

# Feasibility assessment of Cloud SaaS enabled collaboration and information confidentiality for the public accounting industry

Lior Baron<sup>1</sup>[0000-0003-0257-9100] and Tzipora Halevi<sup>2</sup>[0000-0003-3988-0239]

<sup>1</sup> CUNY Graduate Center, New York NY 10016, USA

<sup>2</sup> Brooklyn College, Brooklyn NY 11210, USA

**Abstract.** In recent years, the growing use of Software as a Service (SaaS) presents both new opportunities and challenges for organizations. Specifically, building trust in SaaS as an alternative to traditional methods of conducting business presents unique challenges for the CPA industry, who deals with sensitive financial client information and strict regulations. This study seeks to understand the attitudes and behavior of CPA industry staff members facing changing technology in the workspace. It investigates the usability of cloud SaaS collaboration platform, utilizing Microsoft Office 365 based solution and Microsoft SharePoint Online technology. It examines whether CPA staff members can overcome preconceptions about trust in SaaS tools. Specifically, can these tools, which store client information in the cloud, be used to safely exchange sensitive information between two parties while allowing CPA firms and clients to effectively collaborate on projects.

The study design included a walk-through experiment as well as a semi-structured interview survey consisting of both open and closed-ended questions. The study participants were asked to use a pre-configured SharePoint collaboration portal and execute several predefined financial common tasks, following prescribed testing script, as well as fill an online survey regarding their experience. The study results demonstrate that CPA team members felt the software provides a better platform for communicating with clients than the currently used tools. However, participants' comfort level managing specific sensitive client information on the new online portal was lower, pointing to the potential need for follow-up training and improved education for CPA team members on the SaaS platform capabilities.

**Keywords:** Secured online collaboration, SaaS, Cloud, Accounting, Usability

## 1. Introduction

The interaction between public account firm and their clients makes an interesting case for secured human computer interaction investigation. The nature of the services CPA firms offer to their client requires sharing of large amount of sensitive financial and operational information between clients and CPA firms which typically clients will not share with outsiders.

Public accounting firms in the US and elsewhere offer several services to clients which require collaboration during time bound projects. For example, most tax compliance work, whether personal or corporate tax filings, require the CPA firm to meet deadlines set by the federal or state government and missing deadlines could potentially result in financial penalties to clients. During the preparation of a tax return, the accounting firm will ask the clients to produce sensitive financial information and will use this information to prepare the tax return. The challenge many

accounting firms face is how to effectively collaborate with clients while not compromising the client's sensitive financial information and maintaining a high level of trust with the client.

Before the age of electronic records, firms and individuals communicated with accounting firms either in person (e.g. delivering required documents for tax preparation) or via US Postal Mail, in which case both parties trusted the US post office and mail delivery to be secured and had high confidence that the information sent by mail will not be compromised. Since electronic records became the prevailing methods during the 1990s, secured means of electronic communication had to be established directly between the accounting firm and their clients since no third-party standard (like the US postal mail) was acceptable as reliable and secured. Many software companies rose up to the challenge and provided secured email communication and secured file transfers. As a result, CPA firms have many software solutions available for secured collaboration from several vendors which don't integrate well and present challenges for effective collaboration. For example, a CPA company might use a product like ShareFile or sFTP site for secured file transfer and MimeCast for secured email communication. When interacting with a client, the CPA firm will ask the client for sensitive information in an email with instructions on how to set up MimeCast secure email login and send the client a ShareFile password using secure email enabled by MimeCast before collaboration can take place. The client will then use the ShareFile password to upload the file. Thus, the client's staff is required to maintain two additional login credentials for collaborating with the CPA firm. If the CPA firm uses other products for collaboration (Chat software or online survey tools) the number of credentials managed by the client will increase. The collaboration process requires the CPA firm's client to manage a set of passwords for several tools and client standards for maintaining password could become an issue, especially in situations where there are several people at the client organization that require login to ShareFile and/or secured email and other tools.

### **1.1 SaaS cloud technologies for collaboration**

There are several SaaS platforms for collaboration that offer secured file transfer, secured communication and secured online collaboration space from which Microsoft's Office 365 and Google's G Suite are probably the most common. These platforms provide an integrated secured environment for individuals and firms to collaborate on files, communications, calendars and tasks. Both platforms [5][6] use security at rest, secure file transfer S/Mime protocols, secured online access using https and two-step verification along with email spam and phishing filtering to ensure secure communication. Both platforms are certified by ISO, AICPA and HIPPA standards. In addition, the platforms integrate with a company's corporate directory, so there is no need for additional password management or risk that a departed employee will maintain access to the company's sensitive information. The integration with corporate security is an important feature of these enterprise collaboration software since it ensures that only active employees of the firm have access to online corporate resources. Once an employee leaves the corporation, their access to corporate resources including online collaboration software is eliminated.

