIL Service Design, 141), which then provide ISM the goals it needs to operate.

Demand management should cooperate with access management. Access management safeguards authorized access to a service while denying unauthorized attempts, based on the policies placed by information security management (ITIL Service Operation 2011, 110). Employee profiles are important to access management because correctly granting access relies on identifying users and managing their access profiles throughout the lifespan of their job contract. Usually access requests are handled as a part of technical support (ITIL Service Operation 2007, 68), which has an innate interest in solving incidents as quickly as possible and therefore requires clear, preset rules. Reversely, helpdesk has an innate temptation to take the quickest solution, which may not be the most correct one.

2.4 User Profiles in Other Literature

User profiles, which may be employees as well, are a common concept to Windows and other operating systems, which is why they are covered in a variety of publications. For example, *Windows 7 Inside Out* discusses user profiles as a local computer account or a number of accounts in AD, which are then managed centrally for passwords, parental controls, names, fingerprints, and type. The type can be administrator, guest, or standard user. (Bott, Siechert & Stinson 2011, chapter 18.) The same approach is taken in *Mastering Windows Server 2012 R2*, which has detailed images on how to create accounts in a number of tools, such as ADAC and Powershell (Minasi et al 2014, chapter 8).

While necessary, these publications are more suitable for technical administration and operative work rather than their governance or management. Governance is about making justified decisions and having a framework for the decision rights (ITIL Service Strategy 2007, 154-155.) Management makes the decisions and executes the processes (ITIL Service Strategy 2007, 155), which involves demand management and the definition of user profiles.

User profiles are also brushed in identity management publications, single sign-on solutions, and general access management concerns. For example, Tipton & Krause write about the use of SSO to centralize the management of user accounts and therefore decreasing the amount of work routine user management requires. By

centrally terminating a user account the administrator can deny access to multiple systems at once. (Tipton & Krause 2007, chapter 66.14.) However, the user accounts are still different because the users themselves work in different roles. By identifying these employee profiles the administration can empower the use of SSO, because granting a single profile can grant access to a number of systems at once -or remove it.

The concept of demand management, to which user profiles belong to, has been well covered in the official ITIL publications, but also in work cases such as *Concept for IT Demand Management: Case UPM-Kymmene Oyj*. The results of the case study state that an effective demand management is possible through good communication with the business, adequate tools for recording demand initiatives, clear view of the dependencies between applications and services, but also development roadmaps. (Laitinen 2016, 25-26.) These results reflect the need for good communication, because without cooperating with the business, the profiles can not be defined and without knowing the business process, setting the correct access rights and system dependencies may be difficult.

For these dependencies, Salovaara (2015, 24-46) presents in his thesis *Developing Service Design and Management Processes Towards ITIL Compliance* a form where the information can be listed. This is presented in figure 5, which closely follows the ITIL Service Design (2011, The form is not the same as seen in ITIL Service Design (2011, 303-305) service design package template:

Category	Sub Category	Description
Require-ments	Business requirements	The initial agreed and documented business requirements.
	Service applicability	Definition how and where the service would be used.
	Service contacts	Business, customer and other stakeholder contacts.
Service Design	Service functional requirements	Utility of the service including planned outcomes and deliverables in a formally agreed SOR.
	Service level requirements	SLR representing the desired warranty of the service SLA's including service and quality targets.
	Service and operational management requirements	Requirements for managing the service including all supporting services and agreements, control, operation, monitoring, measuring and reporting.
	Service design and topology	• Service definition, model, packaging and service options. • All service components and infrastructure including version numbers and relationship. • All user, business, service, component, transition, support and operational documentation. • Processes, procedures, measurements, metrics and reports. • Supporting products, services agreements and suppliers.

Figure 5. In topology: listing components that may require user rights (Salovaara 2015, 24-46), ITIL Service Design (2011, 303-305)

The study proves that by designing services a city can also aid in the design of efficient and secure IT environment. In the case Jyväskylä, there is an application catalog that lists employees responsible for the application, however, it does not list dependencies between processes and applications. This information still needs to be acquired through interviews.

In his book *Sharpening Customer Profiling for Wormhole IT*, Otto Martikainen examined the same issue, but for company outsiders rather than the employees. By understanding customer profiles, the company can reach new customers more effectively, retain the old ones, better customize market messages, and understand who the best customers are (Martikainen 2017, 7-8). The conclusion was that the correct term would be "buyer profiles" and two of these were discovered: one that uses provider software as a part of a consultation service and another who uses the same software to train employees (Martikainen 2017, 44). In both cases access to this software is an important part of their business and proves that profiling can and should be carried out for both internal and external stakeholders. The profiling can also be used for requesting feedback about issues and user satisfaction (Martikainen

2017, 47), which would be interesting to carry out in the case of employees. For example, how satisfied are the employees about the tools they have and the tasks they carry as a part of their profile?

2.5 The Value of Up-to-Date Employee Profiles

Demand management is a process within the Service Strategy partition of ITIL service lifecycle and focuses on identifying, influencing, and anticipating customer demand by recognizing business patterns and user profiles (ITIL Service Strategy 2011, 246). Service strategy is about planning and outlining how an organization will meet the primary goals of its existence. It is about handling impacts inside the organization, uncertainty, priorities, future trends, market environment, and their interactions. Even cities and their IT administrations are subject to competition and market influence. (ITIL Service Strategy 2011, 35-36.) In principle, city IT administration needs to be comparable to similar service providers in the market to remain as a valuable partner within the organization. Failing to do so may increase the appeal of choosing a better performing candidate from the market and spark calls for outsourcing.

Demand management and employee profiles are not a silo: by understanding the employee profiles the service organization also understands what generates demand and how it reflects to the security of systems. Not only the security, but how much, when, and why the resources such as servers are utilized. (ITIL Service Strategy 2011, 107.) Over time, the employee profile information may reflect on the service portfolio of an IT department where information about the use of services is listed (ITIL Service Strategy 2011, 180). Employee profiles can also be created for automated users, or machine accounts, and applications, in which case there is no real physical employee behind the profile, but is still used to produce a service or run a process (ITIL Service Strategy 2011, 250).

Employee profiles add value to city leadership by defining the activities business carries out within the systems and how issues in the profiles reflect to the production of outcomes (ITIL Service Strategy 2011, 253). This could be particularly important for

improving communication, since the information enables accurate impact analysis and therefore informing the impacted employees.

Financial management can use the profiles and the number of profile users to forecast costs (ITIL Service Strategy 2011, 253). The profiles can also be priced if the systems require licenses -a price that can depend on the number of profile members or the importance of the profile. This pricing reflects on the business and the relations IT may have with them. The business may require or produce reports on the usage of these licenses and compare them with the profile members, thus creating basis for service utilization agreements (ITIL Service Strategy 2011, 254). The profiles can also aid technical management to monitor the usage of services and their logs, as well as generate more accurate reports even if the profiles are not automatically connected to events.

The costs and usage are valuable for managing the service capacity. Knowing how many employees and how they use the service enables IT to understand what is sufficient for each service (ITIL Service Design 2011, 154). In cities, more importantly, it allows the administration to evaluate how important one profile group is in comparison to nine others and how much effort should be spent on servicing each group. For example: *user administrator* group consists of four members that use AD and Microsoft Exchange for creating user accounts.

In comparison, *city secretary* group consists of twenty members that use Microsoft Word and a network share with special privileges. Both may require information about changes in the same assets although the needs and methods are different. Part of demand management is influencing these needs so that the current capacity is used wisely (ITIL Service Design 2011, 172). Without employees profiles this mitigative work may be difficult to carry out. In this case, the secretaries' profile would indicate a dependency on a special access group and the administrator's profile would indicate that they can grant it, but also require an administrative access to AD.

The value of up-to-date employee profiles lies in providing a source of information for targeted communication, access management, demand and capacity forecasting, incident impact analysis, and event monitoring. It is worth noting that if access

management defines user access in accordance with the employee profiles, then the security of the software itself should be kept similarly up to date. Applications need periodic changes to correct program errors and enhancements (Senft & Gallegos 2009, Chapter 16), the lack of which may enable bypassing the access controls. For example: Windows OS, Office 365, VLC Player, 7Zip and even the antivirus software itself, such as F-Secure and Windows Defender.

To keep the profiles up-to-date and relevant, they need to be part of change management. The purpose of change management and the meetings of its members is to control the flow of changes to existing IT infrastructure, minimize the disruptions, and act as a clearing house before the change is made (ITIL Service Transition 2011, 61). This means that new employees profile additions and changes to current ones should be cleared in a change management meeting before publication and subsequent changes in access controls -for which the access management should be involved. At minimum, a person knowledgeable of the local and AD access groups and with the ability to relay the information to system specific super users.

2.6 Recognizing the Required Roles

Before the security of the login assets and employee profiles can be improved, the people involved and their roles need to be defined. This serves three purposes: the immediate availability of information for the interviews, the long-term support in maintaining the information, and the generation of value. In the case city, *super users* were an immediately available role that is sometimes accompanied by *application analysts*.

A super user is a role that liaisons with IT and service desk in general. Super users facilitate the communication between the communities and help disseminate the information to their local users. They can also gather together issues that have risen in their area, usually a single application, and prevent multiple calls on the same topic. (ITIL Service Operation 2007, 116.) Usually a super user is an employee who has in-depth knowledge of a specific software, processes involved, and, in most cases: the ownership. They are often involved in the support of the software,

although the technological aspects, such as servers and networking, can be split to IT or an outside provider. For example: the software supplier or a cloud-based service provider. The same software may have multiple super users in different departments and thus the processes, service outcomes, and contact personnel may vary.

Application analysts generally work with the users to create application requirements and communicate this between the involved parties. They also consider the budget and technology constraints, how the applications are managed and which functional tests the application needs to pass to be acceptable for use. Application analyst also defines the maintenance windows and where training is needed. (ITIL Service Operation 2007, 137.) This role is not as recognized as a super user, however, it is nevertheless frequently assumed when the software needs changes or upgrades. The role can group together multiple systems, such as Microsoft or Adobe products.

If the profiling efforts need to expand and involve multiple departments, then the support of the department chief may become necessary. Without his authorization, outside super users may refuse the interviews and discourage participation by word-of-mouth. This is because gaining information is part of a negotiation process, where people and relationships matter due to trust or relationship issues. (Ouellette & Associates Consulting 2009, Three Key Factors; Three-Step Process.) Without the trust, the key stakeholders may not divulge the information needed to profile their groups and, therefore, the goals of the study cannot be reached.

2.7 Bridging Employee Profiles to Automated Access Management

To quote Home Automation for Dummies (Spivey 2014, Home Automation 101): "automation is another step in making life better. Some may scoff at it, but one can wager they appreciate their automatic dishwashers and refrigerators." In the same way account and access automation saves time and frees it for other tasks. Instead of reading request forms manually, an administrator can lead users to a self-service portal for filing the request. Instead of typing in the information to active directory, an administrator can let the scripts handle it.

