SI 487 Senior Capstone
UX Final Report

UM ITS: Public Cloud Team

Somya Bhagwagar
Lucky Chowdhury
Liz Fu
Matt Wolfgram

April 24th, 2020

TABLE OF CONTENTS

PROJECT OVERVIEW

ITS offers its users services which provide provisioned access to cloud vendors such as Amazon Web Services, Google Cloud Platform (GCP), and Microsoft Azure to various campus units. ITS implements a shared responsibility model for cloud service use, meaning that they provide some security features, but customers also have a responsibility to provide security on their end. This project entails creating a tool to display the shared responsibility model based on how a customer consumes a cloud service. The tool will help users parse security requirements and understand their role in protecting their cloud environment. Our customer is anybody who has access to ITS public cloud offerings, meaning that they have filled out the access form and have been approved by ITS to use services of cloud vendors.

PROJECT GOALS

Our overall project goal is to create a product that improves the way that UM employees understand and secure cloud services by making security information more engaging, visual, and accessible.

We broke down the overall goal into actionable milestone goals aligned with our research goals:

1. **Understand the Target User**

   A big problem we faced in understanding our target user was the various groups of users and their respective use cases. Everyone on campus has a different reason to use the cloud, putting them at varying levels of risk; each group also has different technical literacy levels. Our client was not able to provide us with a general description of the audience because each user varied greatly. The scope of this project includes all users who have access to the different cloud vendors. This only occurs if the user has a need for access to ITS Public Cloud platforms and makes a service request. We conducted surveys to understand what types of people used cloud storage, their roles on campus, their fields of study, and their technical literacy level. We interviewed users to better understand how they use the platforms and conceptualize their responsibility for sensitive data. When creating our solution, we catered our tool towards the ‘lowest denominator’ of technical literacy so that our information was accessible to all with access.

2. **Work with UM ITS to rewrite content fitting a spectrum of technical literacy levels, types of data, and levels of access.**

   Since the effectiveness of our tool is predicated on intuitive information architecture, it was crucial that we ensured the content conveyed critical dimensions of cloud security properly. We first needed to understand information security protocols to create technically-oriented resources to convey protocols to

the user. We worked with ITS and the Cloud team to ensure that information was best suited for the technical literacy levels and accessibility requirements of the target user base. This will also target all of the users on a broader level.

3. **Decide on an ideal information architecture for our final product**

   We hoped to reach a point where we decide on a form that will present our information most effectively — this could have taken the form of an infographic, a more interactive tool, or a combination of both. Since our tool will likely be situated online, we had to decide where to place it in relation to preexisting ITS cloud resources. Another factor that we need to keep in mind is accessibility. If our tool is composed in part by an infographic, it may be difficult for those reliant on screen readers to parse this form of visualization. It's important that we factor in the needs of these users within the infographic or web tool we end up producing for this project.

RESEARCH PHASE

RESEARCH QUESTIONS

Optimizing the experience design of our product required clearly understanding our user through their motivations, attitudes, and experiences regarding cloud security. We formulated three broad research questions that we wanted to explore in our research methods during this phase. Firstly, we asked:

How can we influence users to take on the shared responsibility model and be aware of how to operate safely in cloud computing spaces?

Our intention here is to find out how we can best motivate users to care about security protocols.

Next, we came up with a question that addresses accessibility of information. This is because a major problem current users were facing was the lack of an efficient, convenient method to learn more about their shared cloud responsibilities. We asked:
How can end-user cloud security responsibilities be intuitively conveyed and made accessible to UM employees to protect their data stored on these platforms?
Our intention here was to discover the most viable technique to explain security protocols.

Finally, we created a question regarding the practicality and usage of our tool. We want to avoid mimicking resources that do not add value to the user's experience so we asked ourselves:
Which stage(s) of the consumer journey would be most effective to design our tool around, and where should it be situated in relation to existing resources?

Our intention here is to learn where our tool would best fit amongst existing ITS resources in terms of location on the SafeComputing site.

METHODS

We carried out our UX research through four methods: developing personas, consulting with a subject matter expert, and conducting interviews and surveys. A great portion of our research was dedicated towards understanding our user and the technical jargon utilized on the SafeComputing site. Our objective here was to get to the root of clarifying responsibilities of cloud users by navigating the existing perceptions of information security.