Microsoft Office 365 software is the more robust option for both small and large corporations. It does not only include email and file sharing capabilities[5], but also a wide range of products which offer enhanced online collaboration experience. These include tools like SharePoint for online capabilities rich collaborative work space, MS Teams for small team collaboration, MS Flow for data integration, OneDrive for cloud file storage, and other management/survey/editing tools that are useful for collaboration between CPA firms and their clients.

### **1.2 Study contribution**

This is the first usability study in a CPA firm examining online collaboration SaaS software that we know of. Since this software is intended to replace current tools which facilitate information exchange with the client, developing internal methods of assessing the acceptance of such a tool is useful both for understanding the improvements needed for this tool as well as create a method for future tools evaluation.. The CPA firm is seeking new and more efficient ways to work with clients and to leverage the available SaaS technology without negatively impacting client experience or information confidentiality. The CPA company is looking to integrate more SaaS software as a

strategic direction to both cut costs on IT infrastructure and improve operational efficiency of its staff. Therefore, the contribution of this study is twofold. First, this study introduced an assessment methodology for new products in-house, which can be used for follow-up evaluations as well. Second, the study provided insights that helped the CPA firm to assess adoption challenges in using a new SaaS software with Microsoft's Office 365 platform implementation as a client collaboration platform to deliver work efficiently. The findings from this assessment are discussed in detail in the results section.

## **2 Theoretical background**

Qualitative methods have been shown to provide deeper insights into the user experience when working with a new product [7], and have been utilized in previous usability studies in the financial industry by Conway et al. [1]. Accounting staff are facing deadline driven work schedule with pressure to execute a large volume of high-quality work while interacting confidentially with their client. The tight deadlines and pressure to maximize productivity may result in behavior that will compromise client information confidentiality. The qualitative part of our assessment seeks to better understand frame of mind and decision around client information confidentiality. The quantitative testing will assess whether the CPA staff members were able to complete common collaboration tasks while avoiding common mistakes that impact client information confidentiality.

Maxion et. al [11] pointed to usability challenges when conducted a study of file permission interface, developing an alternative file access management system. We use similar testing methods to conduct the usability part of our study. This work assesses whether the file permission interface of our chosen SaaS collaboration platform addresses some of the original challenges pointed out in [11]. Our work further explores additional challenges (beyond file sharing) related to online questionnaires, collaborative work planning, online discussion boards and team announcements.

## **3 HCISEC considerations**

### **3.1 Client Information**

CPA firm's client might be either a corporation or an individual seeking help with tax return, corporate audit, estate planning or other services. Whether the client is an individual entity (e.g. a person or a family) or a corporation, there are norms and guidelines that are generally accepted for interactions between CPA firms and clients as well as regulations set up by AICPA (in the US) and prevailing laws that specify what information the CPA firm needs to collect from clients to perform services. For example, an individual that hires a CPA firm to help with filing an individual federal tax return (form 1040 in the US) will be asked to provide the CPA firm with personal and financial information that will assist in tax preparation. A corporation seeking help with corporate tax might be required to provide information about sources of income (clients), vendors, payroll and products. Although the amount of client information could be large, the client is the source of information and is in full control of what information is shared with the CPA firm. According to those guidelines, the CPA firm must use the information for the sole purpose of providing the tax advice to the client and cannot use it for any other purpose.

### **3.2 Client Information Security**

CPA firms are required to ensure the safety of information provided by clients from the moment the information is shared with the CPA firm. The information might come in several formats, like printed materials, electronic files, emails, and electronic media (DVD or tape). Regardless of the format, the CPA firm must ensure that no outside party can access the data and that only authorized CPA staff members can access it to perform services. In the case of online collaboration portal for corporate clients, the client information security requirement can be satisfied by using a combination of factors:

- Client access - strict external user access provisioning in Office 365 collaboration portal in SharePoint Online using the clients' existing accounts Office 365 can provide the authentication needed for sharing data between clients and the CPA firm. The CPA sends an invitation to collaborate to the user account and the client must accept within a given timeframe. Since the invitation is personalized to a specific corporate named user account, the method will simply piggy-back on existing client authentication capabilities.
- CPA staff access – the Office 365 groups provide an intuitive access provisioning interface for client team with ability to check effective access to verify correct configuration. In addition, by using a SharePoint feature called Site Collection for client collaboration, the chance for unintended staff access is further reduced since each site collection has a dedicated access configuration setup and does not share access credentials with other sites outside the collection. The CPA firm needs to have procedures in place to make sure client team access is properly maintained (by the client team) and change in team membership is reflected in the online collaboration portal.
- Hardware / Server unintended access risk – since the online collaboration portal uses cloud-based SaaS – Office 365, IT staff or non-client team staff member do not need access to the client information at all. The CPA firm does not need to maintain the infrastructure that stores this information, as the software provider (Microsoft) ensures the safe storage of the client information on its cloud servers.