Beside user account management, there are many other tasks that require regular and equally mundane labour. For example: backups, patching, storage, tuning,

auditing, and capacity adjustments. Automating these tasks is not going to take away positions, but free time for other jobs. (Malcher 2018, Chapter 8: Tasks.) In fact, automation may be even mandatory in situations like disaster recovery, where time is of an essence. For example: when a data disk breaks up, leading to the unavailability of business-critical services or files. A higher level of automation reduces the damages, labour required, and prevent breaching a written agreement. (Hill 2010, Chapter 2.7: Disaster Recovery Requires Judgment; Operational Recovery Requires Automation.)

Campi and Bauer, in their book of *Automating Linux and Unix System Administration 2nd edition* (2009, Chapter: 1: What Will You Gain?) summarizes the benefits even better: by easing administrative work via automation, a department will free time for more meritable purposes, reduces errors, forces higher level of documentation, enables tracing action to outcome, and possibly grants other benefits. In the case city, the automation reduced processing times of new user accounts from a minimum of three days to generally guaranteed 20 minutes. Thus creating a new norm for account management and leading administrators away from manual labour to monitoring the account security. All of these are good reasons to automate.

The bridge between employee profiles and system access can be described as a process that follows human workflow. As a one potential example of automated access management is an approach called *orchestrator*. The key feature of an orchestrator is that it's not bound to any single system subscriptions, where one system reads directly from another and has to wait for the output. An orchestrator receives the information, makes the necessary checks, forwards the information to a correct receiver or system, and terminates. (Ferreira 2013, Chapter 4: Orchestration-Level Integration.)

In the following picture, the orchestrator approach was adopted to demonstrate a process flow that involves maintaining user access rights with the information the department of human resources (HR) receives as part of their usual work. For example: employee John receiving a promotion from a regular helpdesk employee to a system administrator, which involves one or more additional tasks that he now needs to be able to carry out.

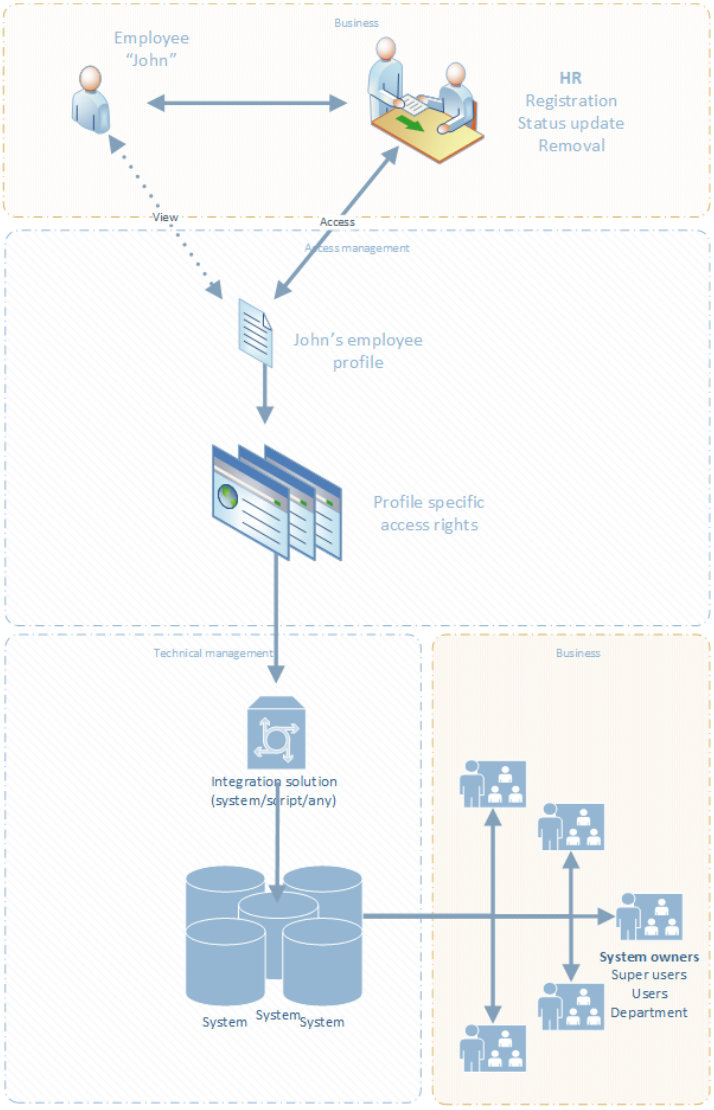

Figure 6. An example structure of automated access management process

Because John was promoted, his foreman informs HR of the decision, which then makes a status update to John's employee profile by changing the job title and salary. The profile could be in any system, such as SAP ERP software, which then reflects to his benefits. Without integrations, that would be the end of the process, unless John or his foreman request for additional access rights from the various super users.

If the profile specific access rights have been pre-defined, then HR and the integration solution readily know what John needs to do to carry out his new tasks even if they do not explicitly request these changes from the super users. The tasks have been listed and the corresponding access rights defined, thus enabling the integration solution to grant these rights -or remove the old ones. The solution could

be a commercial system designed for the purpose or a script custom build for the department. For example: IBM BizTalk or Powershell. BizTalk is a product that enables various systems to communicate with each other in a loose way. It is a collection of applications and tools, such as ports, adapters, pipelines, and a messaging engine (Dunphy 2009, Chapter 1: BizTalk in the Enterprise). Powershell is a text-based command line that can be used to directly control the Windows OS (Ford J, Introducing Windows PowerShell). More importantly, Powershell allows the direct control of various other Windows-based systems and the input of data via scripts. Which then can be scheduled for execution at set intervals for a similar result as BizTalk.

The important result is that the solution brings the necessary changes to the underlaying systems without further manual input, based on the rules defined in the integration solution. The source of the changes could be a file, a database, registry, or even an Excel sheet, but the integration solution takes the data and turns it to usable information in the other parts of the organization.

Gaining an agreement on the rules is an important step in bridging the employee profiles to an actual change in a system, requiring agreements with the system owners, usually the super users. Their interest lies in ensuring predictable levels of data quality, which makes their participation critical for automation attempts (Loshin 2011, Chapter 2 - The Organizational Data Quality Program). In other words: if the rules do not match with the access requirements, then the process cannot be automated.

To summarize, creating employee profiles is about understanding user needs, but to automate their management also requires understanding the process at the management and technical level. As per the research questions, ten profiles are created for this purpose, complete with their importance rating, access related tasks, and target systems.

3 Execution of the Study

Chapter 3.1 reviews the chosen research method and how it is applied during the acquisition of source information. Chapter 3.2 reviews the context of the study and details the goals, which have been touched previously. Here they are set in a more measurable way, enabling comparison of starting situation and the potential gains. Chapter 3.3 describes the current user profile situation in the case city and the potential issues it is facing. Chapter 3.4 explains how the interviews are carried out using a preset formula, who are interviewed, and why. In turn, the last chapter describes how the results are analyzed and briefs on the chosen analysis method. These descriptions are important for the later, improved iterations of the study.

3.1 Qualitative Research Method

Qualitative research method is about using data acquired through interviews, documents, and participant observation data to explain social phenomena. Qualitative research can be positivist, interpretive, or critical. From the three, positivist research assumes reality can be described by measurable properties and tested. (Khan & Huma 2015, Chapter 3: Research Methodology.) It accepts only knowledge that is based on verification, sense, and empirical evidence. The goal of positivism is to identify patterns and cause-effect relationships, preferably in a manner that is independent of the place and time. (Johannesson & Erik 2014, Chapter 12: Research Paradigms.)

The positivist approach, the need to have measurable properties and patterns is applied during interviews. Each study goal has 1-2 corresponding metrics and finding patterns from the resulting lists is in-line with the approach. The interviews also apply a method called *contextual inquiry*, which means the interviewee observes and asks questions as if the super user was a master and he the student (Cooper, Reimann & Cronin 2007, Chapter 4: Understanding Users: Qualitative Research). The interviews are carried out in a normal office environment in collaboration with the interviewee and without suggestions or assumptions. The questions and interview structure give space for cooperation and more informal observations, although the question form (see Table 4) will not include these.

3.2 Establishing a Baseline for Employee Profiling

Improving services requires understanding what the business wants to achieve and setting goals accordingly. These goals should lead to the question of "Where are we now?" To know this, a baseline needs to be assessed with measurable metrics. (ITIL Continual Service Improvement 2011, 35.) In the context of employee profiles and their management, the current situation needs to be evaluated, which then establishes a baseline for comparative analysis.

Baselines are like markers for development. If there has never been a recorded baseline, then the first measurement effort becomes the baseline. Baselines can be established for various goals from strategy to service operation, but in all cases the effort should be documented and accepted by the parties involved. Measurements are done to validate, direct and justify decision-making, but also to intervene for corrective action. (ITIL Continual Service Improvement 2011, 38-39.) Measurements provide the numerical data for decision-making, but the tasks that are carried out as a part of the employee profiles are also important. The tasks evolve over time and thus the baselines should be checked periodically.

The scope of the study is limited to the operative level of employee profiling, so the initial measurement effort is limited to the same ten employees who manage system access: the super users. The case city has many more super users, some unknown, so this limitation is an accepted weakness in the results. The limitation was set to this number as a compromise between value and the required effort to reach the goal. In future studies, the same action is recommended until city leadership has authorized a thorough investigation with the primary goal of recognizing the majority of employee profiles. These could also involve non-employee profiles, such as third-party consultants and service providers.

A larger profiling effort would require the backing of a sufficiently authorative board, involving members from IT and other departments, to succeed (ITIL Continual Service Improvement 2011, 73). Once the benefits have been demonstrated on a small scale, the board could decide if the benefits are worth the time, money, and effort.

The first step in creating a baseline is to document what is currently achieved as-is (ITIL Service Design 2011, 173). In the case city, the baseline begins by recording the informally known profiles, for example, the profiles that are in the memory of a person responsible for managing them. The baseline and the first service draft, which describes the outcomes and how the profiles generate value through automation, to the department lead are created by using a method called the 7-step improvement process. The process' steps are (ITIL Continual Service Improvement 2011, 49-64.):

1. Identify what you are trying to achieve for the department. How will this initiative help the department and how do the metrics connect to its goals? What are the goals?
2. Define what you will measure. What can be and what should be measured? Are these metrics connected to the department's goals? To keep the scope small, this step does not verify if the goals are beneficial to the receiver of the service
3. Gather the data through monitoring. Where are the numbers recorded? How can they be retrieved? How reliable is the source? If there is no raw data, then can the super user make an estimate?
4. Process the data into an understandable format and metrics. If the source is a system or a log file, then it needs to be filtered only for relevant data
5. Analyse the data for meaningful information. The data can then be translated into the metrics and the information that is needed to learn about the impact of managing user rights efficiently
6. Present the information to those who can use it
7. Implement the improvements or make the change

During this study, ten informally known employee profiles are recorded and reported in a more formal form: as an employee profile table. During the analysis the value of automating their creation is described. However, before this is possible, the department's super users need to be discovered and interviewed.