Surveys

The purpose of sending out a Qualtrics survey to the ITS email listservs provided by our client was:

1) To discover any existing biases cloud users may carry
2) To gauge the general demographics of users
3) To learn preferences about security responsibilities
4) To gain feedback on relevant experiences with cloud computing platforms.

We conducted **44 surveys** using the Qualtrics survey platform and analyzed a variety of data provided by our respondents. Please refer to appendix point 1 for the survey materials we used.

Interviews

The purpose of conducting user interviews with ITS stakeholders during this research phase was:

1) To gain a deeper understanding of a typical user's interactions and prior experiences when using a cloud platform
2) To find out what their main pain points are, including their general attitude/sentiments towards current resources available on the public cloud
3) To learn how they would like to see their security responsibilities conveyed to them.

We successfully conducted **six interviews** during this phase. This method allowed us to become more informed on all three of the research questions we mentioned above, primarily because we had the freedom to ask interviewees open-ended questions about their motivations and current level of understanding pertaining to information security. Please refer to appendix points 2 and 3 for the interview materials we used.

Subject Matter Expert

In UX, a subject matter expert (SME) is one who carries extensive knowledge regarding a particular topic which includes a user base. For the sake of our project, we were looking to consult with an SME that could provide us insights about how ITS handles cloud security, and which resources are most sought after for understanding shared responsibility. We spoke with **one SME** who had expertise in the measures taken to prevent security breaches and respond to cloud security needs of users on campus, along with a background in incident response at ITS. Since proper information architecture and design are critical elements of cloud security, the SME helped us

translate our findings into elements for our developing tool. These elements build on the searchability, accessibility, and approachability of the sensitive data guide, which is the primary tool we analyzed before starting our design iterations. With our findings we have been able to iterate on our interactive search function, categorization, and visualization of security responsibility.

Personas

The purpose of creating personas was to apply our findings from surveys, interviews, and the SME to form a cohesive idea of what our tool needs to achieve. It also narrowed the scope of our final tool more effectively while remaining inclusive of more levels of access and technical literacies. The process of understanding our user was difficult since our client did not have access to the users of the cloud. Through insightful discussions with our client, our own research, and testing out the links ourselves, we learned that the user (customer) for our tool is anybody on campus who has access to the ITS Public Cloud. This means that they have filled out the access form and been approved by ITS to use services of cloud vendors.This could be anyone ranging from faculty to staff to students. Next, we had to better understand our user, their purpose for the cloud, and their technical literacy levels. We developed **two personas** that represent our customers:

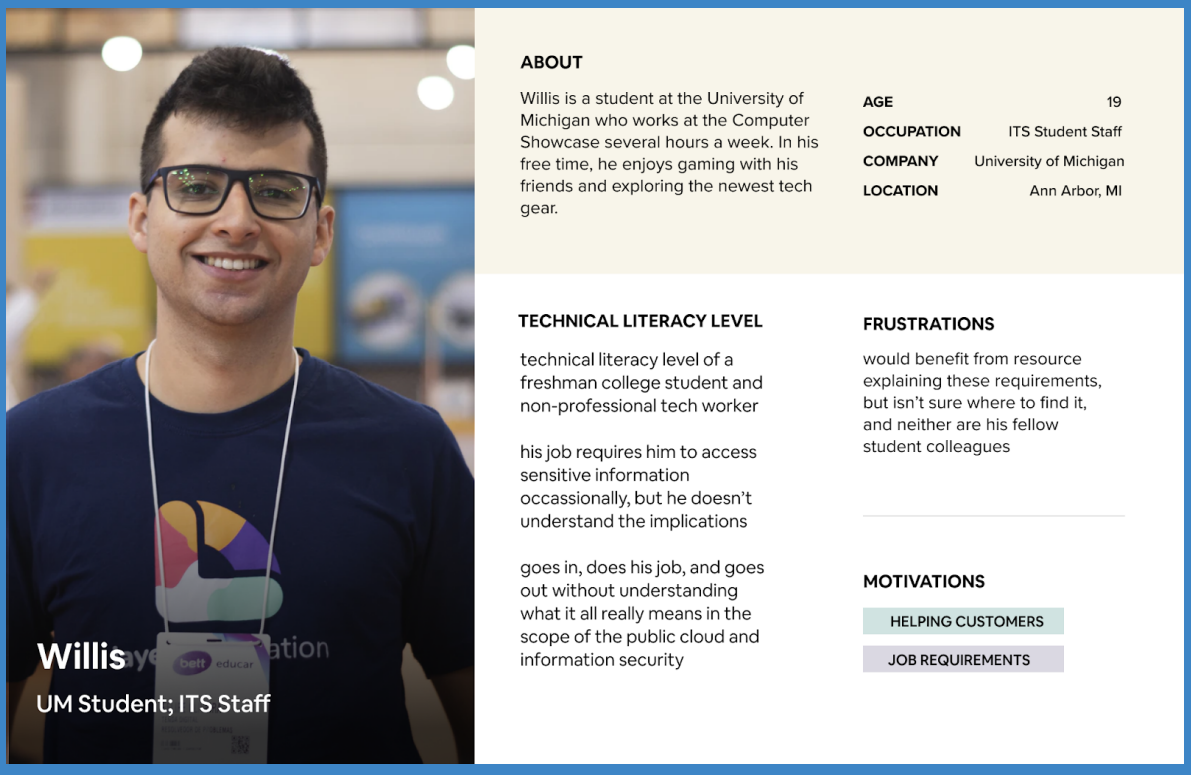


Figure 1: Persona of student

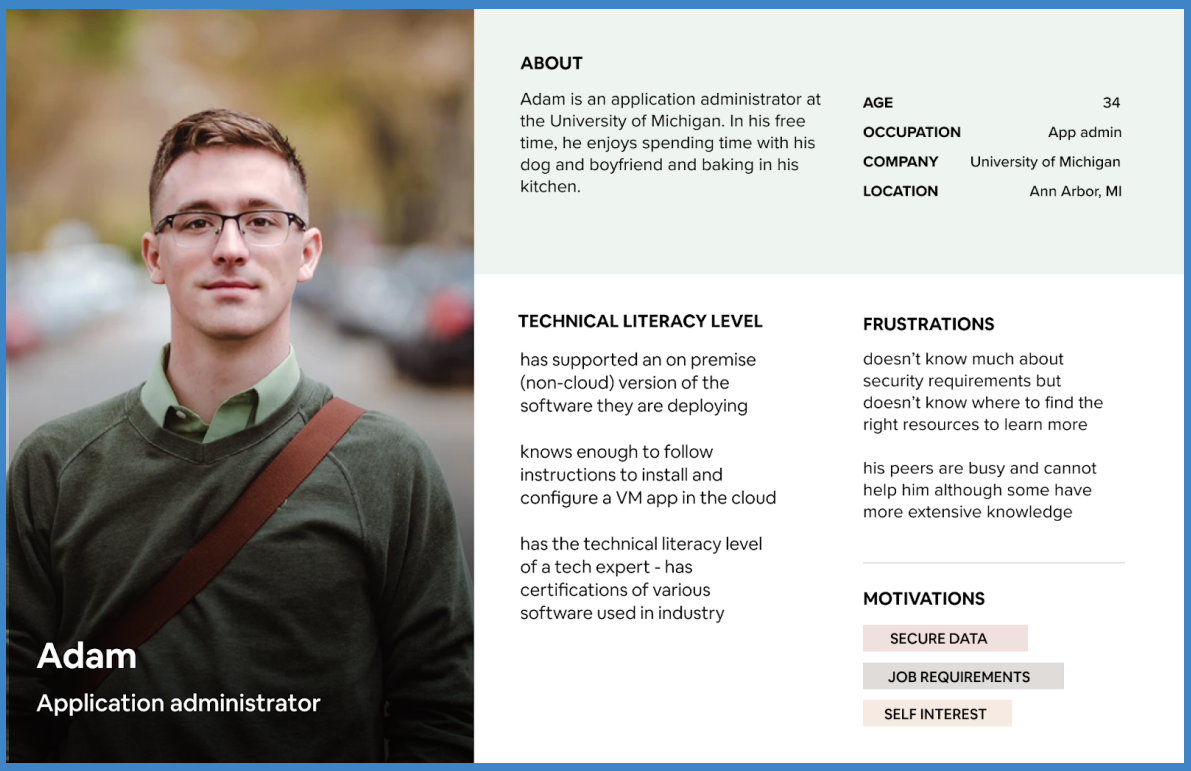


Figure 2: Persona of application administrator

User Journey

Using the two personas above, we created user journey maps. As of now, there are two primary ways to get to the ITS Cloud Service Portal. The first is through the SafeComputing page on the ITS website, and the second is to go through the IA Security Education and Awareness site. The latter website is the workflow preferred by our client.