### **3.3 Encryption consideration for online collaboration**

Encryption at rest - File storage for Office 365 collaboration is using Microsoft product called OneDrive for Business. Encryption for the OneDrive for Business product is facilitated by using bitlocker at the disk level and file / transaction level encryption and are compliant by Federal Information Processing Standard (FIPS) 140-2 according to Microsoft [9]. Encryption-in-transit for SharePoint online and OneDrive for Business uses SSL/TLS connections with 2048-bit keys. The SSL/TLS connections are used by both CPA firm staff and clients to upload or access shared information in OneDrive for Business and SharePoint Online.

## **4 Portal Implementation**

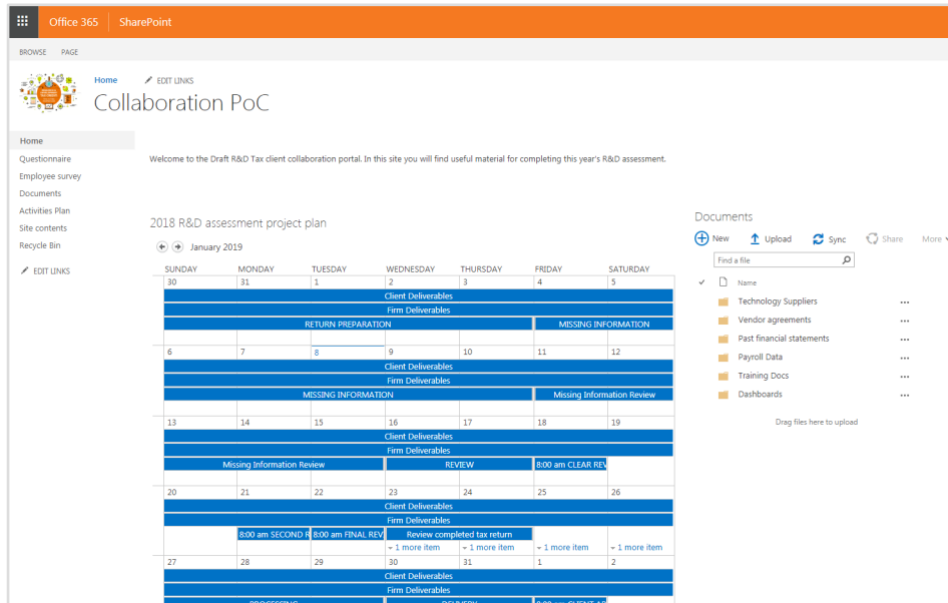
To examine how an accounting firm can successfully collaborate with clients using a cloud based online collaboration tool, we used Microsoft Office 365 based solution which used Microsoft SharePoint Online technology for collaboration. The collaboration portal is used for collaboration between the accounting firm and corporate clients seeking to benefit from R&D tax credits at the federal or state level (IRS Form 6765 and various state tax forms). The tax credit work requires an investigation by the accounting firm of activities that will allow the client to maximize R&D tax credits given by the US federal government or states in which R&D activity took place. Typically, the process of collecting evidence for R&D tax credit requires the following collateral to be provided by the client -

1. A qualified R&D activity (a questionnaire is used to identify activities)
2. Identify R&D related investments to support these activities – Those include
  - An assessment of payroll expenses related to R&D (By employee, how much time allocated for R&D support)
  - Supplies cost related to R&D
  - Contracted support (vendor) cost in support of R&D work
3. For each of the three areas of R&D cost identification, the client needs to provide proof in the form of documentation and answering questions in pre-defined criteria. Depending on what the initial set of questions uncovers, more questions might be used to correctly classify R&D related activities that pertain to tax credit by federal or state level tax return.
4. The online collaboration portal support functionality needed for the R&D tax credit work (questionnaire and ability to upload documents as evidence).

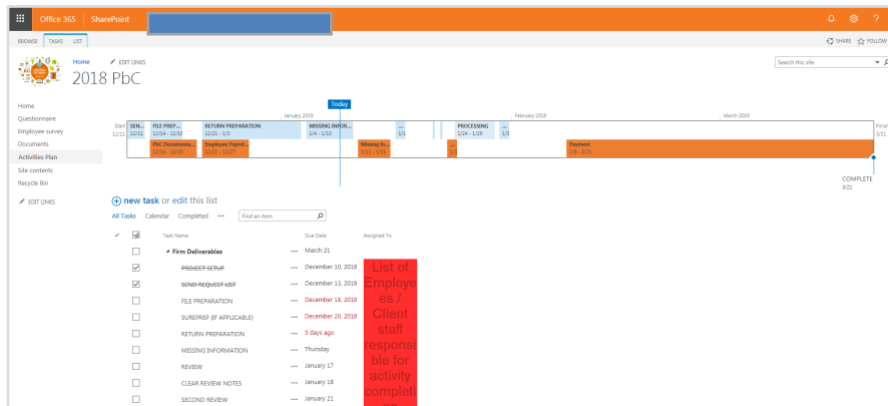
The collaboration portal included the following features to enable successful collaboration:

- A dedicated SharePoint site collection using the accounting firm's Office 365 subscription
- Sharing with external users feature enabled