Discovering super users can happen either by discussing with a business relationship manager, the foremen of the department, or reading any relevant documentation. Business relationship management is about knowing the business activities and requirements of the department that purchases services or goods, the manager acting as a link between the provider and the customer (ITIL Service Strategy 2011, 256). In the case city the provider is the department of IT and customers, even if no actual money is transferred, are all departments that use their services, such as pre-installed domain computers.

The first ten participants were recruited for the purposes of this study after discussing with the foremen and peers of the department of IT. As per Goodwin &

Cooper's (2009, Identifying the Number and Type of Interviewees) method for identifying likely roles, after the discussions likely user roles can be guessed either from systems or services the department provides, both of which the foreman is knowledgeable about. For the purposes of this study, only one super user per system is interviewed, although cross-referencing multiple super users can add reliability.

3.3 Interviewing the Department Representatives

Ten department representatives are selected for the interviews due to their role as the super users of a system. These representatives were selected because of their involvement in the practical operation of a service, such as customer service, and knowledge of its details. They are the practical operators of the job without which the service would no longer be available and acknowledged as such by their peers. Because of this, their description of the duties can be considered both practical and reliable, although open for later amendments.

During the interview, the following template (Table 3) is filled with the duties the employee carries out. An important note is that these tasks are not everything the employee does in his job, including only the duties that require access to systems, related devices, or using software. An employee profile describes a set of tasks that can be moved from person to person and who carries out the tasks should not be important as long as he is suitably competent. For example, accessing user records to verify identities is a duty that any of the profile holders should be able to carry out following the same processes and policies, leading to the same outcome. If writing down the process makes sense for understanding the profile, then it should be recorded.

Table 3. Blank template for an employee profile	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
MEMBERS:	IMPORTANCE:			

Once the sample group has been interviewed, completing the research goal 1 ("Who are the employees that process or need access rights?"), the employee profiles are collected to a master list seen in table 1 and the analysis can begin. For the analysis and reaching goal 2 ("What kind of tasks requires access rights?"), the tables are needed.

The interviews are carried out in a predefined, structured way, where the interaction follows a script and a set of questions. The goal is to ask these the same way, in the same order, and deviate as little as possible. The questions can be open or closed, but generally selected from a number of fixed responses. (Wilson 2014, Overview of Structured Interviews.) More importantly: it's good to ask if the written statement makes sense for the goals. Planning for the interview requires 14 steps:

1. Define the interview's goals
2. Determine the participant's motivation
3. List general questions as a starting point
4. Create a pool of follow-up questions to refine the answers to general questions
5. Select the questions to ask
6. Select how the questions will be answered (verbal, written, online, etc)
7. Optimize the order of questions
8. Script the interview so it can be carried out in a preset manner
9. Review the wording, specify the questions, simplify
10. Pilot test, including meeting and exit
11. Create an introduction
12. Recruit the participants
13. Determine where the interview or interviews are held
14. Assemble the necessary documents (Wilson 2014, Planning the Structured Interview.)

The goal of the interviews is to define an employee profile, which could be the role of the super user himself or the group his system serves. The participant's motivation is the use and maintenance of the system he is responsible for.

The place and time of interviews is determined before recruiting the participants and is always away from their usual working area and the distractions. During the early interview tests, it was proven that interviewing in their usual office lead to interviewees dividing their attention to their work rather than the interview or outside sources interrupting the interview. The interviews are carried out in person and face-to-face, lasting approximately 45-60 minutes. This enables asking interactive questions and showing the respondent the results of their statements

(Baxter, Courage & Caine 2015, Chapter 9: Preparing to Conduct an Interview), thus ensuring an output both sides can sign.

For selecting interviewees out of a group of unknown people, employee motivations and needs can be used to distinguish different stakeholders (Cooper, Reimann & Cronin 2007, Chapter 4: Understanding Users: Qualitative Research), but for these interviews the selected individuals are always from the same group: super users. Using Wilson's (2014) method as listed above, the resultant plan is as follows:

1. Interview system administrators or super users to find out what the employee profiles are
   Find out which systems are utilized by these profiles

2. The participants motivation is to maintain and improve the system they are responsible for

3. The initial questions are:
   a. What is your job title in the city?
   b. Which systems are you responsible for? How?
   c. Which employee groups utilize these systems? Why?
   d. Can you give a categorical name for each group? What is the common factor?
   e. Can you describe with one phrase each task that needs to be carried out?
   f. Can you categorize the tasks by employee group?
   g. How often does each task need to be carried out?
   h. Do you approve of the publication of this data after the names have been anonymized?

4. The refining (optional) questions are:
   a. What would be the best title for this job?
      Does the title reflect what you do in this job?
   b. How much do you work with these systems?
      Do you consider yourself responsible for these systems?
      Do other people come to you when they have issues with these systems?
      How important are these systems to your department or other departments?
      How important is the IT department for these systems?
   c. Are you part of any of these groups?
      Can you say that you represent any or all of these groups?
      How many employees does each one have?
   d. What is the basis of the name?
      Is the name easily recognizable by anyone?
      Is there a "high level" name that could be used for publishing?
   e. Does each task require using a computer or a system?
      Which tasks require access or a login to a system? Name them.
      Are these all relevant tasks by your best knowledge?
   f. Are these groups closely related by location, department, or job?
      Can an employee be placed into many groups?
      How important would be consider these tasks to your department?
   g. -None-
   h. -None

The final questions are demonstrated in Table 4, which were selected on the basis of the blank employee form in Table 3 and which are the most closely related to the research questions. Each question enables the interviewer to fill the employee form and identify the role of the super user in access management -or the lack of. All questions are critical for the process and can not be left blank or insufficiently answered.

However, during the later phases the information gained from interviews might be proven false and therefore the information should be updated as the research matures or new information becomes available. Note that the question form is accompanied by the initially blank employee profile form.

Table 4. Full question form

Date:	**Place:**
Interviewer:	**Interviewee:**
Department:	**Department:**
Thank you for participating to this interview. The goal is to understand what kind of duties employees carry out that involve system access. You were chosen because you have an active role in either requesting or granting these rights for other employees. Which systems do you grant or request access to?	
Which employee groups need these rights? The group can be given a categorical name according to their job title. For example: secretaries, IT experts, department chiefs, hospital nurses, etc.	
What is the task these rights are a part of? In other words: what is the employee trying to accomplish that requires the access right?	
How important is each task to the employee's department on a scale of 1-3? 1 stands for critical, where the task is central for the daily operation of the department. 2 stands for important, where the task is needed, but can wait or has workarounds. 3 is for beneficial, but not acute and will not hinder the work if inoperable for a while:	
How many employees does this employee group (or groups) have? Give a rough estimate based on your experience from the past year:	

How often is each task carried out from these three: regularly, occasionally, or rarely? Regularly means the task is carried out every day or every week. Occasionally is for a few times a month and rarely is a task that is done only a few times a year:
How often do the user rights need to be edited? Is there a credible log? If not, estimate based on your experience from the past year:
(Demonstrate) The tasks and group name have been written down to a table here. Are they accurate?
Do you approve of the publication of this table in the form you have now seen? No personal names, location information, or system names are kept. The purpose of the publication is to give comparable data for other cities, where similar development might be carried out.
Do you have any observations, reservations, or improvement requests concerning the table created today?

Date	30.12.2099
Testifying as true	John Doe Mary Doe

While the questions and their answers are in a central role, the last part should not be forgotten: the signature. Once the results have been analysed, the validity of the results can be put into question by other employees or claimed to have been misunderstood, so having the signature is a necessary proof for everyone involved and should not be ignored. Even if the studies are for the department itself, the signature will confirm the validity when the documents are processed by different people or when the needs change.

3.4 Analysis Method for The Results

The results are analysed using thematic content analysis. The analysis is done manually, without any assistive software. This is possible because the sample size is

small and the analysis is simple. Once the data is within the table, the first analysis is that of importance. It can be divided into three classes: structure, reliability, and lifetime. Structural importance indicates the relative importance of different parts of the whole (Wey & Xiaoyen 2012. Chapter 3. The Essence of Importance Measures.), which is what each employee profile is: part of a whole. Since at this time there is no central way of knowing what kind of employee profiles exist in the entire city, only partial importance ratings can be created.

Each employee profile consists of tasks, which are individually rated by the super users, and a number of role holders. At a larger scale, every department can also be calculated an importance score based on the profiles belonging to that department. As a prospective subject for future improvements, if all the employee profiles have been recorded and ranked, the information could be used to evaluate which tasks are considered the most important by the super users and how the departments compare.

The priority is an estimate from the super user. To calculate the total importance of each profile, a simple numerical formula is used:

$$i = (Ap * Af) * M$$

i = Importance
Ap = Average priority
Af = Average frequency
M = Number of members

The priority number can be used to estimate if the role should be automated and in which order, for example; which employee profiles give the most benefit for the time and money spent. Although the priority may be low, automating the profile's access management aspects would still simplify the process flow, resulting in time savings. Alternatively, combining similar profiles to larger and more logical ones.

The interviews themselves need to be prepared. The participants need to be briefed and invited, timetables agreed, and premises reserved. The interview should be conducted at a separate premise from the usual working area, with no more than one or two observers present (Baxter, Courage & Caine 2015, Preparing to Conduct

an Interview). In the case city, none were required, since the super users carried out their work independently and mostly without supervision.

After the interview data has been gathered, the numerical data will be listed to a table for comparison, gap analysis, and descriptive statistics. Descriptive statistics describe the sample in a numerical way by using averages, dispersion, minimums, and maximums, for example (Baxter, Courage & Caine 2015, Data Analysis and Interpretation). Gap analysis compares two sets of data to identify the differences, commonly used to compare requirements to the actual output. Gap analysis is a valid method for IT, processes, business direction, organizational structure, and many more. (ITIL Continual Service Improvement 2011, 79.) In other words, gap analysis allows to compare the current state to the desired, future state by asking what is currently in place, what is required to get to the desired state, what is the desired state, and consequently: why this change is beneficial (Peltier 2010, 5.1 Introduction).

The tasks the super users carry out are categorized to logical clusters using the methods presented by Rosing, Scheer, and Scheel (2015, conceptual and logical process classification and categorization). The categorization involves four steps, where the described task is assigned a level, type, tier, and nature after decomposing it to smaller objects. These can be seen in closer detail in Table 5 below. By carrying out this categorization the results can be used to understand what kind of work is involved in the tasks and how demanding it is, complementing the answer to research question 2 ("Which kind of tasks require access rights?").

