Tampere University of Applied Sciences

Single sign-on in a growing start-up

Lars Derek Sundell

BACHELOR’S THESIS
March 2021

Bachelor of Business Administration
Degree Programme in International Business

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Bachelor of Business Administration
Degree Programme in International Business

SUNDELL, LARS DEREK:
Single sign-on in a growing start-up

Bachelor's thesis 32 pages, appendices 11 pages
March 2021

This thesis was written to reflect and report on a project to select and implement a single sign-on identity provider at Castor EDC. Castor was in an intense growth phase from under 50 employees to more than 100 the stringent and work intensive access control procedures were proving to be non-sustainable with such a large workforce. Thus, a single sign on service was deemed necessary to improve the scalability of the business. Single sign-on, on a longer timeline, would serve as the replacement to more manual access control procedures currently in place at Castor. The research problem was to determine what advantages the streamlining of access control, and access to services would have on employee satisfaction and effectiveness. Data was gathered via questionnaires of which there were three, two sent to employees before and after implementation measuring satisfaction, as well as one sent to service owners and administrators to gauge satisfaction with the current access control procedures. Additionally, comparisons were made to the standards to which Castor complies.

Once the project was underway and the single sign-on provider was implemented to some of the more widely used tools, advantages started to become apparent to the author. Onboarding to most general tools was streamlined and at the time of writing this thesis, the provider was being integrated with more department specific, yet critical, services. Data gathered from questionnaires revealed mostly lukewarm attitudes toward the password manager previously used with mostly positive first impressions of the new single sign-on provider. According to service owners and administrators, the access control procedure at Castor is error-prone and tedious. This procedure can be streamlined, as a result of SSO implementation. Recommendations to the client include, but are not limited to, adding single sign-on support as a requirement to Castor’s supplier purchasing procedure, rewriting access control procedures to allow for the single sign-on solution to replace old procedures where applicable, and in existing services disabling form-based authentication in favour of single sign-on.

Key words: sso, information security, iso 27001

CONTENTS

GLOSSARY

2FA = Two-factor authentication

API = Application Programming Interface

EDC = Electronic Data Capture

FDA = United States Food and Drug Administration

Form-based Authentication = Username and password authentication

GDPR = General Data Protection Regulation

IAM = Identity and Access Management

IdP = Identity Provider

ISO = International organisation for standardisation

IT = Information Technology

JIT = Just in Time provisioning

LAN = Local Area Network

Mapping = Automation in OneLogin

MFA = Multi-factor Authentication

NEN = Stichting Koninklijk Nederlands Normalisatie Instituut

OIDC = OpenID Connect

PII = Personally Identifiable Information

RESTful API = API using Representational state transfer (REST) architecture

Roles = Determine which services one has access to in OneLogin

SaaS = Software as a Service

SAML 2.0 = Security Assertion Mark-up Language

SMS = Study Management System

SOP = Standard Operating Procedure

SSO = Single Sign-On

1 INTRODUCTION

This thesis inspects the implementation of an SSO solution to a start-up organisation and the effects this has on employee satisfaction, and in turn the effect of higher employee satisfaction and efficiency on customer service and product quality. The effects SSO has on compliance to ISO standards is explored, comparing, and contrasting to requirements from the standards in question. Additionally, aspects investigated are the streamlining of onboarding and offboarding by automation of provisioning. The research questions of the thesis are:

- What are the main benefits of a centralised Single Sign-on service
- How does implementing SSO affect onboarding/offboarding processes
- How does implementing SSO affect employee satisfaction in login flow
- How does implementing SSO improve ISO 27001 compliance
- How does implementing SSO support serving paying customers
    - What benefits do clients see from a more smoothly operating business

Compliance to standards regarding information security and quality control are critical to a company such as Castor, as any system handling medical data is scrutinized for HIPAA, GCP, ISO 27001 and/or SOC 2 Type II compliance to ensure patient data is handled in a manner of ultimate privacy and security. Castor caters exclusively to customers looking for assurances given by these kinds of certifications. These clients may even conduct their own audits of Castor’s procedures and systems to verify high enough compliance.

Another intention for this thesis is to act as a report, with recommendations on what should follow, to the management team, council, and board of Castor EDC. It will attempt to demonstrate the practical benefits of SSO implementation at this stage, with estimation of further benefits down the line as the project proceeds beyond the scope of this report. Whether or not this project was worth the cost will be determined by management at Castor, exact costs of the project may not be disclosed, as they are confidential contract details.

The company, Castor, with inspection of its position in the market and explanation of client expectations of a business in the clinical software space, is introduced. Included is a list of all standards Castor is either compliant with, or certified in. Castor is a start-up, so its business model is focused on getting market share, even at the cost of profitability. As such, Castor got a large Series A funding round of 12 million, the latest funding of which was received in August 2020 (Castor 2020).

Theory on single sign-on and SAML is provided in the third chapter, serving as a brief lesson on the terminology and underlying technology for the reader. While SSO is a technology that is becoming increasingly common in recent years, it is not a new idea, having been in use since the 2000's. LDAP, a predecessor to SSO, was designed for on-premises networks over LAN while SSO was designed to address the challenges of authentication to web-based applications (Lujan 2019). LDAP was in wide use, and still is to some extent. As such, LDAP will not be addressed within the scope of this thesis. SAML 2.0 is a newer SSO standard allowing for just-in-time provisioning of users and real-time access control. SAML will be a focus of the theory portion.

The project came from the need to automate and streamline the access control procedure. This procedure, which has been in use at Castor since it was a dozen employees, is no longer scalable as Castor is about to exceed 100 employees. Before the author started on the project, an SSO was determined to be the resolution to this particular issue. Therefore, implementation of an SSO was made into a QISMS goal. QISMS goals are milestones for tracking the improvements made to compliance of the ISO 27001 and ISO 9001 standards. After comparing several service providers, as required by the supplier purchase procedure, OneLogin was chosen. The selection process is explained in some detail in the fourth chapter.

Data collection methods are discussed, main methods being study of the relevant ISO standard and Castor policies, and questionnaires sent to employees at Castor. The sample size being small, the data is qualitative regardless, and conclusions are based heavily on day-to-day observations from the author. The author is the SSO project runner and IT-support at Castor, so these observations and analysis based on them qualify as expert opinion. Analysis will look at the employee satisfaction in LastPass, administrator experiences with access control procedures, and employee impressions based on the first month of using OneLogin.

Finally, the conclusions include a recap of the results, recommendations to Castor, thoughts on the future of the ongoing SSO implementation project, and a list of all apps successfully integrated during the scope of this thesis. Some speculation about the effects of the project to ISO compliance is given. Exact measurement of these effects is not possible in the scope of this thesis as the next internal audit at Castor is near the end of quarter two of 2021 and the next official external audit is scheduled for October 2021.

2 CLIENT PROFILE

Castor is a SaaS start-up established in 2012 and operating as two legal entities Ciwit B.V. and Castor Research Inc. from Amsterdam, The Netherlands and Hoboken, New Jersey, USA, respectively. Castor is currently at over 100 people strong, including contractors. Castor makes several different cloud-based software products (Figure 1). These products are used by both public and private sectors to conduct various kinds of medical studies. Professional services, such as study building, are offered by Castor. Being post Series-A funding, Castor is in an intense growth phase, growing from less than 50 employees. (Castor 2020.)

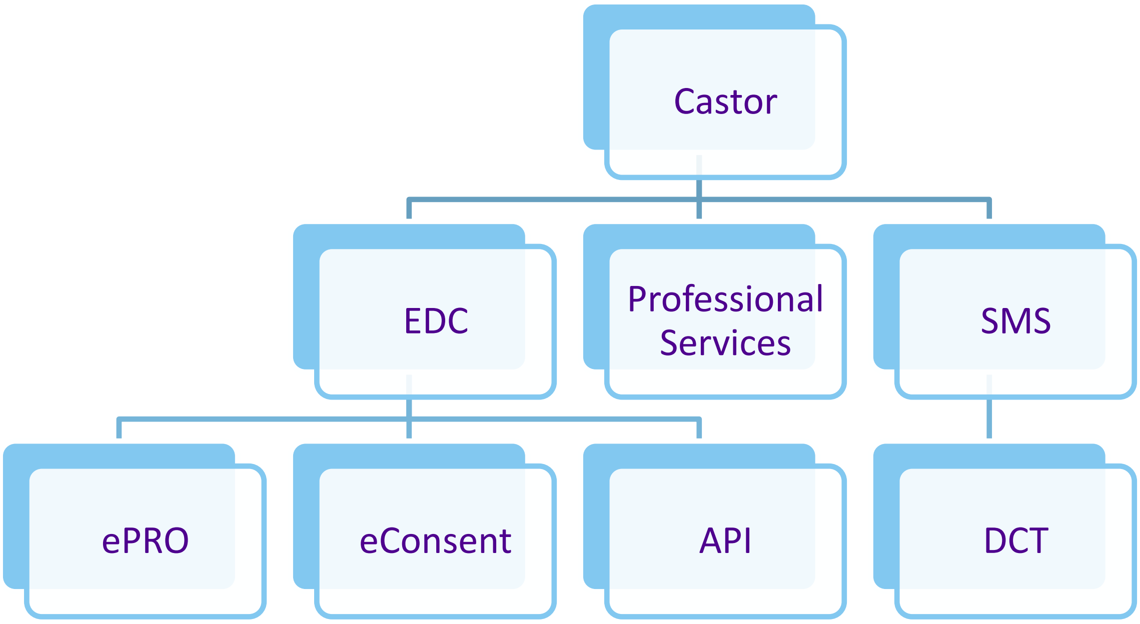


FIGURE 1. Castor product offering

Castor has a wide gamut of products, some mature and released, some in a pre-release status being developed. The original main product, Castor EDC, is a study platform. EDC means Electronic Data Capture, essentially having a cloud-based web service replacing paper forms and spreadsheets for collecting the information from conducting medical studies. A focus product being launched in 2021 is Castor eConsent, due to the COVID pandemic causing a rush to create studies that are conducted partially or completely remotely. eConsent allows for remotely and securely collecting consent information from existing and new patients and test subjects for studies and other research. Castor SMS, which is in a pre-production stage in use by some select clients, stands for Study

Management System and is used to control several studies within an organisation. DCT, referring to decentralized trials, is a key additional functionality being built to Castor's existing platforms. As Castor products are cloud and web based, they already support DCT better than some competitors, but more DCT specific functionality is required. ePRO is an existing part of EDC, abbreviated from electronic patient reported outcome. PROs refer to the forms used to collect data during studies. The API mentioned in Figure 1 is a module built into EDC which uses third party API standards to connect Castor EDC with dashboards, other research software and any software with RESTful API support. An API refers to an Application Programming Interface, or in laymen's terms, software that allows communication between applications.