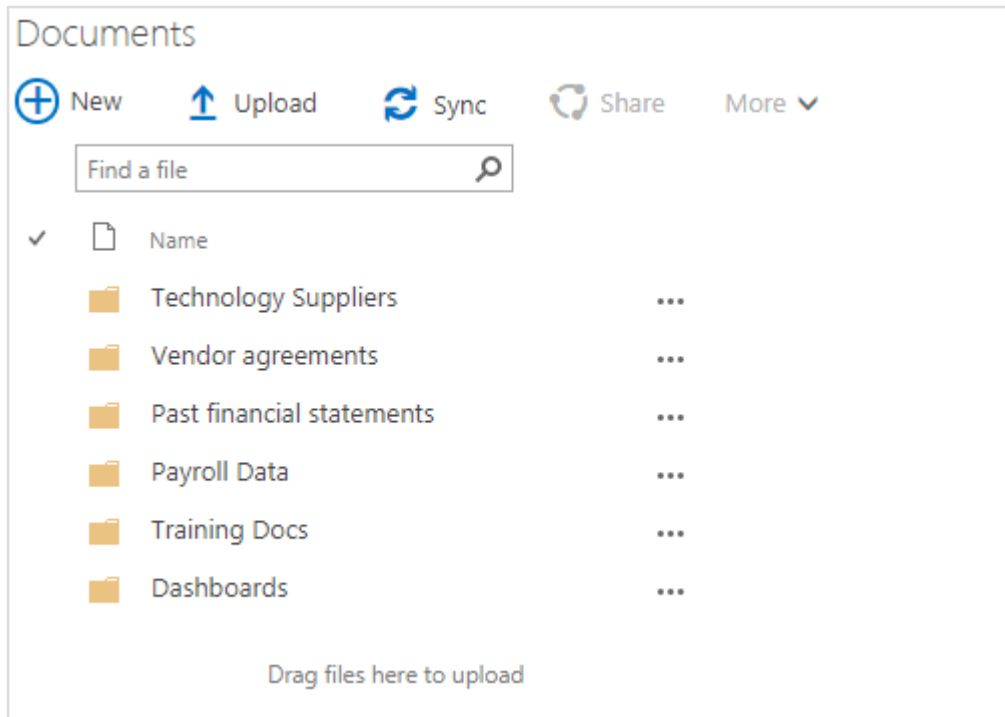
The user interface screens used for setup are shown in figures 1-4.



**Fig. 1.** The Primary landing page of the collaboration portal, displaying a team calendar and a list of online folders



**Fig. 2** SharePoint task list for tracking activities, assignments, dependencies and dates



**Fig. 3.** Shared Documents repository

Home EDIT LINKS

## Employees Questionnaire

Assign Payroll R&D Credit %  
[Stop](#) editing this list

✓	Name	SSN	Annual Payroll	R&D Allocation %	Responsible	R&D Payroll	Validated	+
	Emp ... 1	123-45-6789	\$100,000.00	75 %	Lior Baron	75,000		
	Emp ... 11	123-45-6799	\$100,010.00	24 %	Lior Baron	24,002.4		
	Emp ... 18	123-45-6806	\$100,017.00		Lior Baron	0		
	Emp ... 19	123-45-6807	\$100,018.00		Lior Baron	0		
	Emp ... 2	123-45-6790	\$100,001.00	75 %	Lior Baron	75,000.75		
	Emp ...	123-45-						

**Fig. 4** SharePoint List to capture employee payroll R&D survey. The survey is a SharePoint list containing client's employee classification questionnaire using payroll data – Client subject matter experts will classify portion of time allocation by employees to R&D activities to claim tax benefits