Tables 5. Dissecting tasks into logical groups (Rosing, Scheer & Scheel 2015)

Categorization	Category
Level	Process area (highest)
	Process group
	Process
	Steps
	Activities (lowest)
Type	Management
	Main
	Supporting
Tier	Strategic
	Tactical
	Operational
Nature	Simple

	Generic
	Complex

Process area is the highest level, abstract grouping of all or a set of process groups (Rosing, Scheer & Scheel 2015, Process Area). In this study, none of the profiles fit to this description, so it is excluded. A process group is a bundle of processes to produce a final output with value to stakeholders (Rosing, Scheer & Scheel 2015, Process Group). A process is a subset of this, producing a single result towards the final output (Rosing, Scheer & Scheel 2015, Process). The individual steps progress the process, consisting of the actual activities, like reading an email. These are the steps the automation needs to accomplish in an acceptable manner and could be listed as acceptance criteria for the automation project.

Management processes are mainly involved in controlling the main and supporting processes. They include planning, budgeting, oversight, and monitoring. Main processes deliver the output and supporting processes ensure the main process can realize this. (Rosing, Scheer & Scheel 2015, Process Type.) For example, IT enabling HR to monitor employee check ins and outs.

Process nature can be either simple, generic, or complex. Simple processes are well understood and repeated. Generic processes are partially understood and repeated, but also involve resources, tasks, rules, and measures. Complex processes change over time and may not be repeated the same day-to-day. (Rosing, Scheer & Scheel 2015, Process Nature.) This reflects the difficulty of the work, since profiles that are complex to maintain require the ability to process new and adjust accordingly, whereas simple profiles largely repeat the same. For the automation efforts, simple profiles should be the first to go.

4 Results of the Research

The methods have been explained in the previous chapter and the study has been carried out accordingly. The results and insights are reported here. First, the employee profiles are listed in length and their backgrounds explained. In chapter 4.2 the employee profiles are compared for similarities and possible weaknesses. In chapter 4.3 the question about the effects on management are evaluated, including interfaces to other departments. Lastly, the shortcomings and weaknesses of the study are noted to improve the quality of later iterations.

4.1 Resultant Employee Profiles

The first representative was from the department of urban planning. A user profile was drafted to Table 3 and filled with duties that involve system access. The system and super usernames have been removed and descriptions have been generalized to preserve the security of the case city. For example, using domain computers requires AD accounts or equivalents, depending on the operating system, but instead of stating AD the need of the super user is described. This also aids in understanding the desired outcomes rather than the technology.

The resulting employee profiles can be seen in the tables below. The original interview forms are classified for the same security reasons, thus, no references are written. These tables are the final output and the core of the interviews, providing insight on what the profile holders actually do that requires access rights.

Table 6. Urban Planning Customer Service Person	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Access domain computers for work	3	x		
Access city email software for work	3	x		
Read confidential building information within the city's real estate software	3	x		
Process permits within the city's real estate software	3	x		
Modify locational information within the city's real estate software	3	x		
Read scanned building permits	2		x	
Confirm payments on a 3rd party's website	2		x	
MEMBERS: **20**	IMPORTANCE: **147**			
	(2.71*2.71)*20= 147.35			

Customer service personnel in urban planning use the computers of the city to access email, read real estate information, process payments, and update owner information while servicing the customers in person, over email, or a phone call. Because they process payments, they may also handle money while on the premises. To be able to do their job, they require access to building and personal information, such as addresses, owners, permits, builders, and current residents. Some of this information is confidential.

Table 7. IT Account Administrator	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Access domain computers	3	x		
Access the city's email service	2	x		
Use network printers	1		x	
Read intranet news, documentation, and phonebook	2	x		
Access document management system for manuals	2	x		
Access network shares for access changes	3	x		
Maintain AD user groups	2	x		
Create and maintain email accounts	2	x		
Create and maintain ERP accounts	2	x		
Create and maintain email distribution lists	2	x		
Create and maintain shared calendars	2	x		
MEMBERS: **5**	IMPORTANCE: **30**			
	(2.09*2.91)*5=30.41			

IT account administrators are generalists, whose main interest is to provide and maintain AD accounts. The role takes a duly filled account request form as an input and produces a usable domain account, with the requested access rights and email address, as an output. For the role holder to do his job, he needs a personal email address, a domain computer, and an admin access to the control panel of the email software, domain user management, and an ERP system.

Table 8. Network Share Administrator	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Access company email system	2	x		
Access a domain computer	3	x		
Grant access to network shares	3	x		
Grant access to Sharepoint rooms	3		x	
Grant access to an information management system's login screen	2		x	
MEMBERS: **15**	IMPORTANCE: **101**			
	(2.60*2.60)*15=101.40			

Network share administrators are responsible for the network shares of the company. While the role is similar to IT account administrator, the output from the service is different: it grants access to correct SharePoint rooms, an information management system (IMS), or a network share. The input required for the service is also different: the network share administrator need to know where the employee works and if the access request has been verified by his foreman. For the role holder to be able to do is job, he needs a personal email address, a domain computer, and an admin access to network share servers, sharepoint, and IMS.

Table 9. Population Registry User in Fire and Rescue	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Grant access to a person's information in a national population registry	3	x		
Grant access to real estate information in a national system	3	x		
Use a domain computer	3	x		
Use company email system	3	x		
MEMBERS: **4**	IMPORTANCE: **37**			
	(3.00*3.00)*4=37.00			

The population registry users in the Fire and Rescue Department are concerned of the residents and information of a premise during an emergency that involves said premise, e.g. fire. In these cases, the population registry users find out who and how many people live in the premise, if hazardous materials are present and acquire floor plans as well as any other information that might aid the rescue personnel. Some of which may enter a burning premise.

Table 10. ICT Purchase Agent	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Answer phone inquiries and provide purchase consultation	1		x	
Read for new purchase orders in a helpdesk system and update the status	2	x		
Lodge a purchase and its details to a supplier's purchasing system	2	x		
Read an asset registry for naming new computers	1	x		
Register computers under employee names in an asset registry	1	x		
Remove disposable computers from an asset registry	2	x		
Read supplier notifications in personal email	2	x		

Approve delivery lodgers over email	3	x		
Read accounting details in a document archive	3	x		
Approve and register computer details to a supplier leasing system	3	x		
Read and approve new invoices in a purchasing system for non-leased items	3		x	
MEMBERS: **20**	IMPORTANCE: **118**			
	(2.09*2.82)*20=117.88			

ICT purchase agent is a profile in which the employees purchase and manage ICT hardware and software purchases. In some cases, they also handle ICT service purchases from outside vendors. In the case city, the role is work intensive and crucial for the continual replacement of computers, screens, and printers. After purchase, the agents follow the progress of the delivery, installation, and approve the invoice at the end of the process. While the changes in personnel are rare, they require multiple, special access rights to be able to do their work. These rights are not well known even in the department.

Table 11. Antivirus Administrator	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Create a remote desktop connection to central AV server for support	3	x		
Create remote desktop connections to client computers for support	3		x	
Maintain and update the AV database	3	x		
Sanitatize compromised clients	3		x	
Upgrade AV software versions and deployments	2	x		
Maintain and change client firewall settings	2		x	
Maintain and change AV settings	2		x	
MEMBERS: **2**	IMPORTANCE: **13**			
	(2.57*2.43)*2=12.49			

Antivirus administrators manage the AV software on client computers. The profile requires full administrator access to central AV server and all clients. It is a privileged role that, if compromised, would also compromise the network. A client firewall is part of the software. The required access rights are not many and well documented, but their impact on the security of the network is great.

Table 12. Global Cloud Service Administrator	PRI	REGUL.	OCCAS.	RARE.
Distribute and update mobile phone configurations via cloud-based phone management system	3			x
Distribute and maintain mobile phone software via cloud-based phone management system	2			x
Maintain synchronizations between the cloud-based management system and local domain	3	x		
Create cloud applications for online authentication	1			x
Maintain and repair cloud applications for online authentication	1			x
Login to cloud management portal as a global admin for changes	3	x		
Admit new members to global admin role	1			x
MEMBERS: **2**	IMPORTANCE: **6**			
	(2.00*1.58)*2=6.32			

Global cloud service administrator is a profile with only two regular tasks but a number of rarely carried out configurations. The domain-to-cloud synchronization is checked regularly after login, however, tasks related to mobile phone configurations, apps, and memberships are carried out only at request. This is because the tasks are further divided into other roles within the cloud, which were not clear at the time of the interview due to the new nature of the system. The roles are divided and clarified over the next year, resulting in new access rights and guidelines.

Table 13. Cash Registry Super User	PRI	REGUL.	OCCAS.	RARE.
Login as an admin to cash registry using a software specific account	3			x
Create new accounts for approved users	1			x
Verify approvals before account creation	3			x
Verify the presence of a domain account before creation	1			x
MEMBERS: **2**	IMPORTANCE: **4**			
	(2.00*1.00)*2=4.00			

The case city uses specific software to track how cash payments are processed. The processes around the software are well established and the super users rarely change, involving only one change during the past year, which places the current importance of the role near minimum. The super users are responsible for granting

access to the cash payments system and verifying the people requesting access are who they claim to be. Only few people know about the role.

Table 14. IT Ticket Master	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Follow helpdesk's ticket lifespan and statistics	2	x		
Assign owners to helpdesk tickets	1	x		
Assign and coordinate helpdesk shifts	2	x		
Manage helpdesk employee resourcing, priorities, and time	3	x		
Access asset and ticketing software	2	x		
Develop asset and ticketing system	3		x	
MEMBERS: **2**	IMPORTANCE: **12**			
	(2.17*2.83)*2=12.23			

Helpdesk tickets are generated from emails and phone calls, which is a process the IT ticket masters maintain. The ticket masters monitor the ticketing statistics, employee attendance, and assign helpdesk shifts, adjusting the workload as the situation requires. They do not have a foreman's role or rights, but they facilitate the continual operation of the helpdesk. The profile also involves employee resourcing and development recommendations. The profile is labour intensive and requires daily involvement. Without the correct access rights, the ticket master cannot supervise the status of tickets within the system.

Table 15. Firewall Specialist	**PRI**	**REGUL.**	**OCCAS.**	**RARE.**
Define and maintain firewall rules and configurations	3	x		
Order changes from the firewall SaaS provider	3	x		
Confirm changes by authenticating via SMS	3	x		
Login to firewall SaaS website as an admin	3	x		
Define VPN rules and configurations	3		x	
Troubleshoot connection, port, and routing issues	3	x		
MEMBERS: **3**	IMPORTANCE: **26**			
	(3.00*2.83)*3=25.47			

A firewall specialist is the owner of a network firewall. The firewall is purchased as a service (SaaS) from a commercial provider, but the specialist ensures the settings and configurations meet the needs of the organization. He also troubleshoots issues related to connectivity and cases where the firewall is suspect of causing connection problems, e.g. when a new program fails to connect to the Internet. Although the

importance of the role is only 26 and the role is very stable, the changes in the software have the potential to affect the entire network.