Notable clients of Castor include The World Health Organisation, who use Castor's EDC platform and professional services for the COVID-19 Solidarity trial; The American Board of Medical Specialties, who use ePRO to capture physician feedback; and Amsterdam UMC, a long-time user of Castor EDC. Castor EDC was originally offered to academic clientele for low licensing costs, as a tactic to gain industry experience and user experiences and help build the product. In 2018 and 2019 focus was beginning to shift to commercial clients and larger revenues, contributing to the growth being experienced now. The WHO study, to which Castor is offering their platform free of charge, caused an uptick in publicity for Castor, in addition to the funding received by Castor in the summer of 2020. Castor is making a push into the US market, hiring several salespeople and support personnel for the US entity Castor Research Inc. The US has a relatively large and mature market for the types of products Castor offers.

As a company creating software for medical professionals and handling patient data information security and quality control are extremely high priority both internally and for clients both existing and potential (Castor, 2020). Castor has several international certifications for quality management and information security; therefore, the company has dedicated personnel for managing the compliance to the policies that enable Castor to achieve these standards. The author is one of these persons, working on information security at Castor under the title systems administrator and compliance assistant. Certifications describe requirements for the systems in question, but do not give instructions how to fulfil these requirements. Clients often require any service they purchase to have one or more of these certifications. Castor is compliant with (appendix 1):

- ISO/IEC 27001:13
    - Information security systems certification
- ISO 9001
    - Quality management systems certification
- NEN 7510
    - Dutch analogue of ISO/IEC 27001 required by many local institutions
- FDA 21 CFR Part 11
    - US Food and Drug Administration standard for electronic records and signatures

Part of the ISO/IEC 27001 compliance is Castor's access control policy which describes how tool access is managed. Currently these processes are manual, relying on tool owners modifying a spreadsheet to track account creation and deletion to each tool used by Castor. As such, the spreadsheet not being up to date in real time is a serious concern and requires remedying as Castor continues to grow. (Castor 2020, 9.)

3 ACCESS CONTROL

Access control is the umbrella term for all operations regarding the access of users to tools. Access control procedure is important to any organisation larger than a handful of persons, or any organisation with access to sensitive data such as PII, financial metrics, software code or other similar volatile information. Several standards, such as ISO 27001, require robust access control measures where account creation, modification and deletion is documented.

As ISO, and other, standards only indicate requirements and not methods how to achieve these requirements this theory portion will discuss methods relevant to this thesis, including but not limited to form-based authentication, single sign-on, and SAML. While Castor QISMS policy is not specifically spoken of in this section, it is used as examples of effective policy based on ISO requirements.

3.1 Authentication and SSO

Authentication in information technology has traditionally been form-based, using a username and password. It is a simple method that works, but it is lacking some convenience and security factors that more modern methods can offer. Unlike in the past, the password is not stored in a service but a hash is, this is based on some mathematical problems being easy to solve one way but nigh impossible the other. The service stores a hash that has gone through a password encryption hashing processor, when a user is logging in their password is entered through the same hasher to match the hash to the one stored in the service. If the hash does not match the password is determined to be incorrect. (Arias 2019.)

Switching from form-based authentication to SSO brings benefits and some risks. Potentially making it easier for intruders to gain access to several systems is a major risk, as an intruder would only need to gain access to one set of credentials instead of several. A minor risk is having an intruder access systems by gaining access to the computer of an employee and using existing authentication tokens to access said systems. The benefits outweigh these potential risks significantly. By enforcing measures such as MFA preventing a compromised password from allowing access to systems, appropriate endpoint security mitigating remote access attacks on employee laptops and having policies and monitoring in place to ensure an unattended employee laptop is locked these risks are managed and minimised (Castor 2020, 9). The benefits of SSO, especially if a real-time connection to a directory is established, include but are not limited to real-time access management revoking access mid-session as an employee is deactivated in the “source of truth” directory, ensuring every service is behind MFA, and making authentication more convenient as the user only has to remember one set of credentials. (Knafo 2018.)

Authentication using SSO requires an IdP or identity provider, such as OneLogin or Google Auth. The IdP is responsible for authenticating the user by means of username, password and multifactor authentication using biometrics, mobile phone apps, smart cards, or physical identity keys (specialized USB thumb drives). The login flow can either be prompted by the web application when a user tries to login, or by the IdP from a login portal. In either case, the web application will communicate with the IdP to determine whether the user in question is authorised to access the web application. If a user is authorised, the IdP will respond to the web application, confirming the veracity of the user. There are several interfaces through which the application and IdP can communicate, the most commonly used being SAML 2.0 and OIDC. (Figure 2.; Peyrott 2015.)

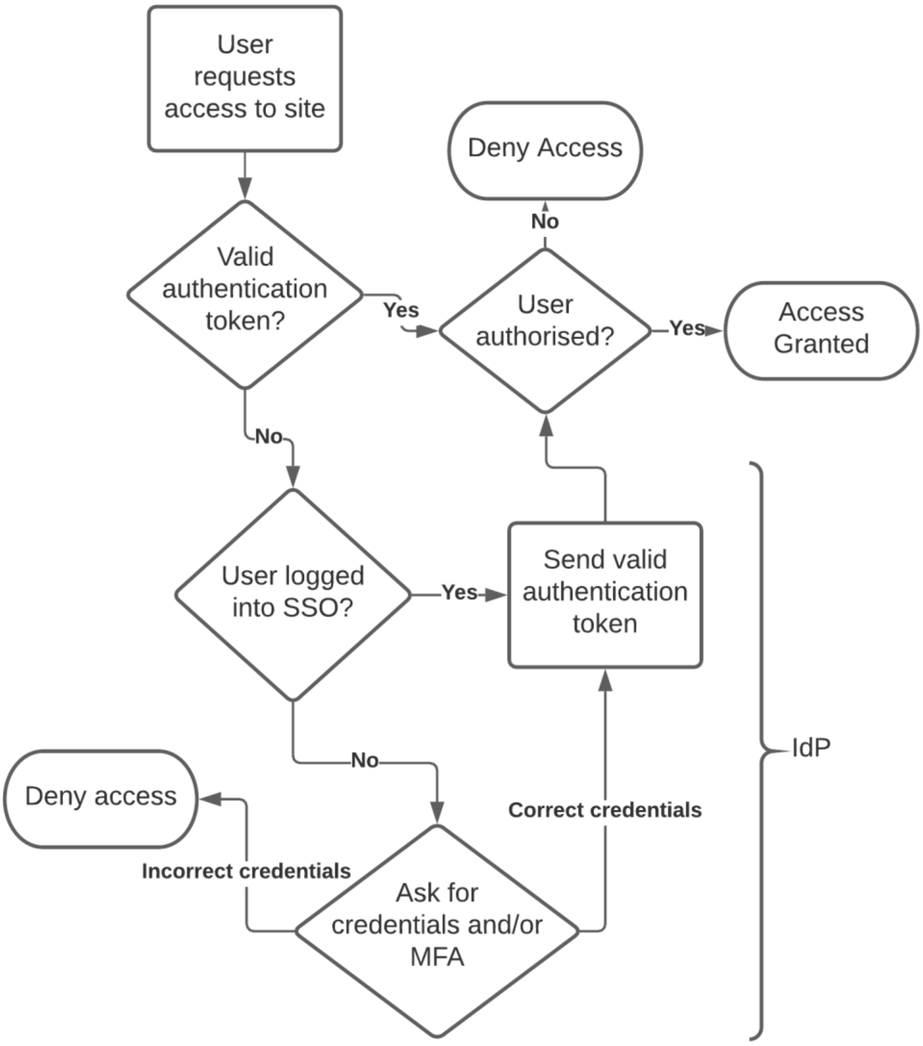


FIGURE 2. Web application login flow using SSO

Most commonly, the IdP is using an active directory as the user database, either with an API connection with no “local” database in the IdP or by pulling and updating data from one or several directories into its own database. It is important to have a main “source of truth” determined in documentation and planning, otherwise the IdP might have trouble determining if a given user is supposed to be active, inactive, or deleted. Source of truth is the technical term for any directory or data source that is considered above all other data streams.

3.1.1 SAML 2.0

Security Assertion Markup Language 2.0 is a communication standard used to authorise and authenticate users. It was launched in 2003 by OASIS, with the standard remaining mostly unchanged since 2005. SAML enables authorisation and provisioning. Provisioning can be done with either proactive provisioning where accounts are created as a user is added to the IdP directory or just-in-time provisioning. As a markup language, SAML offers several different additional possibilities and permutations of authentication flows, but that is outside the scope of this thesis. (OASIS Open 2008.)

3.1.2 OAuth 2.0 and OpenID Connect (OIDC)

OAuth 2.0 is a protocol for authorization developed by the IETF OAuth Working Group. OpenID Connect 1.0 is an identity layer on top of OAuth, which allows for similar operation as SAML 2.0, operating as an interface between the web service a user is trying to log into and an IdP (OpenID Foundation n.d.). OIDC is not as common as SAML, but is gaining traction due to its simpler implementation. It can also be used for JIT provisioning. As can be seen from Figure 3 the operation, from an SSO perspective remains the operation of OIDC is the same as other methods such as SAML.