## 4.1 Security Configuration - SharePoint Site Collection level

### A. Client access:

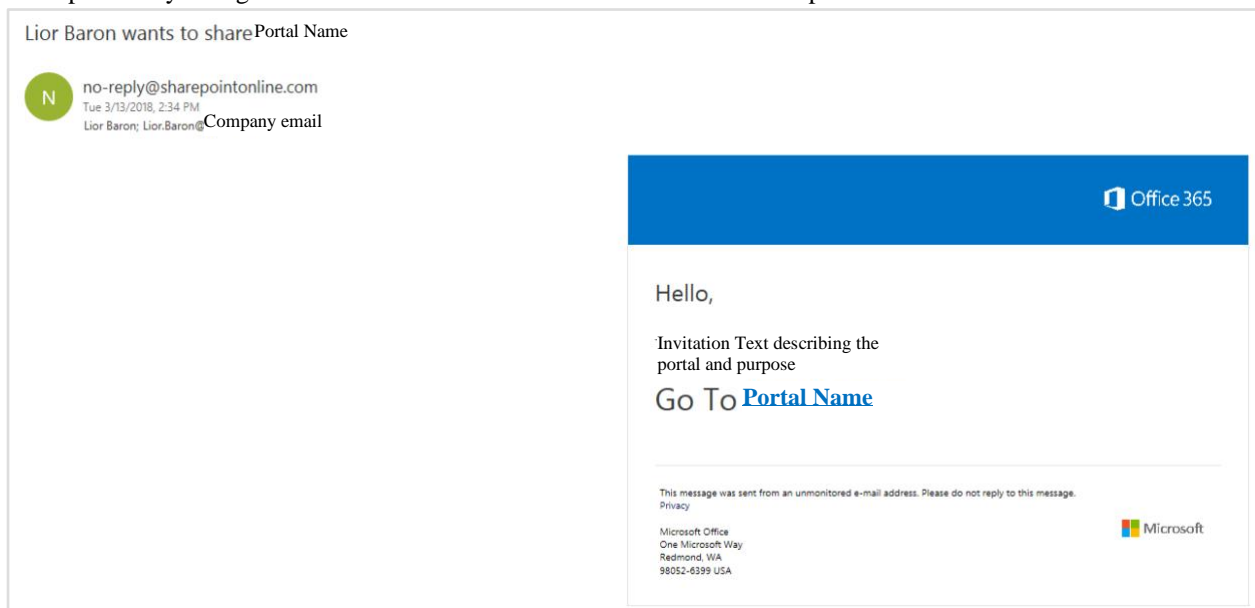
Client personnel which need access to the online portal are sent an invitation by the accounting firm portal team to their business email address (that is linked to the client corporate Office 365 account). To allow addition of users from outside the CPA firm Office 365 domain, an administrator must enable external sharing to the site collection by following the instructions [10]. Due to the expected large number of clients, the configuration used for the CPA firm is to allow external authenticated users to use their Microsoft work or school account authentication to access the shared content.



**Fig. 5** SharePoint Site Collection External User Access Configuration Screen

The email request has a link by default to accept the invitation. Only after accepting the invitation will the client staff members get access to the portal. The invitation is linked to the Office 365 account of the client staff user's email. If somehow another person tries to use the link with a different account (other than the named user in the email) it access will not be granted.

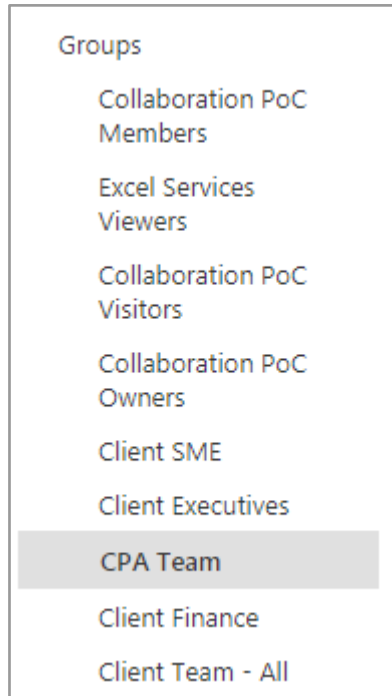
Example of a system generated client invitation to the online collaboration portal sent to client



**Fig. 6** Example of system generated email inviting an external user to log on

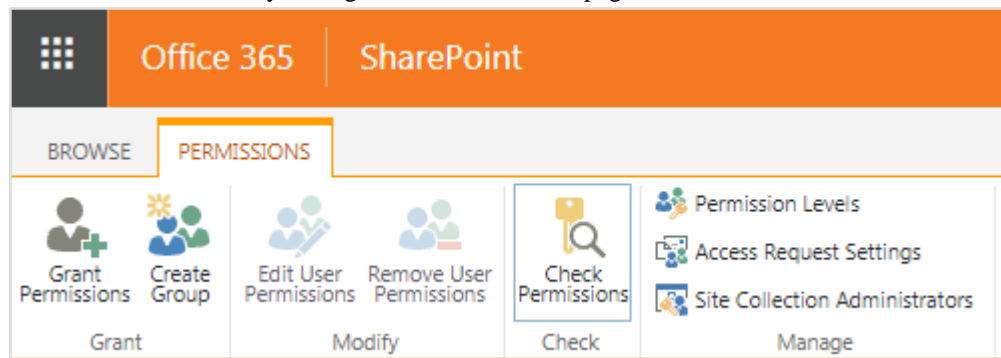
## B. User access right provisioning:

Access rights in R&D credit portal use group membership to allow / restrict access to content in the collaboration portal. Each module in the portal can either inherit access rights from the parent site or specify unique access rights with view / edit / administer privileges. An example of the groups used in the solution is in the image below:

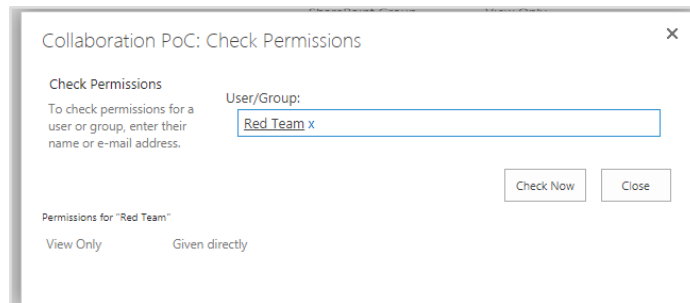


**Fig. 7** List of user security groups in SharePoint used for information access provisioning

Assessing effective user or group access (View / Download / Modify) can be viewed by using a built in feature in SharePoint Online under the security setting for the site / folder / page / item section.