As per table 1, the overall view of these ten roles has been listed to Table 16. The importance of each profile has been added to the table:

Table 16. Confirmed Employee Roles In the Case City

ID	i	Employee profile name	Primary purpose
Table 5	147	Urban Planning Customer Service Person	Customer service, sales
Table 6	30	IT Account administrator	Domain account creation
Table 7	101	Network Share Administrator	File access control
Table 8	37	Population Registry User in Fire and Rescue	Fire and rescue support
Table 9	118	ICT Purchase Agent	Hardware purchasing
Table 10	13	Antivirus Administrator	Clientside AV/FW maintenance
Table 11	6	Global Cloud Service Administrator	Cellphone security, maintenance
Table 12	4	Cash Registry Super User	Cash system access control
Table 13	12	IT Ticket Master	Helpdesk ticketing, resourcing
Table 14	26	Firewall Specialist	Network firewall maintenance
TOTAL	494		

The final value (TOTAL) represents the total importance rating of these profiles. If the study was repeated in multiple departments, then their individual importance and totals could be compared. In the scope of this study, the comparable values would indicate where to spend the money, which profiles should be inspected first, and if there is sufficient grounds for automating at all. If the study was repeated in multiple departments, the total value could indicate which departments could benefit the most and how they compare.

4.2 Employee Profile Results

The employee profile tables yield information that can be used to gain insight of the work that is being carried out. Some of the information is specific to the profile while others are shared by all or most of them. For example: the use of domain computers and city email. First the shared factors are examined, including their importance, and general observations made before moving on to the profile specific factors.

Examining importance ratings and arranging them from the highest value to the lowest, the results can be seen in table 16 below. The table divides these profiles into three groups where there is a clear gap between the values: yellow, green, and red. The first gap is between a network share administrator and a population registry user

in fire and rescue, where the difference in importance is 101 – 37 = 64 points. The next gap is between a firewall specialist and a antivirus administrator, where the difference is 26 – 13 = 13pt. While the second gap is not as large as the first, it is still noticeable when the average increment in red group is (1 +6 + 2) / 3 = 3 points and green (7 + 4) / 2 = 5.5.

Table 17. Profiles arranged by importance

ID	Employee profile name	$A_{priority}$	$A_{frequency}$	Members	i
Table 5	Urban Planning Customer Service--	2.71	2.71	20	147
Table 9	ICT Purchase Agent	2.09	2.82	20	118
Table 7	Network Share Administrator	2.60	2.60	15	101
Table 8	Population Registry User in Fire and--	3.00	3.00	4	37
Table 6	IT Account administrator	2.09	2.91	5	30
Table 14	Firewall Specialist	3.00	2.83	3	26
Table 10	Antivirus Administrator	2.57	2.43	2	13
Table 13	IT Ticket Master	2.17	2.83	2	12
Table 11	Global Cloud Service Administrator	2.00	1.58	2	6
Table 12	Cash Registry Super User	2.00	1.00	2	4
TOTAL	--	2.42	2.47	71	494

Looking at these three groups, the decision would be to prioritize the automation efforts accordingly and begin with the yellow group. Note that this does not imply that the other groups are not important, because the formula places an emphasis on the number of profile holders. Therefore, profiles with more beneficiaries are ranked higher. The yellow group has a total of 20 + 20 + 15 = 55 members whereas the reds have only 8, which means that any money spend on the yellow profiles will have 55 – 8 = 47 more beneficiaries.

At an individual level, one could observe that scores that are close to each other mean that those roles are of roughly equal value, such as an antivirus (AV) administrator and a IT ticket master. Looking at their tasks, priorities, and task regularity, the tables indicate that they have roughly the same number of tasks, but the AV administrator performs critical tasks less often whereas the IT ticket master performs non-critical tasks regularly. Placing them at the same importance. If the AV administrator did not have the required access rights, it could result in critical incidents after a long period of time. However, if the IT ticket master did not have the necessary rights, it would hinder his work and ticketing immediately. Alternatively: if these rights are not removed when the employment ends, the AV

administrator would have much more potential for critical incidents that are harder to spot.

The average priority implies that most participants consider their tasks either important or critical. At the same time, these tasks are carried out either regularly or occasionally, with only a few tasks that are rarely carried out. If all the profiles were mapped within a single department, it would be interesting to see how these values would change. Especially if the rarely carried out tasks are listed the last or easily forgotten.

4.3 Effects on Access Management

The information that was gained can be used to further the automation of access management and ease the burden of management, allowing the organization to gain more with less. In chapter 4.2 the priority of the profiles was determined, listing three employee profiles that should have their access rights automated first. Focusing on the tasks that require access rights, Table 18 was drafted.

Table 18. First three employee profile candidates for access automation

Urban Planning Customer Service Person
Grant/remove access to the real estate software
Grant/remove access to building permits on a network share
Grant/remove access to a 3rd party website
ICT Purchase Agent
Grant/remove access to a helpdesk system
Grant/remove access to a supplier leasing system
Grant/remove access to the asset registry
Grant/remove access to the document archive
Grant/remove access to the purchasing system for non-leased items
Network Share Administrator
Grant/remove access to network shares
Grant/remove access to Sharepoint rooms
Grant/remove access to an IMS login screen
All Employees
Grant/remove access to domain computers
Grant/remove access to a personal email account

The table shows that the access automation requires integration to 11 systems with specific inputs and outputs. These variables are not defined here and are better left

to an actual integration project, which may use this information as a starting point. The project would have to contact the super users for the details, which is a natural bridge for the negotiations needed to change the work process -the work the super users carry out- and defining the critical success factors.

What is common to all the profiles is that they require a reliable access to domain computers, a stable network, a usable AD account, and a secure email account. Consequently, if the access to computers and email is disrupted, then the rest of the work cannot be carried out. As an interesting improvement prospect, should the interviews reveal employee profiles that do not use computers, could they be improved by computerization?

To analyse the effects on access management, a gap analysis is made by comparing the current situation of these 10 employee profiles to an ideal situation. As a basis of this study, explained in the previous chapters, the ideal situation moves the currently manual and repetitive labour to the machine. The comparison can be seen in Table 19 below. *Comms* stands for *communications,* such as sending an email, a telephone call, or contacting directly a person responsible of granting the access. Each of which requires a response, attention, and time.

Table 19. GAP Analysis of current and ideal situation

Urban Planning Customer Service Person	**Current state**	**Future state**
Access to a real estate software	Granted, removed, and changed manually by two helpdesk employees in two different departments. Internal comms required	Granted automatically by machine, based on employee contract data. No comms required
Access to building permits on a network share	Granted and removed manually by a helpdesk employee. Internal comms required	Granted automatically by machine, based on employee contract data. No comms required
Access to a 3rd party website	Manually requested by a super user Internal and external comms required	Automatically generated emails to the 3rd party
ICT Purchase Agent		
Access to a helpdesk system	Granted, removed, and changed manually by a super user. Internal comms required	Granted automatically based on employee contract data. No comms required
Access to a supplier leasing system	Manually requested by a super user. Internal and external comms required	Automatically generated comms to the 3rd party
Access to the asset registry	Manually granted by a super user. Internal comms required	Granted automatically based on employee contract data. No comms required

Access to the document archive	Manually granted by a helpdesk employee, guidance required from other role owners	Granted automatically based on employee contract data. Instructions delivered automatically
Access to a purchasing system for non-leased items	Manually requested by a super user Internal and external comms required	Automatically generated comms to the 3rd party
Network Share Administrator		
Access to network shares	Granted, removed, and changed manually by a helpdesk employee Internal comms required	Granted automatically based on employee contract data No comms required
Access to Sharepoint rooms		
Access to an IMS login screen		
All Employees		
Access to domain computers	Granted, removed, and changed manually by a helpdesk employee Internal comms required	Granted automatically based on employee contract data No comms required
Access to a personal email account		

Knowing what is required to automate the access management is the result of this study. The next step is how to carry out these changes. As seen from the table, the most common access management tasks involve adding and removing members from user groups, which may be located either in the system itself, on a server, on a workstation, or in AD. Knowing where the access groups are and how they work is part of the profile owner's job, but the knowhow may not be documented or the documentation is not easily available when it is needed, by those who need it. A new employee profile member may not know who to consult for the information, the tutor is not immediately available, or the quality of tutoring is not sufficient. Elevating the need for clear communications, which is required in all tasks. With automation, the need shifts from promoting communications to tuning the documentation and automation rules, which can deliver the instructions the moment a new employee profile member is appointed.

The tasks the super users carry out can be categorized for insights. Following the method presented by Rosing, Scheer & Scheel (2015) to further answer the initial research question of *what kind of tasks require access management*, the categorized tasks can be seen in appendix 1. The tasks were placed into the categories logically, which lead to a result where most of the tasks were either individual tasks in a process or processes with specific outcomes. Half of the tasks were supporting tasks, enabling the main tasks to be carried out, whereas only 9% were management related tasks. Meaning that 91% of the listed tasks were directly involved in access

management and 98% with the operative side of it, correlating with the focus of the interviews.

71% of the tasks were simple, 23% generic, and 6% complex. This means that a large part of the tasks are easy to carry out and repeated the same way. Consequently, even if some of the tasks are too complex to automate, at least 71% and up to 94% of the tasks pose no obstacle. In Figure 6 an automation chart was presented, but it did not specify the practical steps needed to automate the process of access management. Using the information gained from the interviews, the necessary steps can be presented to the integration software and system providers in a swim lane flowchart, which is also known as a sequence diagram.

A sequence diagram describes a process and is important to the design of process-driven applications, both at an application and business level. It provides a common, understandable language for all involved parties, such as the super users, programmers, and system specialists. (Stiehl 2014, 2.4 The Role of BPMN (Business Process Model and Notation) for Process-Driven Applications: Basics.) In practice, the swim lanes are a visually easy way to grasp the idea of how a process needs to progress and what are the roles of the different stakeholders.

In Figure 7, the stakeholders are placed to a sequence diagram with a number of possible tasks they may want to carry out. These tasks can generate value to the city by enabling information-based decision making. The automation can grant access to specific software and also report of the changes to financial management, allowing them to better control the use of licenses. As in ITIL Service Strategy (2011, 201), the purpose of financial management is to identify the costs of providing services, such as access management via helpdesk, and account for the money spend on supporting them.