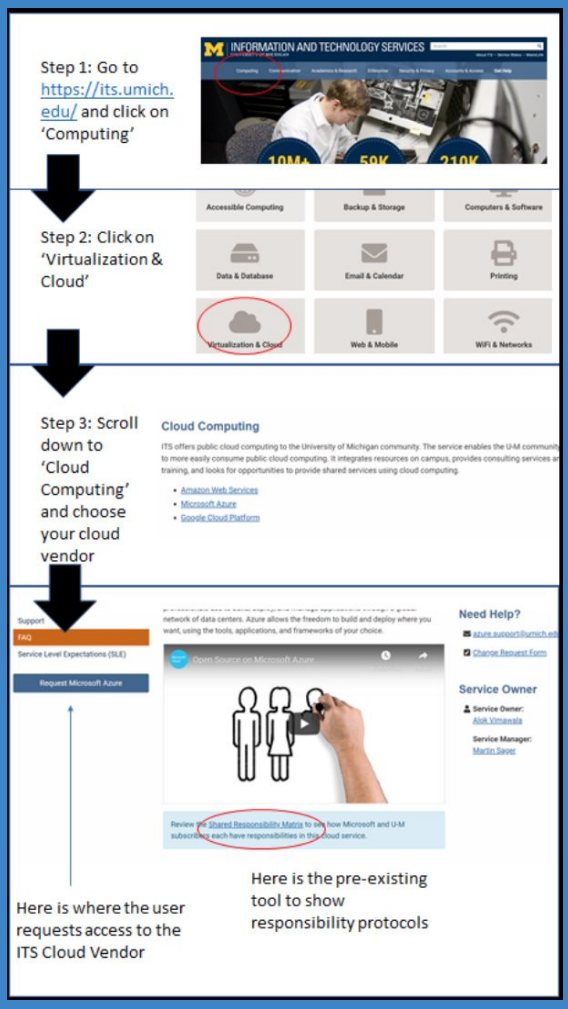


Figure 3: In order to get access to the ITS Cloud Service Portal, Willis might go through the IA Security Education and Awareness Site having needed to do some research before choosing to use a cloud vendor

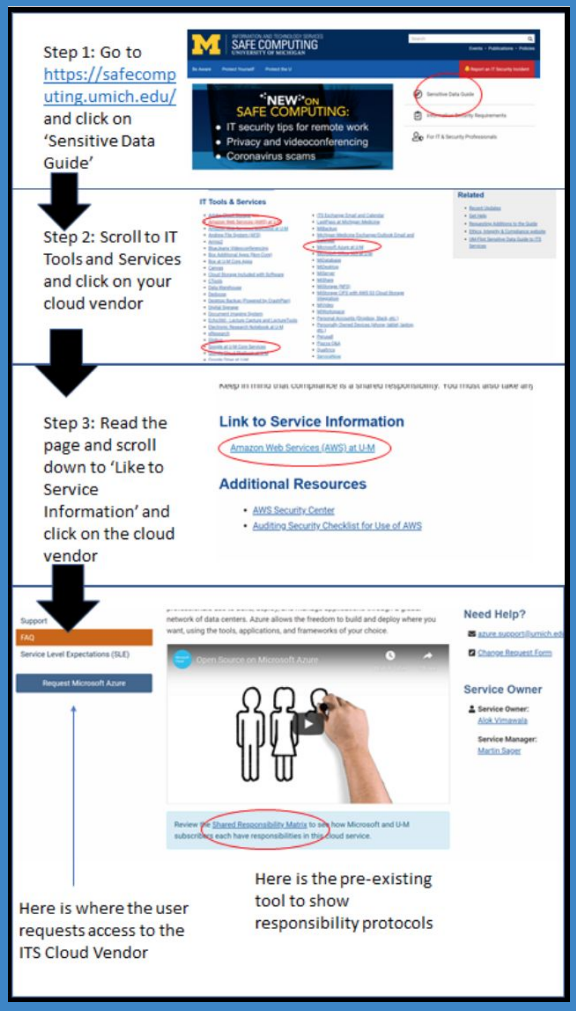


Figure 4: In order to get access to the ITS Cloud Service Portal, Adam might go through the SafeComputing website since he is already familiarized the ITS SafeComputing site, having used it in the past

In order to request access to a cloud vendor, after following the above journey, the user will be brought to this link — This link is only accessible to faculty and staff. They will have to fill out a form when requesting AWS, GCP, or Azure Cloud Services. The form is screenshotted below.