**Fig. 8** SharePoint Security Permission Screen Ribbon. By clicking on “Check Permission”, the user can enter the name of group or individual user and click on “Check Now” to view effective permissions

## 5 Study

The participants were divided into two groups, one simulating a CPA staff member and the other simulating a CPA client subject matter expert (CPA). The scenario used for the testing was an employee classification for R&D tax credit in which both CPA staff members and clients collaborate to complete information. This process is typically done in the context of R&D tax work with client by CPA firms in the US. All participants were CPA company employees. Half of the participants played the role of the client and the other half played the role of CPA firm team members. Participants were asked to complete a survey at the end of the study to provide feedback. In addition, to assess understanding of security and access, the study administrator played the role of the CPA firm’s client staff trying to access non-authorized information using a non-CPA firm Microsoft Office 365 account with a Client SME role (SharePoint Online security group membership).

### Study Tasks

The testing team was divided into two roles

- CPA team – CPA staff that provide a specific R&D Tax Credit Study service to a client
- Client SME team -

Below is a description of the test tasks that the team members were asked to perform during the study.

#### CPA team -

Step 1 - View the list of qualified projects (do not add new project or change project description - This will be done in future phases)

Step 2 - Assign SME to help with employee classification - Use the "Responsible" column

#### Client SME team -

Step 3 - Select each employee from the list and assign relative time to each on the projects on the right part of the screen

#### CPA team -

Step 4 - Ask two questions in the client Questionnaire per instructions below:

- Click on "Client Questionnaire" link and review the list of existing questions and answers
- Post a question on the questionnaire list
- Assign a person to answer from the client
- Ask a sensitive question to client finance team in questionnaire list
- You'll need to ensure that the Client SME Team does not have access to view the question

## 5.1 Survey

Participants in the test were asked to complete a survey – see below and section 6 for questions and results

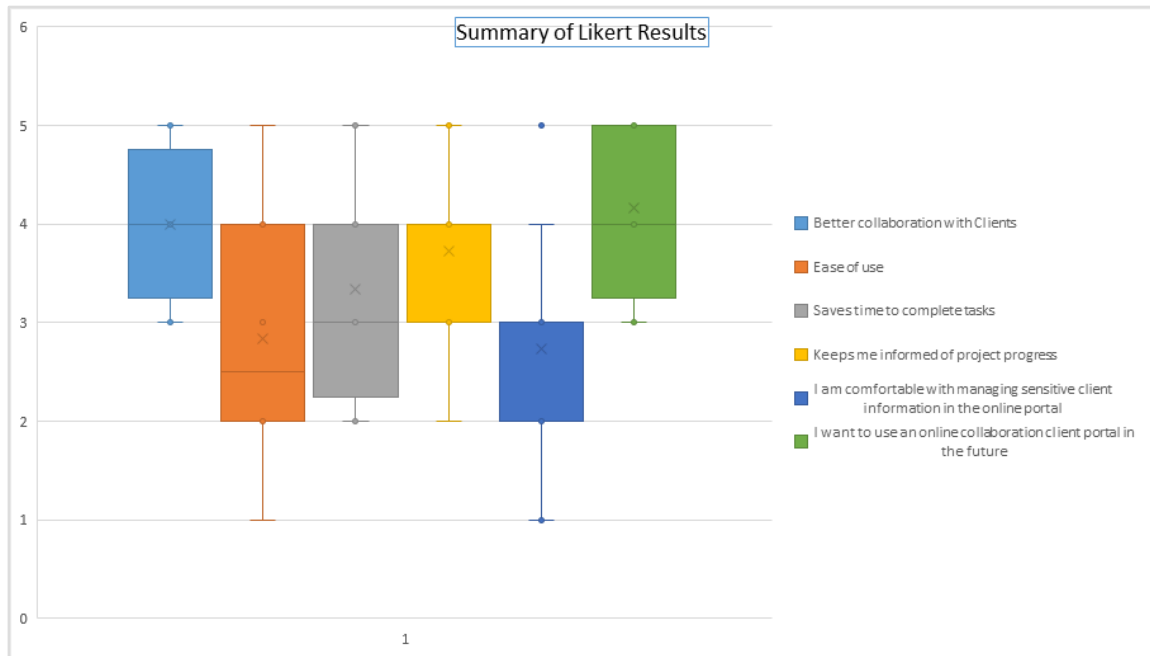
In the survey, the participants were asked to fill out the Likert table below. The results of the Likert were statistically analyzed to assess user experience

8. Online collaboration portal ranking - Please rank from 1 (lowest) to 5 (highest) your experience

	1	2	3	4	5
Better collaboration with Clients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ease of use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Saves time to complete tasks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Keeps me informed of project progress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am comfortable with managing sensitive client information in the online portal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I want to use an online collaboration client portal in the future	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Fig. 9** Likert part of online survey asking participants to rank from 1 to 5 different categories

The results from the survey to the Likert question appear in the summary table below in a box and whisker chart. Note that x in the indicating the median value of responses (1 being the lowest and 5 being highest). The box boundaries represent the 2<sup>nd</sup> and 3<sup>rd</sup> quartiles.