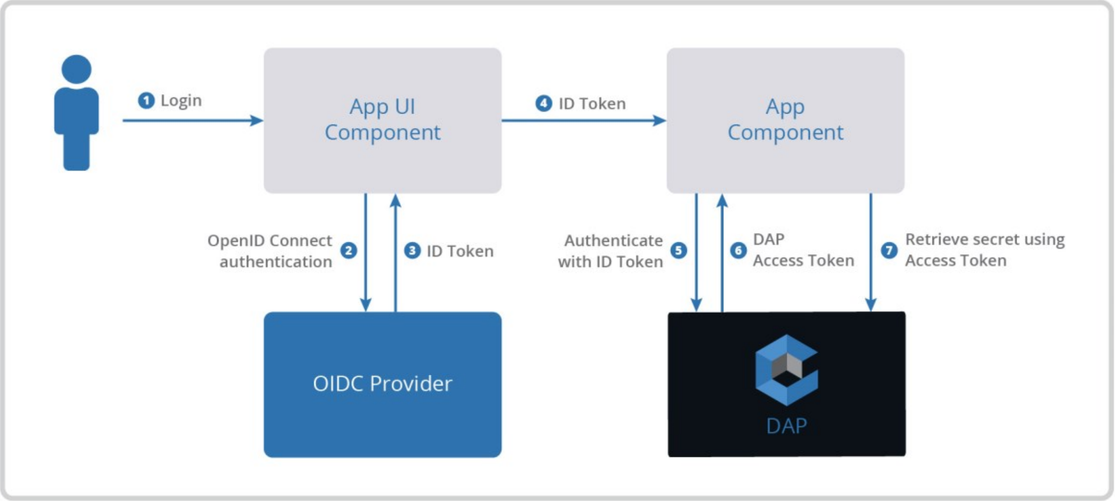

1 Login
App UI Component
4 ID Token
App Component
OpenID Connect authentication 2
3 ID Token
Authenticate with ID Token 5
6 DAP Access Token
7 Retrieve secret using Access Token
OIDC Provider
DAP

FIGURE 3. SSO operation using OpenID Connect (CyberArk Software Ltd. N.d.)

3.2 Account management and provisioning

Account management, also known as IAM, is a work intensive process tightly entwined in access control management. Provisioning is the process that enables automating the task of account management. Most commonly provisioning is done using SAML, a mark-up language used to communicate between directories containing user details and applications that are being used, often via a third party identity provider. With provisioning set up and supported by applications used by an organisation an administrator can make changes to users and groups in a single directory and affect their privileges in, and access to, applications across the catalogue of applications in use by the organisation. Without provisioning, access control is a fully manual process usually involving a spreadsheet where every user and their access must be tracked. (Lutkevich 2020.)

3.2.1 ISO requirements

ISO 27001:13, regarding information security, requires access to systems and applications to be restricted and controlled. Strong authentication is required, usually fulfilled by second factors of authentication such as OTP (one time password), biometrics or smart cards. Regardless of the strength of authentication, if access is given incorrectly, or not removed when appropriate, information security will be compromised in that scenario. Robust policies are needed to ensure access is given, modified and revoked in a controlled manner. Automation can be a tool to achieve this end, but it needs oversight and regular reviews. (NEN-ISO/IEC 2015.)

4 PROJECT AND TIMELINE

To support compliance with the access control policy a project was devised to augment and partially replace the very manual procedure described in the policy with more automated processes. A single sign-on (SSO) service was determined as the way to achieve this goal. Following the written supplier purchase procedure, the author compared different SSO service providers and chose a service called OneLogin for the project. The features offered by this solution allow for provisioning, the automated creation of accounts and assigning privileges to new and existing users; as well as sending automated notifications to tool administrators for tools that do not support provisioning. OneLogin was chosen for its SSO feature set and reasonable pricing structure. (OneLogin N.d.)

The author was tasked with implementing an SSO service to Castor's IT infrastructure, to partially automate account creation, privilege adjustment and revoking access. OneLogin was chosen in accordance with Castor's supplier purchasing procedure, being compared to other options before being selected. The implementation is intended to automate access control and the processes therein, provisioning or account creation and privilege escalation and de-escalation as well as onboarding.

4.1 Project background

The project is spurred on by a growth phase in Castor's development from an HR perspective. After a large round of investment funding received in July 2020 the HR department, called the People Team, has been hiring new employees at an unprecedented rate in Castor history. With hiring large numbers of people comes significant strain on the infrastructure for both onboarding and access control management, as these processes have been largely manual up until now. In addition to the SSO project to automate and streamline access control there are projects at Castor aiming at automating other aspects of onboarding, such as new hire training and acclimatisation to Castor products and conventions. These are being achieved with the implementation of an eLearning platform.

4.1.1 Acute problems

At Castor access control has been done manually with a spreadsheet, see a simplified example of the format of this spreadsheet in Table 1. As Castor's access control procedure requires, whenever a person is given access to a tool, they are given an X in a sheet named "Access Control for Tools". The individual responsible for adding this X is the asset administrator. This individual is also responsible for removing persons' access to the tools they are administrators of and marking this in the sheet. These procedures are performed whenever a person is added to the organisation, transfer within the organisation, and removed from the organisation. Additionally, asset owners, who are required to be managers, perform a semi-annual or quarterly check of the people with access to a tool according to the spreadsheet. The frequency of these checks is determined by the classification of the application, the more sensitive information stored in said tool, the higher the classification (Castor 2020, 3).

TABLE 1. Access Control for Tools sheet format demonstration

Tool	*Check required*	*Classification*	*Asset owner*	*Asset administrator*	*Last check date*	*User A*	*User B*
Google	Yes	Key services	Manager	Employee	October 2020	X	x
Server access	Yes	Processes medical data	Manager	Manager	January 2021		x
Zoom	No	Nonessential services	Manager	Employee	July 2020		x

The access control procedure in place has a high probability of human error, being a fully manual process, with significant time spent each quarter on double checking critical tools. As the number of personnel increases the time spent and opportunity for errors compound unsustainably, automation is needed for creating accounts, removing them, and reviewing who has been granted access. No serious incidents have been reported, but the potential for more serious incidents exists as long as processes remain manual. Some mistakes are being made already (Appendix 2). With automated provisioning in use the only manual process remaining will be for tool owners to check user lists of applications to ensure no unauthorized access, this still differs from the fully manual process in that if any unauthorized access is detected the automation can be adjusted to avoid similar occurrences in the future. The whole process changes from reactive to proactive.

4.2 The solution

Automation of these processes leads to customer benefit in a direct way. With onboarding procedures of both HR and IT departments streamlined, with SSO and an eLearning platform, new employees are onboarded at much greater speed and efficiency and thus can get to work quicker. Giving access to contributors such as third-party support contractors is also faster and more secure, with more strict controls in place that do not require as much manual setup. In an indirect effect on customer benefit it improves on the daily efficiency of employees. With less time spent on authentication an employee saves time and has fewer opportunities to get distracted whilst ‘on the way’ to a tool or service.

An automated SSO aids in compliance with the standards Castor adheres to. These standards and the certifications therein are critical to Castor clients due to Castor’s platforms handling the clients’ patient data. As the number of personnel increases the processes foundational to compliance such as access control are under increased strain. In this direct manner an SSO improves on compliance to the access control policies of Castor, by lowering the need for manual labour and decreasing the factor of human error.

Castor has used, and still uses, a password manager, LastPass, to store and share passwords and other confidential data such as SSH keys and WiFi passwords. This password manager has regular issues related to its function and employee satisfaction suffers as a result (Figure 4). With proper implementation and employee education, OneLogin is planned to be a complete replacement for LastPass. Beyond sharing of passwords, sharing of other confidential data via secure notes is an important feature.

4.3 Timeline

When the author arrived at Castor in October 2019 the SSO project became a topic of discussion and began development almost immediately. It has been underway since. The SSO solution was chosen and purchased following Castor's supplier purchasing procedure. As per the procedure, a need had been established before the author began work on the project. The author proceeded with the procedure, assessing alternatives such as Google Auth, Okta, and others, with a final choice of OneLogin. Council approval was received, and the author continued to follow the procedure. The SSO solution being deemed a critical service, due to having a significant potential effect on availability, security and critical supplier checklists were filled out and certifications asked from OneLogin to ensure OneLogin has sufficient security and quality to be a tool Castor can use without endangering its own ISO, and other, certifications. Legal diligence was provided by Castor's legal department, for example determining the need for a DPA, or data protection addendum, due to OneLogin's service handling Castor employees' personally identifiable information. (Castor N.d.)

Once OneLogin passed these checks and diligence the contract was signed, and it was purchased in June 2020. In July 2020, the author attended a two-day training on SSO implementation as provided by OneLogin. The implementation project was prepared, and stalled for some time, over the autumn of 2020. In November 2020 with the integration of Zoom and some other minor services to OneLogin the implementation kicked off. A major milestone was reached on Christmas of 2020 when the author integrated Google and Atlassian to the service (Figure 6). Google Workspaces services are used by Castor for authentication to several services, email, collaborative documents, file storage and sharing, and more. Additionally, this means any service using Google Auth is also using OneLogin instead, with Google Auth as a proxy. Atlassian covers Confluence and Jira, internal information sharing and project management platforms respectively.

To enable automation of account creation with provisioning and revoking access immediately, BambooHR and Google are used as the directories for OneLogin. OneLogin pulls from these services to create its user database against which authorisation is checked as part of IdP operations. BambooHR is used as the main “source of truth” as it is where long-term contractors and employees are entered, and their status kept accurate in real-time by the HR team at Castor. What this also means, in effect, is that HR can create users in Google (email, calendar, etc.) without needing interference from IT-support. This in turn helps HR be more self-sufficient in preparing onboarding for new employees as there is one “middle-man” fewer.

4.3.1 Communication and issues

Communication of these changes has been critical to minimize the negative impact on Castor employees’ work. As part of this the author began the practice of sending a weekly email newsletter with info on the OneLogin implementation project progress as well as other IT related news and announcements. The challenges addressed with increasing communication were employees not creating their OneLogin accounts when prompted, unawareness of the project and its goals, and the risk of someone being locked out of their accounts when working. Thanks to this increased communication the integration of Google caused fewer problems than anticipated by the author upon employees returning to work after the winter holidays.

A goal of the project is for OneLogin to effectively replace LastPass. OneLogin’s password management features are not as robust as LastPass but with the proper implementation of SAML and other SSO features this should not be a serious hindrance. As part of this, getting all departments that are heavily dependent on LastPass features, such as engineering, migrated onto OneLogin with minimal disruption to workflows is a significant challenge and the main challenge of the first quarter of 2021. In February 2021 Castor’s LastPass subscription was extended by a year, due to the impractical time constraints of offboarding all employees to OneLogin at such short notice. As planned by the author and the COO of Castor, LastPass will be phased out of use in Autumn 2021 (Konterman 2021).