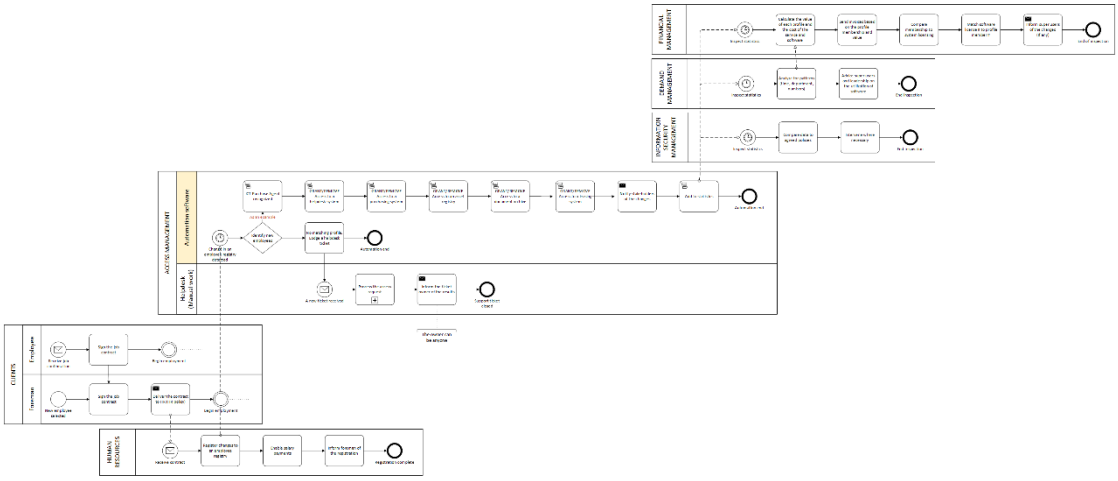

Figure 7. A simple IAM diagram to visualize the role of various stakeholders. A larger picture is available in appendix 4

Other stakeholders are demand management, information security management, helpdesk, foremen, and human resources. As explained before, demand management seeks to understand what initiates demand for services, what are the different user groups, and ensuring the resources are on par with the demand - without overprovisioning (ITIL Service Strategy 2011, 245). In the case city the employee profiles are what the demand management needs to understand the users and automation is what can provide an additional stream of data for understanding the utilization of IT's resources.

Note that an access request needs to be verified in two ways: (1) that the one requesting access is who they claim to be and (2) the need is legitimate (ITIL Service Operation 2011, 111). However, an automated task is a standard, pre-authorized change that always follows a preset pattern. This leaves the responsibility of the change to the source of the information, which should be clearly stated in the information security policies. In the case city, the source of the information is the foreman of the new employee, who may have become accustomed to HR and IT "just knowing" what to do or letting the employee request the change from helpdesk. Automation would introduce an organizational change when the responsibility of knowing who-is-who shifts from helpdesk to the foremen themselves, which may prompt change resistance. Especially if the information security policies are not well acknowledged or agreed on.

The shift in responsibility does not involve only the foremen, but also the HR and super users. Good access management requires regular review of the employee profiles (ITIL Service Operation 2011, 113), which leans on input from both. If the changes come with delay or the profiles are outdated, then the automation is not performing at an expected level and the tasks easily default to manual labor. This eventuality should be accounted for in the policies established between HR, IT, and super users.

4.4 Criticism and Improvement Considerations for Later Iterations

During the execution of this study several issues and improvement considerations were discovered after interviewing the super users. Should this study be repeated later on as a work project, with clearly expected returns, one of the first things to consider is if interviewing is the best method for gathering data in that particular organization. Using the question form presented in Table 4, each interview took approximately 45 minutes from the interviewee and the participant, 15 minutes of preparation, and roughly an hour of cleaning and understanding the completed forms. This translates to 2.75 hours of work per interview and the attention to arrange them. If a later iteration would also want to record and transcribe the spoken words, which was not done in this study, the time required could double.

This raises the question if the data could be gathered without interviews by using a tailored, guided webform, for example. This improvement idea is not without merit, however, the practical experience proved that many participants were of varying expertise. The fastest interview took only 10 minutes whereas the slowest took 1.5 hours, where the participant was clearly unwilling to divulge the information. If the goal is to gather a per centage of employee profiles from a large count of super users, then email and webform could be acceptable. For example: attempting an acceptable return rate of 20% out of 50 individual super users. However, if the number of super users is much less or unknown, like in the case city, then the interviews are a more reliable way to acquire data.

In hindsight, if this study had attempted to acquire the data in any other way but interviews, the participants either wouldn't had replied, replied at a much later time,

or the replies would had been too low quality to be useful. The critical success factors were the engagement by the interviewer and the ability to direct the participants to the questions. If the interviewer is not able to engage the participants, preferably in person, the interviews will fail. A solution could be to create a webform that allows only specific actions, such as selecting task priority from a scale of 1-3, and acquiring sufficient authority from the leadership to state that filling the form in a set deadline is mandatory.

The practicalities of arranging the interviews highlighted the importance of preparing the interviews. Holding the interview at the participant's usual office should be avoided in most cases, even if requested by the participant, since the interview is bound to be interrupted by phone calls, messages on the screen, and passing colleagues or customers. In one such case the participant lost interest in the interview altogether, causing the interview to be cancelled and repeated at a later date.

Briefing the participants should not be overlooked, especially if the project does not have a formal backing by the leadership. The backing should be acquired as soon as possible, because the first thing every participant asked was why the interview was necessary and, right after, who authorized them. The authorization could be made more visible by adding it to the question form to alleviate security concerns. Authorization states who signed off the plan, who owns it, and who it is meant for, giving weight to its execution (ITIL Service Strategy 2011, 153). The authorization further enables the interviewer to keep the participants engaged.

The introduction could also include demographics, which might garner interest in the department of human resources or just the local leadership. Demographics can give a picture of who the super users and profile holders are by, for example, describing age, ethnicity, gender, amount of time in the role, and the length of their employment (Goodwin & Cooper 2009, Identifying the Number and Type of Interviewees). These demographics could prove valuable if the employee profiling is carried out in a larger setting or as a part of a readily existing demographic practise.

Another aspect to consider in later iterations is the total scope of the project. If the project begins with a sample of 10 profiles to automate and succeeds, then what is

the total number of profiles to automate? Is there any way to estimate or should the project simply proceed department-by-department? As seen in chapter 2.2, the case city has 23 lower level departments, Brisbane 41, and Perth 27. Would this be a fair progress indicator? Instead, a better solution could be to include the discovery of all, or most, super users and their access management components to the initial, pre-project study. This would require visiting every department, either by a project member or a business relationship manager, but since it does not involve in-depth interviews or specifics, it's possible to keep the visits brief.

There might also be a way to calculate the importance of each employee profile in a more expressive way. The current method places the main importance on the number of profile members, which does correctly emphasize how many would benefit from automating the access related tasks, but some importance could be placed on network-critical profiles and profiles that have many tasks. Thus the formula could be revised to a more mathematically competent version or replaced by an industry standard, if such exist.

The original interview form fulfilled the required task, but could still be better. The current form cannot be filled by the participant alone and was not designed for such, but by revising the form to a simpler, more pre-defined format it opens a chance to gather the data over email -without interviews- while simultaneously easing the interviews by allowing the participant to fill out the data. During this study, the interviewer had to fill out the form while interviewing and, in the end, let the participant check the paper, which would be unnecessary if the participant had the paper all along. Because of these factors, the revised question form is presented in Appendix 3, providing more clarity and an easier interview experience.

This study did not have a project group to carry out the changes in the case city, so a return of investment (ROI) was not calculated. Employee profiling is, in the end, a service provided by one of the city's departments to the rest. The success of providing this service is measured by its ROI (ITIL Service Strategy 2011, 106). In the case of employee profiling, the primary monetary value can be calculated from time savings. For example: if the interview form had included a question about the duration of each task, then it would had been possible to calculate the ROI by estimating how each working hour costs and multiplying that with the number of

repetitions. The more often the tasks is repeated, the bigger the savings, multiplied by the number of profile members.

This has been noted in the revised question form, since presenting the monetary savings would strengthen the case for continuing the automation efforts. ROI does not, however, include softer factors, such as the increased reliability of access management and the agility of making changes when doing so requires no labour. These are better described as intangible benefits and listed separately (ITIL Continual Service Improvement 2011, 108). Otherwise the leadership may not realize the full value of the initiative.

Lastly, employee profiles are about ensuring that people have sufficient access to systems when they need it. Access rights that need to be revoked when there are no tasks to require them. Consequently, physical access management and actual guards require the same knowledge. In other words: if a city employs guards, in places like hospitals and social security offices, then these employees need to be aware of who is and who isn't allowed to enter a premise. Employee profiling could have close ties with them, providing the information automatically when the changes are applied. Depending on the agreement with the departments, these access rights could be halted for vacations and off-hours as well.

5 In Conclusion

Continual service improvement is about increasing efficiency, maximizing the outputs, and minimizing the costs (ITIL Continual Service Improvement 2011, 35). Access management and the automation of access related tasks is one way to achieve this, resulting in doing more with less. If a city grows, so does the workload of maintaining access rights. Moving the mundane tasks for a computer to perform is one way to cope with the situation. The categorized tasks and statistics (Appendix 1) show that most of the individual tasks are relatively simple, therefore, identifying these in the organization and automating them would benefit both the administration and the end-users.

The Deming Cycle is a cycle consisting of four stages: plan, do, check, and act (PDCA), which is a fundamental part of many quality standards (ITIL Continual Service Improvement 2011, 38). By carrying out several iterations of PDCA, new baselines and, thus, higher quality is established with each new round. This applies to this study as well, this chapter concluding the first cycle and proving that the development is iterative. A city organization needs to be able to accommodate this by preparing for changes in the data collection process and how the access right automation is carried out. Meaning that the city needs to plan for the interview and how the changes are put into use, carry out the plan, periodically check on the progress, and act accordingly.

As a final output of this study, a new question form and a process checklist have been presented in Appendix 2 and 3. Together these will help a reader to repeat the study in a different environment, but to reach the same goals. The goals which were:

1. Who are the employees that process or need access rights?
    - Goal 1: Interview super users to define employee profiles
        - Metric: 10 employee profiles defined
2. What kind of tasks require access rights?
    - Goal 2: Define what kind of tasks are involved
        - Metric: 100% of access related tasks stated
        - Metric: 100% of access related systems stated
3. How important are these profiles to access management?
    - Goal 3: Define how important each employee profile is
        - Metric: Importance rating per employee profile

After discovering the 9 super users with a specialist role in any system, 10 employee profiles with specific access right requirements were drafted, thus reaching goal 1. Each profile included a list of necessary tasks which were then categorized, revealing that most tasks are simple in nature and pose no obstacle to automation. The access related systems were also noted and the resultant employee profiles were rated by their importance to access management, emphasizing the number of profile members. The ratings created a priority list, which could be utilized by an automation project as a starting point for the efforts. Although the combination of these systems may be unique to the case city, the tasks are universal. For example: any city with a fire and rescue department most likely has a role for employees gathering information about the targets of rescue operations. Consequently, profiling could also create a basis for comparing the functions of different cities.