**Fig. 10** Likert results summary using box and whiskers chart

## 5.2 External user access and information security assessment

Members of the CPA team were asked to perform step 4 in the testing script which includes asking a sensitive question to the client finance team in the questionnaire. The expectation from the investigator is that the CPA team member would check access to the sensitive question and its answers and adapt as necessary by changing the permission level to the questions (a SharePoint list item) from the default setting which allows access by all client teams to just the client finance team. There are two aspects to this step in the testing which are of interest from HCI-SEC perspective.

- Would the user be aware that they need to change default permission?
- Would the user be successful in changing the default permission using the software interface?

At the completion of testing, the principal investigator used an external user account simulating client SME role to assess proper access to sensitive questions. There were only two questions posted by the team (out of 12 participants) that simulated sensitive questions. None of the sensitive questions had its default access setting modified.

## 6 Results Analysis and Discussion

The open ended questions were designed to capture feedback from the participants regarding tool usability, relevance to current work practices and client experience. A summary of the main point is below:

*What is your role in the organization?-*

To evaluate whether there were differences in experience between a junior vs. a more experienced user, we collected responses from several roles, including R&D Tax Team Associates, Seniors and Managers. Note that in the R&D team, Associates are the more junior team members and will focus on information collection, while Seniors and Managers will focus more on work quality and supervision responsibilities.

*In your opinion, what are the benefits of using the online collaboration when compared with how you previously collaborated with clients?*

In order to understand how CPA staff perceived future work using SaaS tools when compared with current tools and methodologies. The responses included a view that efficiency and client experience will improve since all information will be available to both client and CPA team in one location, better use of time by client and CPA staff member and shifting more work to the client which will increase utilization of CPA staff members.

One response summarized few points shared by other participants well -

“Using the online collaboration tool will provide our teams with the ability to seamlessly communicate with our clients on a real-time basis. The tool will enable efficient communication channels, real-time updates on engagement status, and the ability to effectively manage client engagements from an external and internal perspective. The tool will provide greater engagement transparency for our clients and provide us with a multitude of options on improving our internal and external processes.”

*Where you successful in completing your task in the online portal?*

This question was designed to gauge how CPA staff perceived their own success in completing all testing activities. The results indicated some challenges and confusion regarding client role access and the information participants were required to provide. Out of 11 responses, two indicated successful completion, four indicated no success and the rest five responses indicated partial success. Comments included:

“Validating access wasn't assigned to me. I didn't see sensitive data, such as wages on the SME facing page.”

“No, in the SME role I could still see all of the questions and answers, not just those assigned to me.”

*Where you able to validate proper access to client files with sensitive information?*

This question examines the perception of the CPA staff regarding their own success in setting up proper client information to sensitive question (the last step in the testing script). Two responses out of 11 indicated successful completion (although when we tested the actual configuration we discovered only partial success in securing access to sensitive survey questions). The rest of the responses indicated none or partial success, which corresponds with our findings of only two question responses two step 4 in the test script.

*In your opinion, will our clients like to use the new online portal?*

As the CPA staff is familiar clients' input, their estimate of clients impression would provide an indication to their trust in the platform. The CPA staff study participants work closely with clients regularly and are familiar with client's behavior. Responses were mixed and indicated that the tool needs to be properly tested and enhance the user experience with configuration and proper training.

Example for a responses which captures key points:

“It will depend on the client. Some clients will love this tool while others will not have the time, patience, or capabilities to effectively use it. When evaluating whether we should use this tool for a client or not, we can always provide options and different processes on a case by case basis. Overall, I see a lot of potential with this, especially in R&D where we could even use Sharepoint as a more "tech savvy client" option or even "the budget friendly" option where there are clients that prefer to be more hands on with their engagements or prefer to work on engagements on their own time.”

“I think it could be useful, given there aren't too many communication channels in use. If there are too many places to check for information/ sending messages, information can be missed. However, it would be nice to have a platform that is less unwieldy than GoFileRoom and more organized than outlook.”

The overall impression from the team to using the online collaboration tool was positive given that the overall median score for the Likert data (median above 3) and narrative of feedback was positive [See Appendix A]. The two main areas that scored unfavorably (median below 3) were the “Ease of use” and “I am comfortable with managing sensitive client information in the online portal”. The narrative comments in Q3 – Q6 supported this view with several participants indicated that they found the information access management confusing. With the exception of the ease of use and information access management, the narrative feedback to tool usability in Q1 – Q6 was mostly positive with main takeaways appear to be around training and configuration.