4.3.2 SAML, provisioning and form-based authentication

There are several ways to integrate a service to an SSO. In order of most desirable to least desirable: SAML with provisioning, SAML with JIT provisioning, SAML login only, and form-based authentication. SAML with provisioning involves creation of accounts in services in advance, this enables having automation to grant and revoke privileges within the service in question. SAML with JIT provisioning will grant basic access to any employee that has been mapped to have the application within OneLogin, further privileges must be granted or revoked manually by an administrator. SAML without provisioning requires account creation by administrators, but no password need be set or configured. Even without provisioning, SAML will enable revoking access automatically.

There are several applications that do not support SAML and thus cannot be fully or partially automated. These applications use form-based authentication or, in laymen’s terms, username and password. For form-based applications OneLogin supports sending automated tasks to application admins to create or adjust accounts. This introduces some room for human error, but significantly less than having every part of the process be manual, as it was before OneLogin.

An anomaly, though a common anomaly, are services that use Google for authentication such as Slack, Asana and BambooHR. As Google access itself is determined by SAML and OneLogin, these services, by executive decision, may continue to be authenticated by Google without detriment to security or access control. Most of these services support JIT provisioning, thus automating granting basic access as described.

5 DATA GATHERING AND ANALYSIS

This chapter will describe first the data collection methodology, then expected results and finally the results as based on gathered data. The purpose of the data collected is to attempt to qualify the impact of SSO implementation on a business, more specifically a growing SaaS start-up. Most, if not all, of the tools used by Castor are cloud based, so an SSO utilizing SAML has the potential to have a significant effect on daily operations of most employees. Potential effects and practical applicability of SSO on ISO requirements are aspects considered in the following chapters as well.

5.1 Methodology

Two types of data will be used. ISO and GCP standards and the Castor policies derived thereof, as well as questionnaires conducted on employees of Castor. The ISO and GCP standards were explored in the theory portion of this thesis, here connections between those standards and the improvements SSO brings to policy adherence will be made. Castor's policies hold a higher position in practical terms, as they are the method to fulfilling any requirement set by the ISO.

With an employee count of about 100 any data gathered will be qualitative, even if response rates were 100 percent, which they were not. Some attempts to quantify data will be made, but no statistical significance can be derived from a sample this size. That said, subjective feelings and the qualitative data therein is an important indicator of employee efficiency, as employee happiness and contentment are critical modifiers to workplace efficiency in office jobs (Halkos 2008, 21.)

This data gathering methodology will not address some of the other effects and benefits of SSO, such as improvements to ISO compliance. These effects are difficult to quantify in the scope of this thesis as they would require an ISO audit to get comparative data to the previous audit. Also, the access control automation afforded by OneLogin is not yet all in place at the time of writing, and will mature over time, beyond the scope of this thesis.

Data was collected with questionnaires (Table 2), distributed with Google Forms, before and after the implementation of the SSO solution. Questionnaires before the project gauged opinions on LastPass and the access control procedure from both end users as well as service owners and administrators. The questionnaire after implementation was used to gauge satisfaction in OneLogin and subjective experiences on how well it was replacing LastPass after about 1,5 months of usage. The questionnaires were short in the intention that a short form would alleviate responder fatigue and ensure a higher answer percentage. All questionnaires were anonymous with plenty of fields available for custom answers.

TABLE 2. Questionnaire questions

Question	Answer type
Tool owner and administrator questionnaire (pre-implementation)	
(Roughly) how many tools do you own and/or admin in Access Control for Tools? *	Multiple choice radio buttons (number of tools)
How much time would you estimate you use to work in Access Control for Tools on a monthly basis? *	Multiple choice radio buttons (minutes) + other
How happy are you with the Access Control procedure in place? *	1-5 scale
How many times in the past quarter have you noticed someone having access when they shouldn't have? (Unauthorized access) *	Short text answer
Which of the following do you spend time on each month? (select all that apply) *	Multiple choice checkboxes (tasks) + Other
Do you have any other comments about the procedure as it currently stands?	Long text answer
End user questionnaire (pre-implementation)	
How happy are you with LastPass? *	1-7 scale
[Roughly] how often do you have to reset passwords to services due to misplacing them or LastPass not saving them properly? *	Multiple choice radio buttons (timespans) + other
In the past 3 months, how many times have you needed access to a tool but haven't had it and have thus had to wait for an admin to give you that access? How long was the wait?	Long text answer
End User Follow-up (post-implementation)	
Have you been able to stop using LastPass since OneLogin became available? *	Multiple choice radio buttons (yes, no, somewhat)
How happy have you been with OneLogin *	1-5 scale
Do you feel you were informed sufficiently on the OneLogin implementation? *	Multiple choice radio buttons (yes, no, other)
Any other comments? (Voluntary)	Long text answer

Considering what requirements are stated by ISO 27001:2013 it requires an access control policy is established and followed. “Access to information and application system functions shall be restricted in accordance with the access control policy.” and “Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.” as stated by the ISO requirements (NEN-ISO/IEC 2013, 13).

5.1.1 Expectations

LastPass has been a source of frustration for IT management and some users in the Castor organisation and the author expected this to be reflected in the questionnaire replies. Regarding OneLogin, there was an expectation that having the login flow of all services be via one portal would be preferable to end-users in the organisation. The access control procedure, being a manual process, was expected to be a point of tedium and exasperation among owners and administrators of tools. The questionnaire aimed at the aforementioned group was intended to gauge feelings and opinions on the efficiency and practicality of this procedure.

It was anticipated there would be mixed feelings about OneLogin. Castor employees are used to working with a password manager, and while OneLogin has some functionality to that end, but it is not a password manager. Countering this, SSO in a wider sense makes authentication to services much simpler so wherever SSO, either via OneLogin or Google Auth, is enabled users should experience no login screen mid-session or will only have to click one button to login to a service. Thus, the expectation was that satisfaction would be high, even with the confusion surrounding a new tool.

5.2 Results

The pre-implementation questionnaires/polls ran for approximately one month before the ramp-up of the project, before most tool owners and administrators, as well as end-users, had any experience of using OneLogin day-to-day. There was not time within the scope of the thesis to properly gauge effect on tool administrators and owners as to how effective the new onboarding automation was, but post-implementation impressions were gathered from end-users.

The questionnaires were distributed via the #general channel in Slack and the IT newsletter distributed by the author. Pre-implementation the questionnaires garnered answers from approximately 50 percent of the workforce at the time. The tool owner and administrator questionnaire received 12 responses, the pre-implementation end user questionnaire received 38 responses and the post-implementation questionnaire received 30 responses, which represents approximately 40 percent of the workforce at that time.

5.2.1 Analysis

With a sample size of 12 to 38 depending on the questionnaire, all conclusions derived from this data are qualitative. The author acts as the IT support and compliance assistant; thus they operate as the main support for all the applications and processes in question, including the access control procedure. As such, the qualitative analysis performed by the author will include, and be affected by, expert opinions.

The employee satisfaction of LastPass was higher than anticipated, with an average satisfaction of 4,52 on a scale of one through seven (one meaning extremely dissatisfied, seven meaning perfectly happy) and a median score of five. Lastpass' learning curve is potentially high for an inexperienced user, and Castor's requirements for MFA and master password complexity meant issues requiring the attention of IT support were common. In late 2020 these requests were less frequent, as LastPass had apparently addressed some common issues.

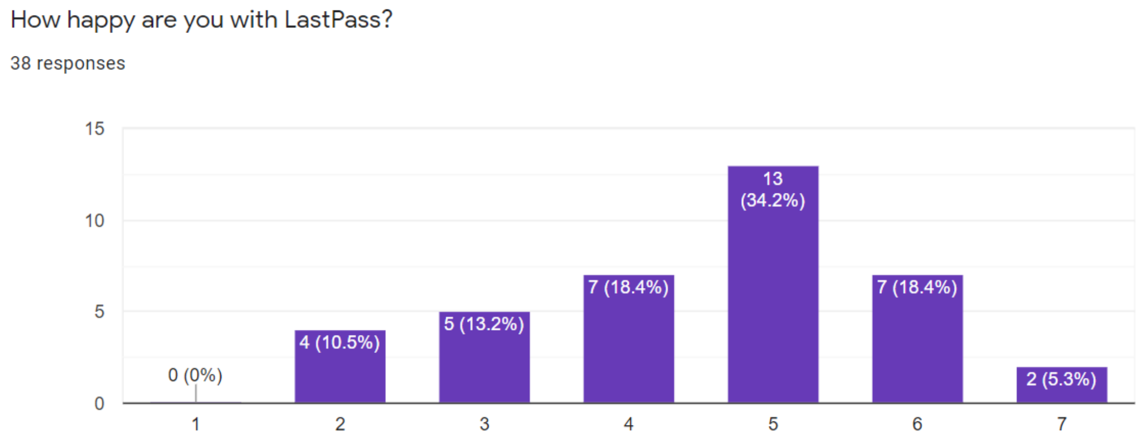


FIGURE 4. LastPass satisfaction distribution

To compare, the satisfaction to OneLogin was relatively high, considering it is a new service of which users do not have much experience (Figure 5). The second questionnaire was answered by 30 employees between the first and fourth of February 2020. If one considers the beginning of January as the first effective usage date in earnest, as this is when people returning from Christmas vacations were first forced to use OneLogin on a daily basis to access Google and Atlassian services, this means the questionnaire was answered based on approximately a month of active usage. The average satisfaction to OneLogin, on a scale of one (least happy) to five (most happy), was 3.47 with a median rating of three. This means most users seem to be onboard and generally positive about OneLogin and its usage. Some outliers on the lower side, three people rated their experience with a two, are probably likely due to early confusion about the role of LastPass and whether OneLogin is a replacement to LastPass. Some early issues with using OneLogin were also included in the free-form comments, with several stating more instruction is necessary. After these results, the author included instructions in their weekly newsletter to help with users migrate to OneLogin more seamlessly. Additionally, several users complained that OneLogin requires logging in several times per day, at the time of publishing this issue has already been remedied by the author.