Before a city organization begins a larger scale effort, having a smaller test run is recommended. Not only for gathering the employee profiles, but to also test the organization's capabilities in bringing the automation efforts to concrete results. This study recommends that cities first profile and document their employee's access rights, including their justifications, and then carries out a small scale testing run. Based on the results, a larger project charter can be created and costs calculated.

To aid in chartering for the project, a checklist was created to Appendix 2. A checklist is a condensed guide and a tool for reducing risks in complex tasks by ensuring simple errors are not made (Wilson 203, Overview of Checklists). The checklist should be used to ensure all steps in a task have been completed (Wilson 2013, When Should You Use a Checklist?), but also to ensure that nothing has been omitted. In this case, the checklist is a behaviour sampling checklist, where the important actions have been listed. Failing to do all the tasks does not mean the profiling will not succeed, but having them done will aid in achieving success.

Collecting sufficient information during the interviews and asking the right questions is important for the success of the access automation efforts. If the important tasks are omitted, then the super user may still remain involved in the upkeep of the process. The automation should aim to completely remove the manual labour from simple and routine tasks, enabling the super users to focus on monitoring and handling a minority of exceptions. One of the important questions was left out in the

original question form, the question regarding the duration of each task, and so the question form was revised. The revised form can be seen in Appendix 3, which should be used for later iterations and improved in the process. The duration of each task is important for calculating how much time the automation saves, which in turn enables the project to estimate monetary savings through the value of each employee hour. A benefit that is understood in any city.

To return to the original issue, which is the constant need to change and manage access rights in helpdesk, the study proved that this work can be automated if the employee's needs are known. It proved that the needs in this sample of 10 were mostly simple and the profiling can be used to bring clarity to the automation efforts, which ultimately aims to eliminate the manual labour. Once eliminated, not only does it decrease the workload and difficulty of working in helpdesk, but also bring ease, agility, and security to the business side. Or in other words, by ITIL: "the more roles and groups exist, the more likely that role conflicts will arise" (ITIL Service Operation 2011, 113). This may be less of an issue in a small city, but the earlier the issue is recognized, the easier it will be to track the roles as the city grows, avoiding the need to interview a large number of super users and enabling the management to understand what drives demand for access rights.

Recognizing the employee profiles also creates a new business opportunity. One of the major activities of demand management is to identify and influence customer demand through incentives, penalties, or differential pricing (ITIL Service Strategy 2011, 246). Once the employee profiles have been recognized and if the IT's budget is tied to the use of its services, then the IT can charge other departments based on the number and importance of employee profiles, since the maintenance of access rights is a critical IT service. Connecting information security policies to this service could also encourage departments to cooperate with the IT if the establishment and maintenance of access policies is viewed as a *paid* service.

In conclusion, profiling and automation should not be carried out in isolation. Once the first results are in, technical personnel with sufficient amount of time and knowhow should be available to take the next step in bringing the results to practise. All of which costs money, which is why a ROI analysis should be considered and if the costs could be divided with other parties. Other cities with similar needs and

structure, for example. More important, though, is to begin from somewhere and evolve the design as more information becomes available. With iterative design and implementation, the organization also has more time to adjust to the changes, which might shift responsibility from helpdesk to HR and foremen themselves. A shift that is not solely about code and systems, but how the employees behave and what they expect from IT.

This study was of limited scope, proving that profiling through interviews is a valid method to gather data for easing the burden on helpdesk, but only for one city. Only after the profiles have been compared between multiple cities it is possible to identify how reliable the results are in general. Which is another task to add to the next iteration of employee profiling and access management automation.

References

Baxter K., Courage C., Caine K. 2015. Understanding Your Users: A Practical Guide to User Research Methods, Second Edition. Morgan Kaufmann Publishers: Burlington. ISBN 9780128002322.

Bott E., Siechert C., & Stinson C. 2011. Windows 7 Inside Out, Deluxe Edition. Microsoft Press: Redmond. ISBN 978-0735656925.

Campi N. & Bauer K. 2009. Automating Linux and Unix System Administration, Second Edition. Apress: New York. ISBN 978-1430210597.

COBIT5: A Business Framework for the Governance and Management of Enterprise IT. Illinois: ISACA. Accessed 22 June 2019. Retrieved from https://isaca.org/COBIT/Pages/COBIT-5.aspx.

Cooper A., Reimann R., & Cronin D. 2007. About Face 3: The Essentials of Interaction Design, 3rd edition. John Wiley & Sons: New Jersey. ISBN 978-0470084113.

Clines S., & Loughry M. 2008. Active Directory For Dummies, 2nd Edition. John Wiley & Sons: Chichester. ISBN 9780470287200.

Dunphy G. 2009. Pro BizTalk 2009. Apress: New York. ISBN 978-1430219811

Farenden P. 2012. ITIL for Dummies. John Wiley & Sons: Chichester. ISBN 978-1119950134.

Ferreira D. 2013. Enterprise Systems Integration: A Process-Oriented Approach. Springer: Kista. ISBN 978-3642407956.

Ford J. 2007. Microsoft Windows PowerShell Programming for the Absolute Beginner. Cengage Course Technology: Boston. ISBN 978-1598633542.

Goodwin K. & Cooper A. 2009. Designing for the Digital Age: How to Create Human-Centered Products and Services. John Wiley & Sons: Chichester. ISBN 978-0470229101.

Hill D. 2010. Data Protection: Governance, Risk Management, and Compliance. Auerbach Publications: Washington. ISBN 978-1439806920.

Johannesson P. & Erik P. 2014. An Introduction to Design Science. Springer: Kista. ISBN 978-3319106311.

Organisaatio. A page on the City of Jyväskylä's website. Accessed 30 April 2019. Retrieved from https://www.jyvaskyla.fi/organisaatio.

Khan E. & Huma A. 2015. Research Methods of Computer Science. Laxmi Publications: New Delhi.

Kuo W. & Xiaoyan Z. 2012. Importance Measures in Reliability, Risk, and Optimization: Principles and Applications. Joh Wiley & Sons: Chichester. ISBN 978-1119993445.

Laitinen P. 2016. Concept for IT Demand Management: Case UPM-Kymmene Oyj. Espoo: Laurea. Degree thesis. Retrieved from http://www.theseus.fi/bitstream/handle/10024/112077/Laitinen_Pekka_korjattu.pdf;jsessionid=8593C073B4FECACDB5C747812B334096?sequence=1.

Malcher, M. 2018. DBA Transformations: Building Your Career in the Transition to On-Demand Cloud Computing and Extreme Automation. Apress: New York. ISBN 978-1484232422.

Martikainen O. 2017. Sharpening Customer Profiling for Wormhole IT. Jyväskylä: JAMK. Retrieved from http://urn.fi/URN:NBN:fi:amk-2017060913144.

Minasi et al M. 2014. Mastering Windows Server 2012 R2. John Wiley & Sons: Indianapolis. ISBN 978-1118289426.

Miles M., Huberman A. & Saldana J. 1994. Qualitative Data Analysis -A Methods Sourcebook. 3rd edition. SAGE Publications: Thousand Oaks. ISBN 78-1452257877. Retrieved from https://umich.instructure.com/courses/122789/files/4114526/download?verifier=8LwPnM4b7RQbxwiVdNLRkFZtOc71OOtFZOwLlE3U&wrap=1.

Morris H. & Gallacher L. 2016. ITIL Intermediate Certification Companion Study Guide: Service Lifecycle Exams. John Wiley & Sons: Indianapolis. ISBN 978-1119012214.

Hennink, M., Hutter I., & Bailey A. 2011. Qualitative Research Methods. London: SAGE Publications. ISBN 978-1412922265.

The City of Brisbane 2019. Brisbane City Council -Organizational Chart as of April 2019. Accessed 1 May 2019. Retrieved from https://www.brisbane.qld.gov.au/about-council/governance-strategy/organisational-chart.

The City of Perth 2018. Council Organisational Structure Chart. Accessed 1 May 2019. Retrieved from https://www.perth.wa.gov.au/council/city-of-perth-staff/organisational-structure.

The Ministry of Finance 2017. Kuntien lukumäärä ja vireillä olevat muutokset. Accessed 22 June 2019. Retrieved from http://vm.fi/kuntien-lukumaara.

The Official Introduction to the ITIL Service Lifecycle. 2007. London: TSO. ISBN 978-0113310616.

Edgar T. & Manz D. 2017. Research Methods for Cyber Security. 1st Edition. Syngress Publishing. ISBN: 9780128053492.

Loshin D. 2011. The Practitioner's Guide to Data Quality Improvement. Morgan Kaufmann Publishers: Burlington. ISBN 978-0123737175.

Tommila, P. 1972. Jyväskylän kaupungin historia 1837-1965 I. Jyväskylä: J.K. Gummeruksen kirjapaino.

ITIL Continual Service Improvement. 2011. London: TSO. ISBN 978-0113313082.

ITIL Service Transition. 2011. London: TSO. ISBN 978-0113313068.

ITIL Service Operation. 2007. London: TSO. ISBN 978-0113310463.

ITIL Service Strategy. 2007. London: TSO. ISBN 978-0113310456.

Organization chart of the City of Jyväskylä 10.08.2018. Accessed 10 October 2018. Retrieved from https://www.jyvaskyla.fi/organisaatio.

Peltier T. 2010. Information Security Risk Analysis, Third Edition. Auerbach Publications: Washington. ISBN 978-1439839560.

Rob T., Boyce J., & Shapiro J. 2015. Windows 10 Bible: The Comprehensive Tutorial Resource. John Wiley & Sons: New Jersey. ISBN 978-1119050056.

Rosing M., Scheer A., & Scheel H. 2015. The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM, Volume I. Morgan Kaufmann Publishers: Burlington. ISBN 978-0127999593.

Salovaara A. 2015. Developing Service Design & Management Processes Towards ITIL Compliance. Helsinki: Metropolia. Degree thesis. Accessed 22 June 2019. Retrieved from https://www.theseus.fi/bitstream/handle/10024/92863/Salovaara-Antti_Masters-Thesis.pdf?sequence=1.

Senft S. & Frederic G. 2009. Information Technology Control and Audit. Auerbach Publications: Washington. ISBN 978-1420065503.

Spivey D. 2014. Home Automation for Dummies. John Wiley & Sons: New Jersey. ISBN 978-1118949269.

Ouellette & Associates Consulting. 2009. Leading IT Transformation: The Roadmap for Success. Kendall Hunt Publishing Company: Dubuque. ISBN 978-0757558337.

Wilson C. 2014. Interview Techniques for UX Practitioners: A User-Centered Design Method. Morgan Kaufmann Publishers: Burlington. ISBN 978-0124103931.