**Efficiency:** An interesting takeaway we observed is that the vision of using SaaS for collaboration to increase team efficiency was well received and accepted as a strategic direction for the CPA firm by the more senior participants (Manager and senior) while the junior staff member who participated in the study feedback focused more on time saving for their own work while working with their clients. The senior members were more likely to point out where the software did not meet their expectations and the additional work needed to bring the collaboration portal to broad adoption with clients.

**Access rights to information:** This aspect is a main security concern, as it deals with sensitive client information. The default setting of the software allows access by all the different client teams. Users can change this setting to allow access just to the client finance team. To test participants understanding of this setting, participants were asked to enter sensitive questions that they client than needed to respond to. Users of the software are expected to change this setting if sensitive information is being asked from the clients. users were asked whether they were able to validate proper access to information (Q5) with few respondents indicating that they believed that the access right to the sensitive questions scenario in step 4 of the testing was successful while in fact sensitive questions in the client questionnaire were not properly configured for access as confirmed by the authors. The gap between user perception and actual access management is concerning and demonstrate the need for additional user training and / or simplified UI design for access management in SharePoint.

## **7. *Summary and Future Work***

Finally, the significance of this study captures the experience of a mid size CPA firm (with about 500 employees) trying to challenge the client collaboration status quo software by leveraging emerging SaaS collaboration capabilities in the hope for improving client experience and in parallel improve their own staff team efficiency and experience. The collaboration challenges CPA staff members face are unique to their industry who is very specialized and require a high level of trust to deliver services. Future work will focus on finding the right balance between SaaS configuration, user training and client experience setup in order to enable the CPA firm to achieve the efficiency and client experience it desires.

## References

1. Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., & Chen, F. (2017, July). A qualitative investigation of bank employee experiences of information security and phishing. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association (pp. 115-129).
2. <https://customers.microsoft.com/en-us/story/plante-moran-professional-services-office-365>
3. <https://big4careerlab.com/big-4-accounting-firms/>
4. <https://www.smartvault.com/resource/setting-up-shop-in-the-cloud/>
5. <https://products.office.com/en-us/business/office-365-trust-center-security>
6. [https://gsuite.google.com/security/?secure-by-design\\_activeEl=data-centers](https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers)
7. <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>
8. <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurity-resources-for-organizations-and-cpa-firms.html>
9. <https://docs.microsoft.com/en-us/office365/securitycompliance/data-encryption-in-odb-and-spo>
10. <https://docs.microsoft.com/en-us/sharepoint/external-sharing-overview>
11. Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. International Journal of human-computer studies, 63(1-2), 25-50.
12. E. M. Trauth, Qualitative Research in IS: Issues and Trends. IGI Global, 2001.

## Appendix A - Table of Terms

**Table 1: table of terms**

SaaS	Software as a Service
FileShare	Secured File Sharing software by Citrix <a href="https://www.sharefile.com/filesshare">https://www.sharefile.com/filesshare</a>
MimeCast	Secured email software <a href="https://www.mimecast.com/">https://www.mimecast.com/</a>
Office 365	SaaS collaboration platform by Microsoft <a href="https://www.office.com">https://www.office.com</a>
CPA	Chartered Public Accounting
HCI-SEC	Human / Computer Interaction - Security

## Appendix B – Training materials

### 6.1.1 Testing Preparation Instructions:

Thank you for helping our firm assess the functionality of the new collaboration portal for R&D projects. We would like you to perform a few activities in our portal to help our team deliver better client experience and collaboration for R&D Tax credit work.

Note - As a part of the assessment, you will be asked to provide feedback on both functionality and information access. You can see a step by step instructions at this link. To view access for any item (Task, question or document) select the item by clicking on it's row and then click on "Share" and then in the popup window click on the three little dots next to the close screen X button and then on "Manage Access" --> Advanced. In this access management window, Click on a button called "Check Access" and then enter the person's name you want to check access for. In

this screen you will be able to assign / remove access by first "Stop Inheriting" access and then remove / add access as needed. For questions please contact Lior Baron

And now for the actual testing activities:

You are asked to complete a series of activities that will be similar to how the R&D team interacts with some clients. You will be asked to play one of these roles:

CPA Firm team member

Client Finance Team

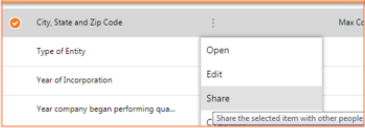
Client SME team.

The testing will be made of steps 1 - 4


### 6.1.2 Training Slide - User access management in SharePoint

## MODIFY ITEM ACCESS IN SHAREPOINT

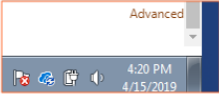
1 – Select item and open Additional Action Menu




2 – Select "Manage Access"



3 – Scroll down and select "Advanced"



4 – Check Permission or to change permission click on "Stop Inheriting"



4 – Remove / Change / Add permission as needed