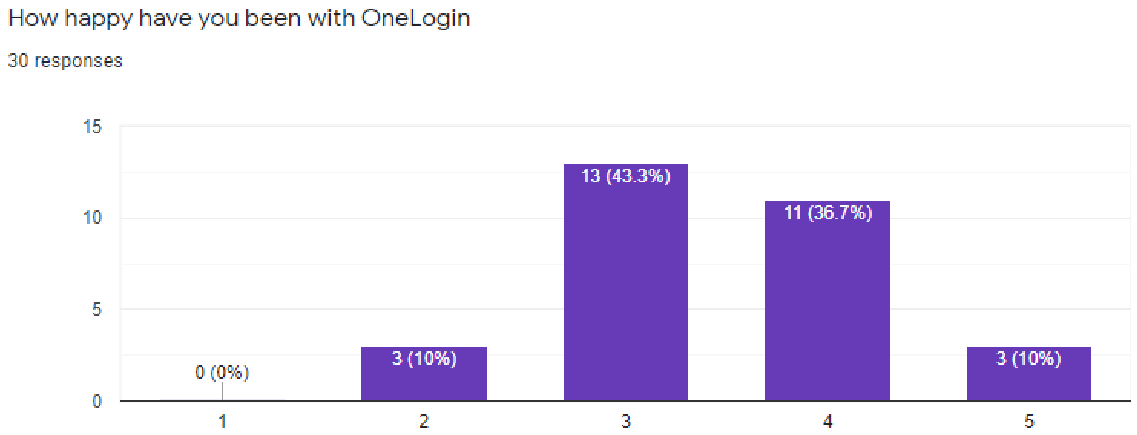


FIGURE 5. OneLogin satisfaction

The author experienced a significant streamlining effect to onboarding new employees, even with only a few of the general tools used by Castor integrated into OneLogin. Previously the author would have to create every account manually, sending a customised email to each starting employee containing unique information for each. With OneLogin pulling new employee data from

BambooHR the creation of several important accounts was automated using the provisioning feature offered by OneLogin. What could not be automated was manual work, but there was significantly less for the author to do manually. A single group email was sufficient to send to all new employees in February and March.

6 CONCLUSIONS

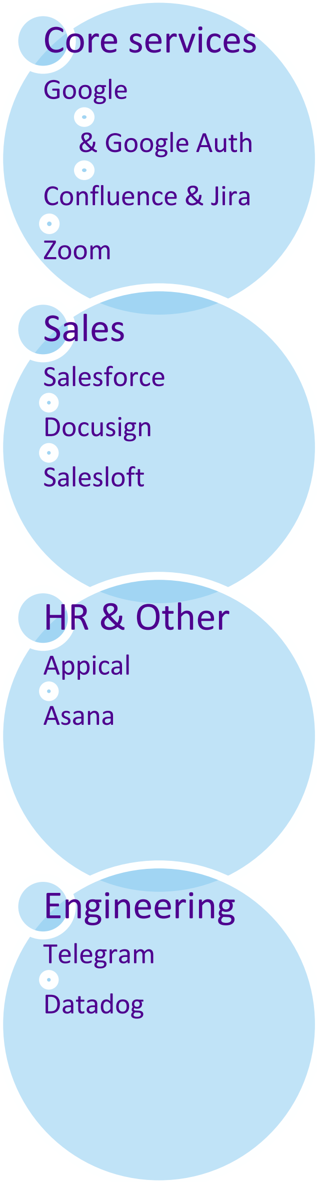
The effect SSO had on the onboarding procedure was demonstrated to the author when they onboarded eight people, a record-breaking number, on the fourth of January 2021. The author’s workload had been greatly reduced by automated provisioning creating accounts. During the onboarding session for new employees, the process of users logging into their tools was much simpler, with users only needing to login once to OneLogin, instead of separately to several services (Figure 6). Further automation will improve this effect on the efficiency of the onboarding process even more. Combined with the automation of other onboarding processes with e.g. eLearning and Appical, the onboarding of new employees will take less time and effort from HR and IT, as well as direct managers, whenever a new employee joins Castor.

Access control management is a critical component of the compliance to standards Castor has certifications for. Automating this process, while making it less work intensive and thus saving the time of Castor personnel in both access control and accessing applications, will improve Castor’s compliance and thus make its products easier to sell to increasingly more security conscious commercial clients.

The results from the data collected were both surprising and expected. More employees than anticipated were happy with LastPass, while there was some lukewarmness to OneLogin. This reaction to OneLogin was to be expected, as it is a paradigm shift in how authentication works at Castor. OneLogin is not a password manager, but it can operate as such enough to compensate, as there will always be some web applications that are not compatible with SSO. Password sharing capabilities, which OneLogin does not have currently, are less important as Castor policy states sharing of accounts is no longer allowed.

Suggested changes to the access control procedure will be as follows. Services successfully integrated to OneLogin can be removed from the Access Control for Tools sheet. Instead, at each check interval a report of each tool will be generated for tool owners to review. Workflow-wise this will differ little from how the work was done with the sheet. As a result of access control being automated in this way, the Access Control for Tools sheet can be shrunken down significantly, and continue to shrink as more services are either added to OneLogin or replaced with services that do support SSO.

Recommendations for changing the purchase procedure for tools are: add requirement for every new tool to either support SSO via SAML or Google. This will ensure no further pressure is put upon onboarding or offboarding procedures and will improve on security by minimising human input required for granting, and more importantly revoking, access. With this simple addition to the Supplier Purchase Procedure, Castor can improve its infrastructure scalability considerably.



Core services

- Google
- & Google Auth
- Confluence & Jira
- Zoom

Sales

- Salesforce
- Docusign
- Salesloft

HR & Other

- Appical
- Asana

Engineering

- Telegram
- Datadog

FIGURE 6. Castor tools with SSO implemented at time of publishing.

REFERENCES

Arias, D. 2019. Hashing Passwords: One-Way Road to Security. Auth0 Blog. Auth0® Inc. Published on 30.9.2019. Read on 8.3.2021. https://auth0.com/blog/hashing-passwords-one-way-road-to-security/

Castor. N.d. About us. Read on 2.3.2021. https://www.castoredc.com/about-us/

Castor. N.d. Compliant with ISO Standards. Read on 2.3.2021. https://www.castoredc.com/compliant-with-iso-standards/

Castor. 2020. Information Security policy. Unpublished. In thesis author's possession.

Castor. 2020. Access control procedure. Unpublished. In thesis author's possession.

Castor. 2020. Castor Raises a $12M Series A to Further Their Support for COVID-19 Research.

CyberArk Software Ltd. N.d. OpenID Connect (OIDC) Authenticator. Read on 8.3.2021. https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-DAP/Latest/en/Content/OIDC/OIDC.htm

Halkos, G. 2008. The influence of stress and satisfactionon productivity. Department of Economics. University of Thessaly. Research Paper in Economics. https://content-webapi.tuni.fi/proxy/public/2020-04/thesis-report-guide-april-2020_2.pdf

ICH GCP. 2016. Guideline for good clinical practice E6(R2). London: European Medicines Agency. Read on 7.3.2021. https://www.ema.europa.eu/en/documents/scientific-guideline/ich-e-6-r2-guideline-good-clinical-practice-step-5_en.pdf

Knafo, J. 2018. Password Manager vs. Privileged Access Management (PAM) vs. Single Sign-On (SSO). In The Trenches blog. Published 20.12.2018. Read on 8.3.2021. https://blog.devolutions.net/2018/12/password-manager-vs-privileged-access-management-pam-vs-single-sign-on-sso

Konterman, R. Chief Operations Officer. 2021. Meeting on 26.2.2021. Private meeting with author.

Lujan, V. 2019. What's the Difference b/w SSO (Single Sign On) & LDAP?. Blog. Read on 7.2.2021. https://jumpcloud.com/blog/sso-vs-ldap

Lutkevich, B. 2020. Access control. SearchSecurity. TechTarget. Updated on 9.2020. Read on 8.3.2021. https://searchsecurity.techtarget.com/definition/access-control

NEN-ISO/IEC 27001. 2013. Information security management systems – Requirements (ISO/IEC 27001:2013,IDT). Amsterdam: The Royal Netherlands

Standardization Institute. Read on 7.3.2021. In thesis author’s possession. Castor’s purchased copy.

Smidt-Verhulst, V. 2019. Supplier / Purchasing procedure (v.75). Unpublished. Accessed on 7.3.2021. In thesis author’s possession.

Oasis Open. 2008. Security Assertion Markup Language (SAML) V2.0 Technical Overview. Read on 8.3.2021. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

OneLogin. N.d. Secure Single Sign-on (SSO) Solution. Read on 2.3.2021. https://www.onelogin.com/product/sso

OpenID Foundation. N.d. Welcome to OpenID Connect. Read on 8.3.2021. https://openid.net/connect/

Peyrott, S. 2015. What Is and How Does Single Sign-On Authentication Work?. Auth0 Blog. Auth0® Inc. Published on 23.9.2015. Read on 8.3.2021. https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/

APPENDICES

Appendix 1. Castor’s Procedure Table of Content

1 (2)