Stiehl V. 2014. Process-Driven Applications with BPMN. Springer: Kista. ISBN 978-3319072173.

Appendices

Appendix 1. Categorized tasks and statistics

TASK CATEGORIZATIONS				
Urban Planning Customer Service Person	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Read confidential building information within the city's real e	Process	Main	Operational	Simple
Process permits within the city's real estate software	Process	Main	Operational	Generic
Modify locational information within the city's real estate sof	Steps	Main	Operational	Simple
Read scanned building permits	Steps	Supporting	Operational	Simple
Confirm payments on a 3rd party's website	Steps	Supporting	Operational	Simple
IT Account Administrator	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Use network printers	Steps	Supporting	Operational	Simple
Read intranet news, documentation, and phonebook	Steps	Supporting	Operational	Simple
Read sharepoint manuals and documentation	Steps	Supporting	Operational	Simple
Accessing network shares for access changes	Steps	Main	Operational	Generic
Maintaining AD user groups	Process	Main	Operational	Generic
Creating and maintaining email accounts	Process	Main	Operational	Simple
Creating and maintaining ERP accounts	Process	Main	Operational	Simple
Creating and maintaining email distribution lists	Process	Main	Operational	Simple
Creating and maintaining shared calendars	Process	Main	Operational	Simple
Network Share Administrator	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Grant access to network shares	Steps	Main	Operational	Generic
Grant access to Sharepoint rooms	Steps	Main	Operational	Generic
Grant access to an IMS login screen	Steps	Main	Operational	Simple
Population Registry User in Fire and Rescue	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Grant access to a person's information in a national populati	Process	Main	Operational	Generic
Grant access to real estate information in a national system	Process	Main	Operational	Generic

ICT Purchase Agent	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Answer phone inquiries and provide purchase consultation	Process	Supporting	Operational	Generic
Read for new purchase orders in helpdesk system and update	Process	Main	Operational	Simple
Lodge a purchase and its details to supplier system	Process	Main	Operational	Generic
Read an asset registry for naming new computers	Steps	Supporting	Operational	Simple
Register computers under employee names in an asset regist	Steps	Management	Operational	Simple
Remove disposable computers from an asset registry	Steps	Management	Operational	Simple
Read supplier notifications in personal email	Steps	Supporting	Operational	Simple
Approve delivery lodgers over email	Steps	Management	Operational	Simple
Read accounting details in a document archive	Steps	Supporting	Operational	Simple
Approve and register computer details to a supplier leasing s	Process	Main	Operational	Generic
Read and approve new invoices in a purchasing system for nc	Process	Management	Operational	Simple

Antivirus Administrator	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Create a remote desktop connection to AV software server fc	Steps	Supporting	Operational	Simple
Create remote desktop connections to client computers for s	Steps	Supporting	Operational	Simple
Maintain and update the AV database	Process	Main	Operational	Simple
Sanitatize compromised clients	Process	Main	Operational	Complex
Upgrade AV software versions and deployments	Process	Main	Operational	Generic
Maintain and change client firewall settings	Process	Main	Operational	Simple
Maintain and change AV settings	Process	Main	Operational	Simple
Azure Global Administrator	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Distribute and update mobile phone configurations via Intun	Process	Main	Operational	Generic
Distribute and maintain mobile phone software via Intune	Process	Main	Operational	Generic
Maintain Azure AD Connect synchronizations	Process	Main	Operational	Complex
Create Azure Enterprise Applications for Azure AD authentica	Process	Main	Operational	Complex
Maintain and repair Azure Enterprise Applications for Azure A	Process	Main	Operational	Generic
Login to portal.azure.com as a global admin for changes	Steps	Supporting	Operational	Simple
Admit new members to global admin role	Process	Supporting	Operational	Simple
Cash Registry Super User	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Login as an admin to cash registry using a software specific a	Steps	Supporting	Operational	Simple
Create new accounts for approved users	Process	Main	Operational	Simple
Verify approvals before account creation	Steps	Supporting	Operational	Simple
Verify the presence of a domain account before creation	Steps	Supporting	Operational	Simple
IT Ticket Master	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Follow helpdesk's ticket lifespan and statistics	Process	Main	Operational	Simple
Assign owners to helpdesk tickets	Steps	Main	Operational	Simple
Assign and coordinate helpdesk shifts	Process	Management	Operational	Generic
Manage helpdesk employee resourcing, priorities, and time	Process	Management	Tactical	Generic
Access asset and ticketing software	Steps	Supporting	Operational	Simple
Develop asset and ticketing system	Process	Management	Tactical	Complex

Firewall Specialist	**Level**	**Type**	**Tier**	**Nature**
Access domain computers for work	Steps	Supporting	Operational	Simple
Access city email software for work	Steps	Supporting	Operational	Simple
Define and maintain firewall rules and configurations	Process	Main	Operational	Generic
Order changes from the firewall SaaS provider	Process	Supporting	Operational	Simple
Confirm changes by authenticating via SMS	Steps	Supporting	Operational	Simple
Login to firewall SaaS website as an admin	Steps	Supporting	Operational	Simple
Define VPN rules and configurations	Process	Main	Operational	Generic
Troubleshoot connection, port, and routing issues	Process	Main	Operational	Complex

Level		
Steps	46	58 %
Process	34	43 %
Type		
Supporting	40	50 %
Main	33	41 %
Manageme	7	9 %
Tier		
Operational	78	98 %
Tactical	2	3 %
Nature		
Simple	57	71 %
Generic	18	23 %
Complex	5	6 %
Total		
Tasks	80	

Appendix 2. Action checklist for employee profiling

Employee Profiling For Access Management

CHECKLIST v1.00

INSTRUCTIONS

Double-clicking **Done** will mark the task as complete. Macro must be enabled

Done	Category	Item
✓	Plan	EXAMPLE
	Plan	Defined how employee profiles can benefit my city
	Plan	Defined how they could be used technically and process-wise
	Plan	Defined how many employee profiles will be gathered for the sample
	Plan	Discovered any readily documented employee profiles
	Plan	Discovered a sufficient number of super users for the interviews
	Plan	Decided on the interview venue and approximate length
	Plan	Decided which statistics and attributes are to be collected
	Plan	Created a customized interview form (if not using the one provided)
	Plan	Decided on recording/transcribing the interviews or not
	Plan	Created a project charter, collecting together the information and decisions
	Plan	Presented the charter to leadership and acquired an authorization
	Do	Contacted the super users for interviews and invited them to the venue
	Do	Reserved the venue for agreed times
	Do	Send the calendar reservations
	Do	Pre-filled the question forms with the personal data of the participants
	Do	Carried out the interviews with the agreed number of participants
	Do	Cleaned up the filled interview forms
	Do	Send a copy of the individual interview forms to each participant's email
	Check	Made a backup copy of the original interview forms and other media
	Check	Created a master list of all the profiles and their statistics/attributes
	Check	Analyzed the importance of each profile
	Check	Arranged the master list by importance
	Check	Excluded profiles that can not or should not be automated
	Check	Marked other development observations gained from the interviews
	Check	SWOT analyzed the results from the perspective of a project
	Check	(Optional) Performed a return of investment analysis
	Check	Gathered together all the results to a presentation and a project proposal
	Act	Presented the project proposal to leadership and acquired a project group
	Act	(Optional) Drafted the first service design package
	Act	Hand-off to the project group

Appendix 3. Revised question form for interviewing employees

EMPLOYEE PROFILING

INTERVIEW

BRIEFING

Thank you for participating to this interview. The purpose of the interview is to identify what kind of access rights you require in your job as a _____, or grant to others as the super user of _____, in an attempt to automate the admission and removal of these access rights.

These interviews have been authorized by _____ and the duration of the interview is roughly 45 minutes. During the interview phones, tablets, and computers should be turned off. The answers are public and may be inspected by your foreman, peers, and various project members.

The interview is finished when the question form has been signed as true and correct by your current, best knowledge. After the interview, a copy of the question form will be delivered to your email address.

1. PERSONAL DATA

Date		Place	
Interviewer		Department	
Participant		Email	
Age group		Years in service	
Other notes			

2. YOUR ACCESS RIGHTS

☐ You were chosen because you have an active role in either requesting or granting access to a system. Which system or systems do you grant or request access to? What would be a suitable title for this role? For example:

SAP BI Login Administrator / SAP BI Viewer				

☐ Which tasks in this role require access rights, are closely related to handling them, or are required to necessary for the role? Briefly describe them. Access to a personal email and domain computer is not necessary for this listing. For example:

SAP BI Login Administrator / SAP BI Viewer				
I grant access to SAP BI Login / I request access to SAP BI Login				
I grant transaction rights to BI / I use BI to view information				
I process emailed access requests / I email access requests to admin				
I answer to phone inquiries / I phone the admin for access advice				

☐ How often (FRQ) are these tasks carried on a scale of 1-3? 1 is rarely, 2 is occasionally, and 3 is regularly. For example:

SAP BI Login Administrator / SAP BI Viewer	FRQ			
I grant access to SAP BI Login / I request access to SAP BI Login	3			
I grant transaction rights to BI / I use BI to view information	3			
I process emailed access requests / I email access requests to admin	3			
I answer to phone inquiries / I phone the admin for access advice	2			

☐ How important (PRI) are these tasks to your role on a scale of 1-3? 1 is beneficial, 2 is important, and 3 is critical without which the work immediately halts. For example:

SAP BI Login Administrator / SAP BI Viewer	FRQ	PRI		
I grant access to SAP BI Login / I request access to SAP BI Login	3	3		
I grant transaction rights to BI / I use BI to view information	3	3		
I process emailed access requests / I email access requests to admin	3	2		
I answer to phone inquiries / I phone the admin for access advice	2	1		

☐ How many members does this role have? For example:

SAP BI Login Administrator / SAP BI Viewer	FRQ	PRI		
I grant access to SAP BI Login / I request access to SAP BI Login	3	3		
I grant transaction rights to BI / I use BI to view information	3	3		
I process emailed access requests / I email access requests to admin	3	2		
I answer to phone inquiries / I phone the admin for access advice	2	1		
Members 5				

☐ How much time (TIME) does each task usually take per day? Express in hours, in average. For example:

SAP BI Login Administrator / SAP BI Viewer	FRQ	PRI	TIME	
I grant access to SAP BI Login / I request access to SAP BI Login	3	3	2	
I grant transaction rights to BI / I use BI to view information	3	3	0,5	
I process emailed access requests / I email access requests to admin	3	2	0,5	
I answer to phone inquiries / I phone the admin for access advice	2	1	0,25	
Members 5				

3. SIGNING

We hereby declare this information sufficient and true by our current knowledge. We approve the use and publication of the data within the city's organization.

☐ Interviewer's signature: ___

☐ Participant's signature: ___

Appendix 4. A simple access management framework for automation software, containing only the main points