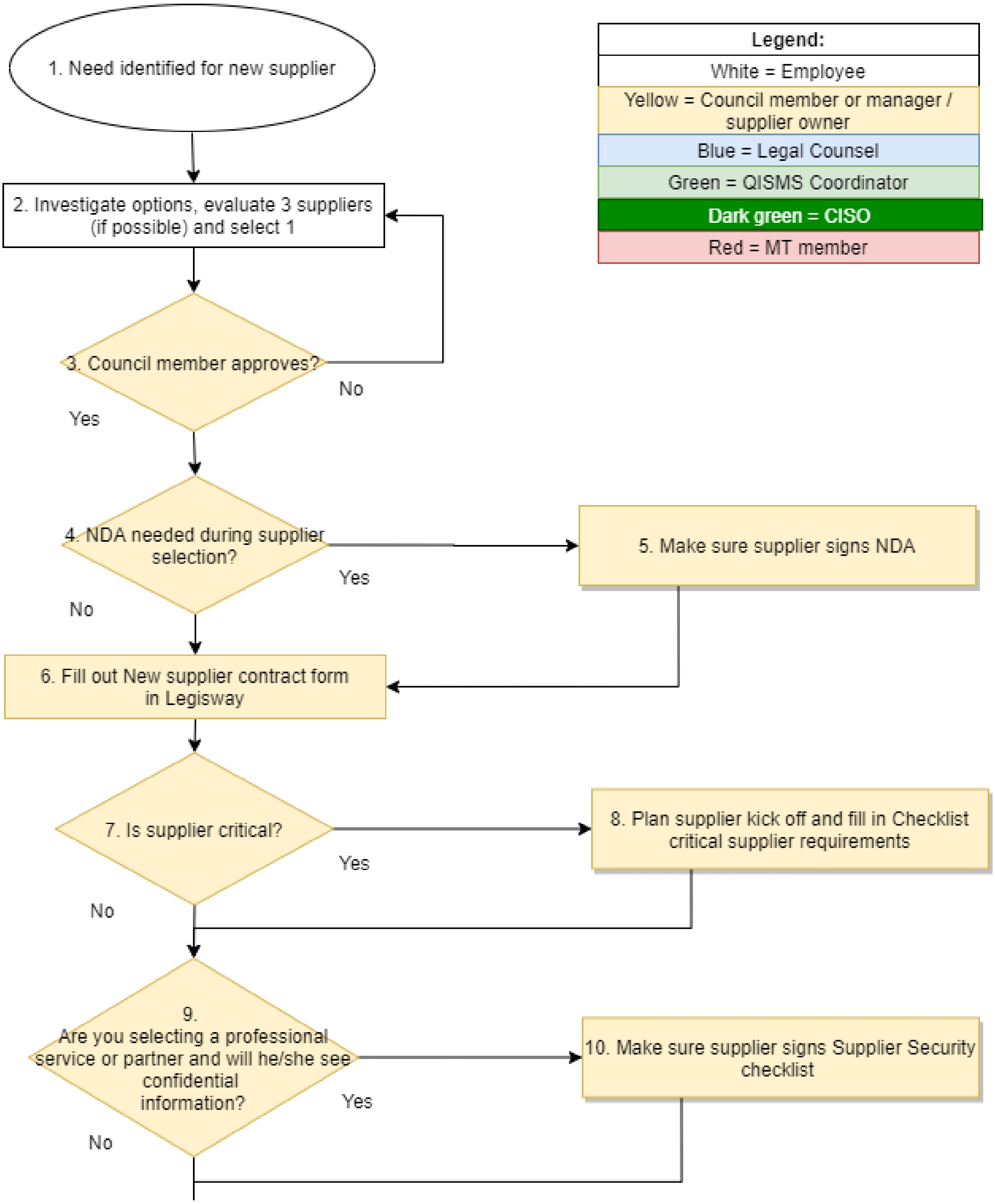
Disclosure: *This information is proprietary to Castor EDC and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.*

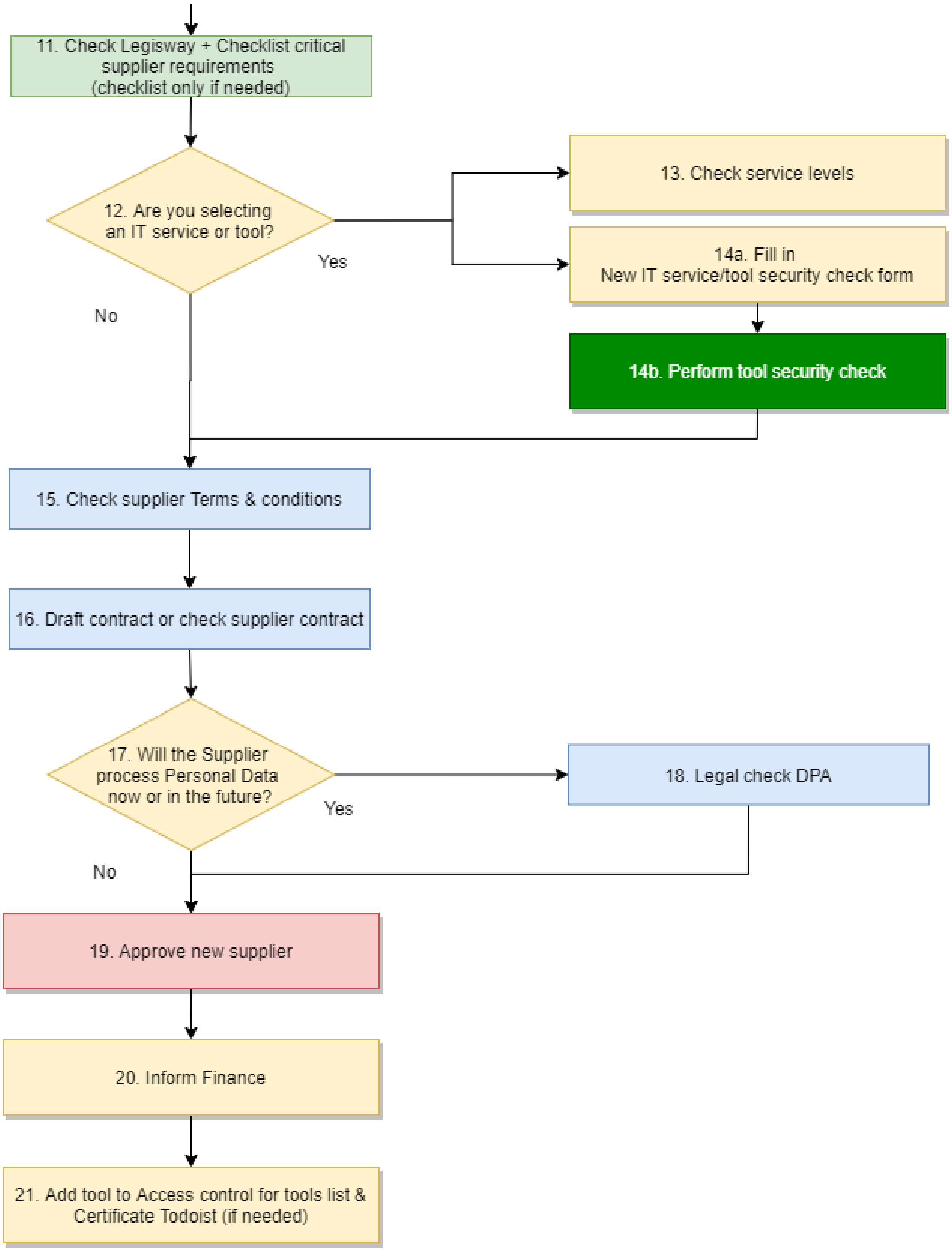
Domain	**Document / Subject**
Operational processes	QISMS Process model
ISO for Management	Stakeholder and context analysis
ISO for Management	Risk Assessment and Risk Treatment Methodology
ISO for Management	Risk Assessment and Risk Treatment Table
ISO for Management	Scope QISMS CIWIT BV & Castor Research Inc
ISO for management	Quality Policy
General ISO documents	Information Security Policy
ISO for Management	Communication structure (internal)
ISO for Management	Communication structure (external
People management	Security checklist
ICT management	Operating Procedure for ICT
ICT management	Office IT Management procedure
ICT management	Secure Development & Quality Assurance Policy
ICT management	Access control for tools
ICT management	Access control procedure
General ISO documents	Business Impact Analysis
Operational processes	Marketing Procedure
Operational processes	Sales Procedure
Operational processes	Procedure for onboarding institutes, commercial customers and researchers
Operational processes	Procedure for offboarding institutes and researchers (to be drafted)
Operational processes	Account Management Procedure
Operational processes	New product/feature procedure - EDC
Operational processes	New product/feature procedure - SMS
Operational processes	New product/feature procedure - eCOnsent
Operational processes	Study Mangement System Implementation procedure
Operational processes	Customer Success Management Procedure
Operational processes	Invoicing procedure
General ISO documents	Security statement
General ISO documents	Privacy and cookie policy

Legal & Privacy	Register of Relevant Law & Regulations Ciwit B.V.(in Legisway)
People management	Recruitment process (Confluence)
People management	Onboarding guide & Onboarding checklist & Offboarding checklist (Confluence)
People management	Contractor Onboarding checklist & Contractor Offboarding checklist (Confluence)
People management	Non Disclosure Agreement (one & two-sided)
People management	Code of Conduct
People management	Registration physical access office (tag registration)
GDPR Data Processing Activity Register	GDPR Data Processing Activity Register
People management	Employee Evaluation Procedure
People management	Supplier Policy
ISO for management	Supplier / Purchasing procedure (Confluence)
Supplier management	Procedure for offboarding a supplier (Confluence)
Supplier management	Procedure for Contracting a Contractor (Confluence)
Supplier management	Template Checklist critical supplier requirements
Supplier management	Information Security Incident Management Procedure
General ISO documents	Personal Data Breach Management Procedure
General ISO documents	Statement of Applicability ISO27001
General ISO documents	Statement of Applicability NEN 7510
General ISO documents	Document Management Procedure
Internal audits	Internal audit procedure
Internal audits	Internal audit program
Project Management	Project risk procedure
Project Management	Template Project risk analysis
General ISO documents	ISO 27001 and ISO 9001 action list (CAPAs) in Legisway
People management	Organizational chart (Bamboo HR)
Audits	Internal audit program
Audits	External audit plan 9001
Audits	External audit plan 27001
Continuity	Continuity policy
Continuity	Contact info key contacts (Confluence)
Continuity	Continuity tests
Continuity	Safety instructions
General ISO documents	Procedure for non conformities and corrective actions (CAPA)
General ISO documents	Castor EDC 21 CFR part 11 Compliance statement
General ISO documents	Castor SMS 21 CFR part 11 Compliance statement
General ISO documents	Castor EDC Web Accessibility policy
General ISO documents	Castor EDC Public Web Accessibility Statement
Legal & Privacy	Data Subject Request Procedure
General ISO documents	Castor list of quality and information security documents
Legal & Privacy	MHRA Serious Breach Management Procedure

Appendix 2. Supplier purchase procedure flowchart

1 (2)

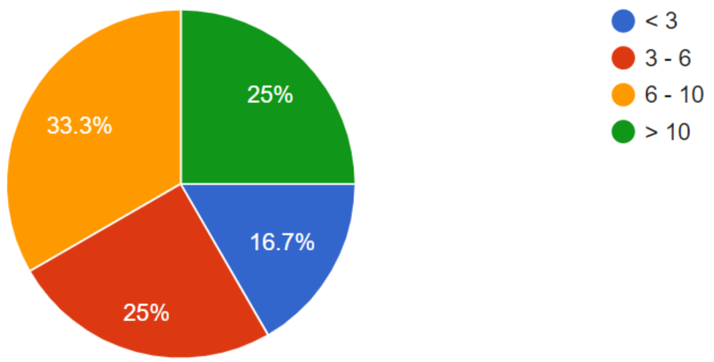

Legend:
White = Employee
Yellow = Council member or manager / supplier owner
Blue = Legal Counsel
Green = QISMS Coordinator
Dark green = CISO
Red = MT member
1. Need identified for new supplier
2. Investigate options, evaluate 3 suppliers (if possible) and select 1
3. Council member approves?
No
Yes
4. NDA needed during supplier selection?
Yes
No
5. Make sure supplier signs NDA
6. Fill out New supplier contract form in Legisway
7. Is supplier critical?
Yes
No
8. Plan supplier kick off and fill in Checklist critical supplier requirements
9. Are you selecting a professional service or partner and will he/she see confidential information?
Yes
No
10. Make sure supplier signs Supplier Security checklist


11. Check Legisway + Checklist critical supplier requirements (checklist only if needed)
12. Are you selecting an IT service or tool?
Yes
No
13. Check service levels
14a. Fill in New IT service/tool security check form
14b. Perform tool security check
15. Check supplier Terms & conditions
16. Draft contract or check supplier contract
17. Will the Supplier process Personal Data now or in the future?
Yes
No
18. Legal check DPA
19. Approve new supplier
20. Inform Finance
21. Add tool to Access control for tools list & Certificate Todoist (if needed)

Appendix 3. Tool admin/owner questionnaire results

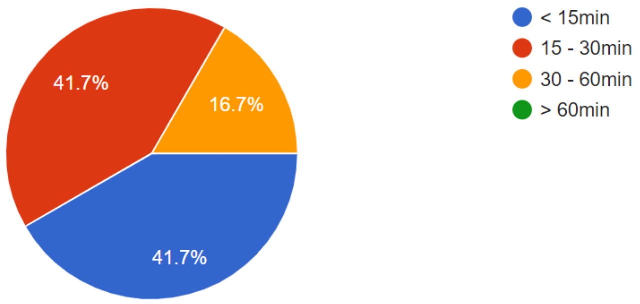
(Roughly) how many tools do you own and/or admin in Access Control for Tools?

12 responses



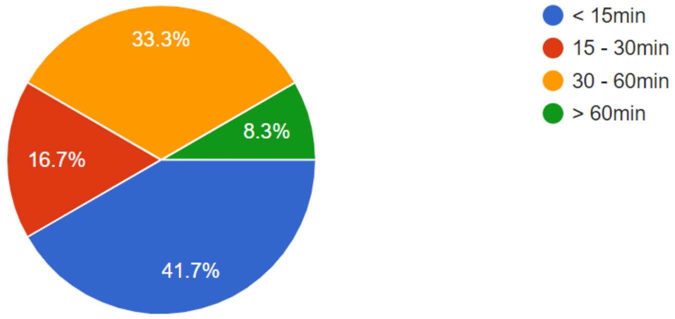
How much time would you estimate you use to work in Access Control for Tools on a monthly basis?

12 responses



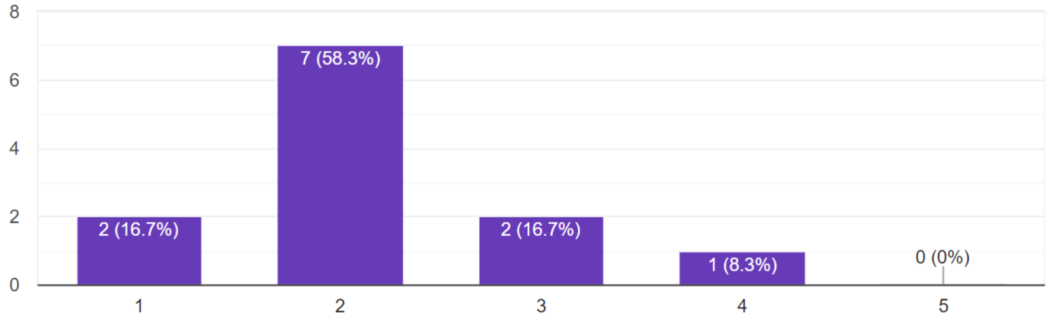
How much time would you estimate you use to work on account management in the tools you own/admin on a monthly basis?

12 responses



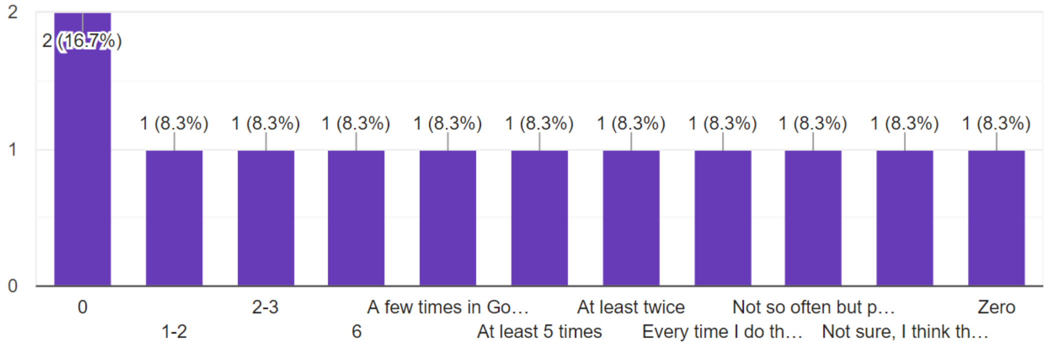
How happy are you with the Access Control procedure in place?

12 responses



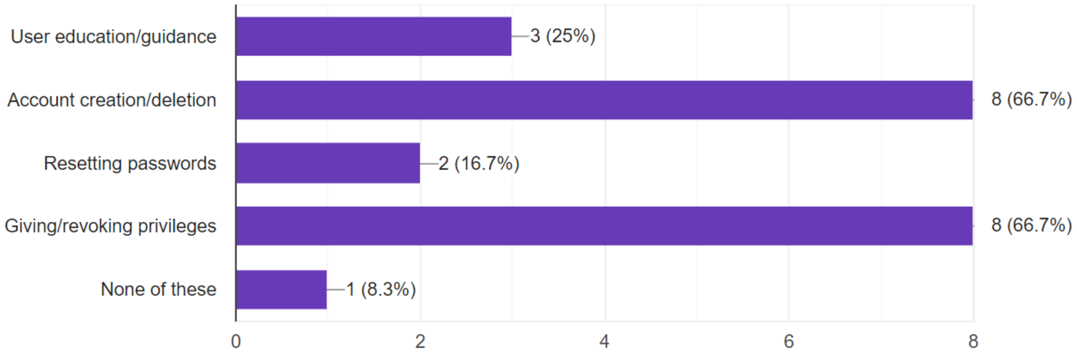
How many times in the past quarter have you noticed someone having access when they shouldn't have? (Unauthorized access)

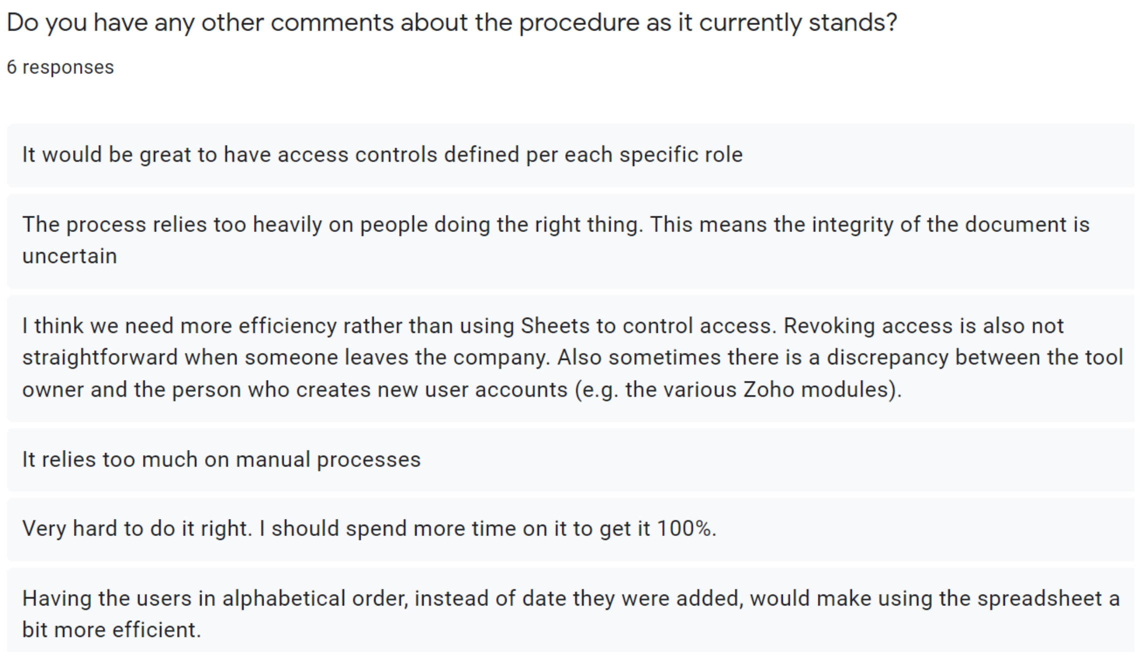
12 responses



Which of the following do you spend time on each month? (select all that apply)

12 responses





Do you have any other comments about the procedure as it currently stands?

6 responses

It would be great to have access controls defined per each specific role

The process relies too heavily on people doing the right thing. This means the integrity of the document is uncertain

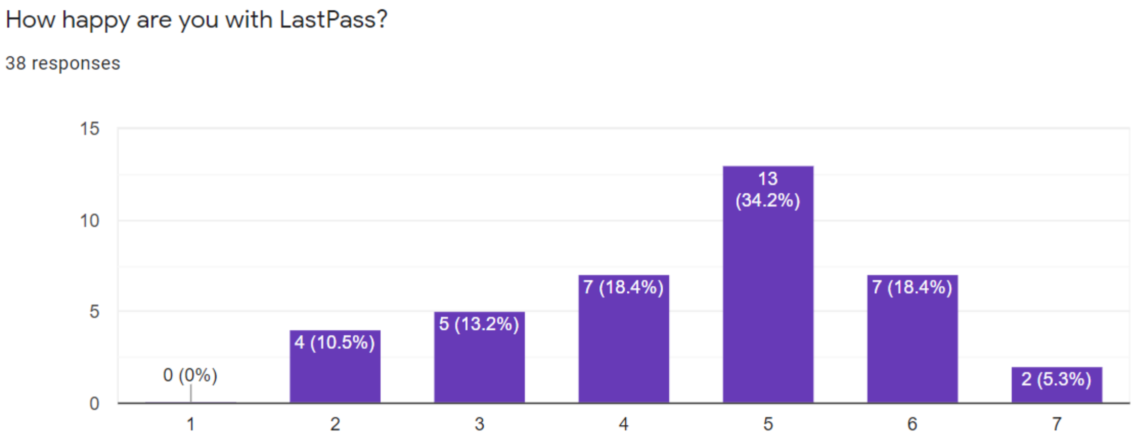
I think we need more efficiency rather than using Sheets to control access. Revoking access is also not straightforward when someone leaves the company. Also sometimes there is a discrepancy between the tool owner and the person who creates new user accounts (e.g. the various Zoho modules).

It relies too much on manual processes

Very hard to do it right. I should spend more time on it to get it 100%.

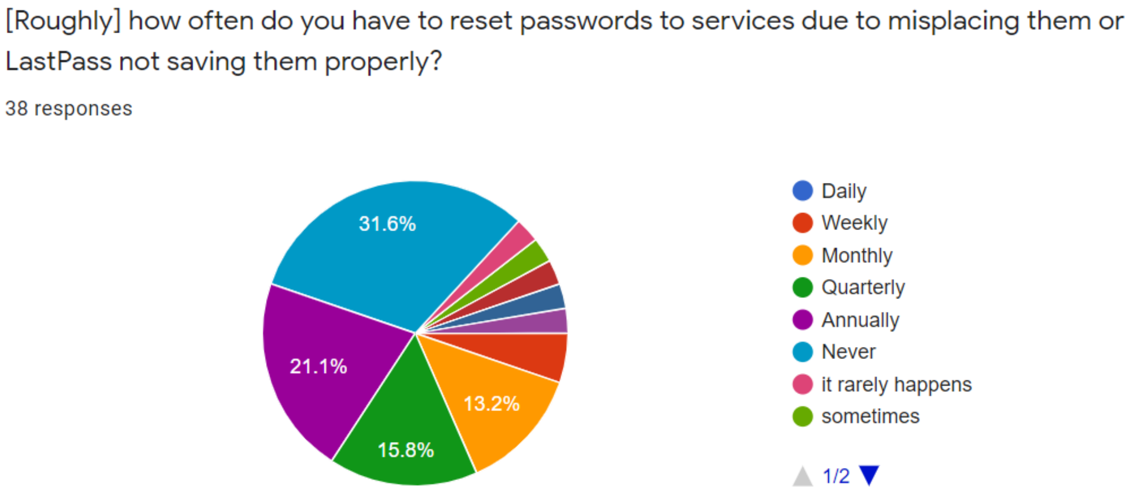
Having the users in alphabetical order, instead of date they were added, would make using the spreadsheet a bit more efficient.

Appendix 4. First end user questionnaire results



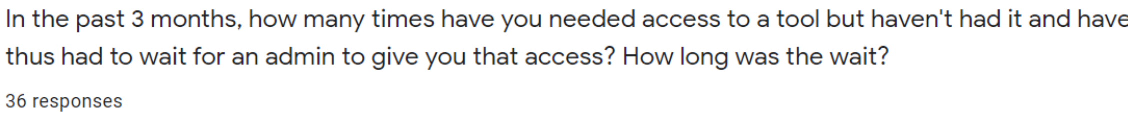
How happy are you with LastPass?

38 responses



[Roughly] how often do you have to reset passwords to services due to misplacing them or LastPass not saving them properly?

38 responses



In the past 3 months, how many times have you needed access to a tool but haven't had it and have thus had to wait for an admin to give you that access? How long was the wait?

36 responses

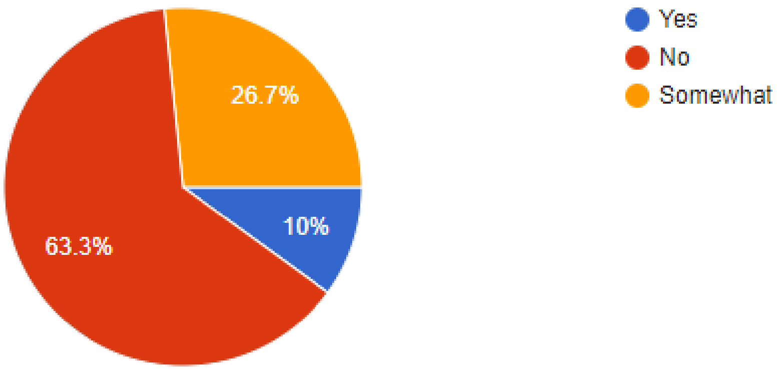
- 0
- n/a
- -
- None
- I'm a new starter, so the frequency would be higher for me. This has happened twice and I've had to wait about an hour for this.
- maximum 3 business days
- I started fewer than 3 months ago, so I'm not statistically valid
- 3 times, less than 24 hours
- Happened once, and I waited for less than one hour
- Zero times
- 1-2 days

- 1-2 times, a few hours up to ~2 days
- Within the day
- Once, and I got the access within an hour
- at least 4. Waiting was short, less than 1 day
- About 4 times, waited a few hours at most
- None
- Only had to do it once, access was given promptly, perhaps 30min wait?
- Once
- Once, 1 day
- 1 time, had to wait only 1 hour.
- I think once or twice, never had to wait long to get it - happy with that
- 3 times / 1 day
- Haven't experienced this.
- 1 time. Wait time ~2 hours.
- maybe 3-5 times. I did not have to wait long: maybe a few minutes
- 3 times. 1-2 days.
- 1-2 times, 30 minutes tops
- 3 times and I had to wait a few hours tops
- Few times (1-3), usually only a few hours.

Appendix 5. Second end user questionnaire

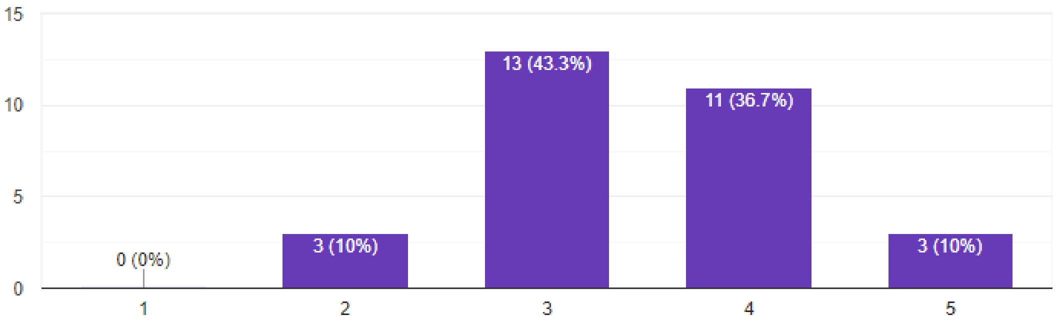
Have you been able to stop using LastPass since OneLogin became available?

30 responses



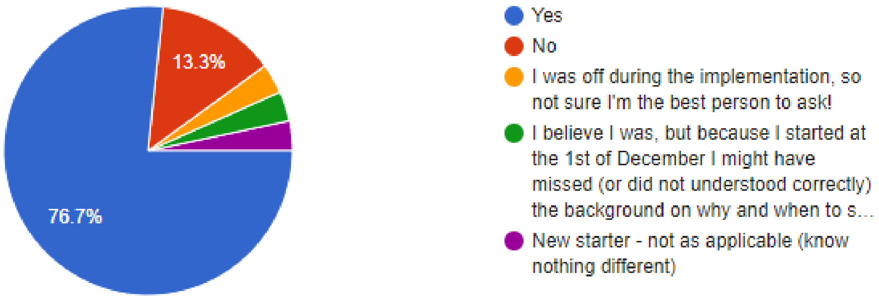
How happy have you been with OneLogin

30 responses



Do you feel you were informed sufficiently on the OneLogin implementation?

30 responses



Any other comments? (Voluntary)

15 responses

- It looks like it is not possible to add websites manually to OneLogin?

- I memorize all the passwords, from my use case both LP and OL add noise; still good transition from one to the other
- I don't quite seem to get OneLogin. How do I save a password? It only has these "Apps", and if one doesn't exist, there's no way to add one (the "Don't see what you need? + New" button doesn't work). Regarding migrating from LastPass: most of my staff there is shared, so I guess someone else has to migrate that? I also don't see anything about shared credentials in OneLogin.
- It's hard to communicate these "life admin" type things across the business, and I think you did a pretty good job of using multiple channels to keep everyone up to speed. :)
- OneLogin logs you out too frequently.
- The issues with the shared people inbox have been annoying. I'm still using LastPass because I didn't realise we can use OneLogin as a password manager too. If it aint broke...
- I don't use it, it's often not turned on and therefore not saving passwords.
- I could use some tips on how to move away from lastpass completely. I saw I have a few accounts that require a username and password (like calm, quay.io, jetbrains). Would like to know how I can still keep those passwords stored safe somewhere
- Do we let go LastPass now?
- Thanks for making the transition to onelogin smooth and for helping out always.
- I've not spent the time transferring all my passwords across to OneLogin from Lastpass as I've not had too many issues with Lastpass in the past. From what I've seen, OneLogin works well for those sites where I have passwords stored in OneLogin. I've just not used it enough to comment further.
- unclear on the interaction and preferred approach between OneLogin and Google Auth. It seems One Login can act as Google Auth. Unsure of the company recommandations and expectations
- The interface is oversimplified compared to LastPass, and yet there isn't a big, obvious "add new site here" which makes it difficult to quickly switch over. It doesn't seem to detect sites with passwords as well as LastPass and doesn't offer to save them automatically.
- As a contractor I totally missed this
- It would be nice if we don't have to log into OneLogin every 2-3 hours. Also, I feel like OneLogin does not give the option to store your passwords as often as LastPass does. Is there some instructions?