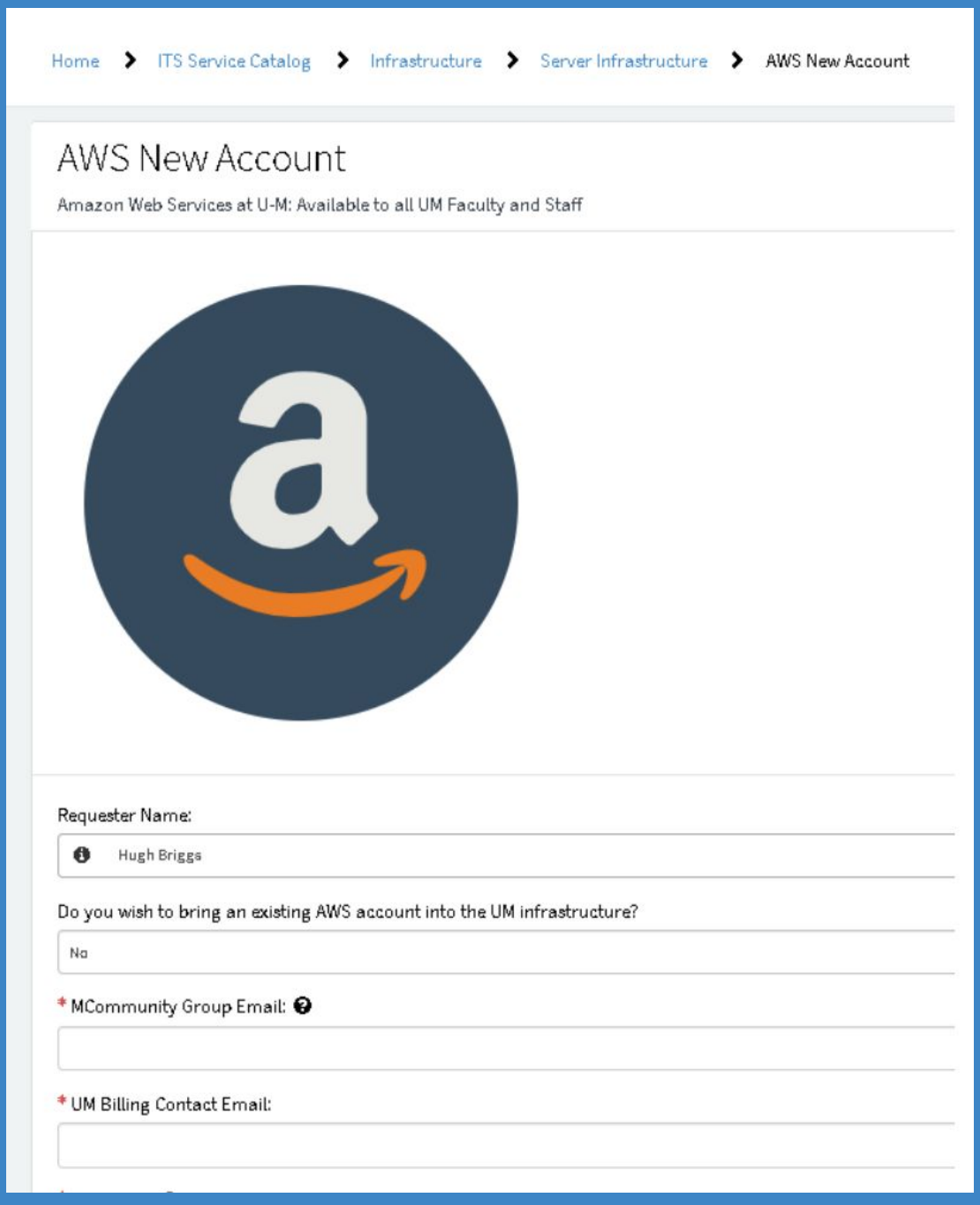


Figure 5

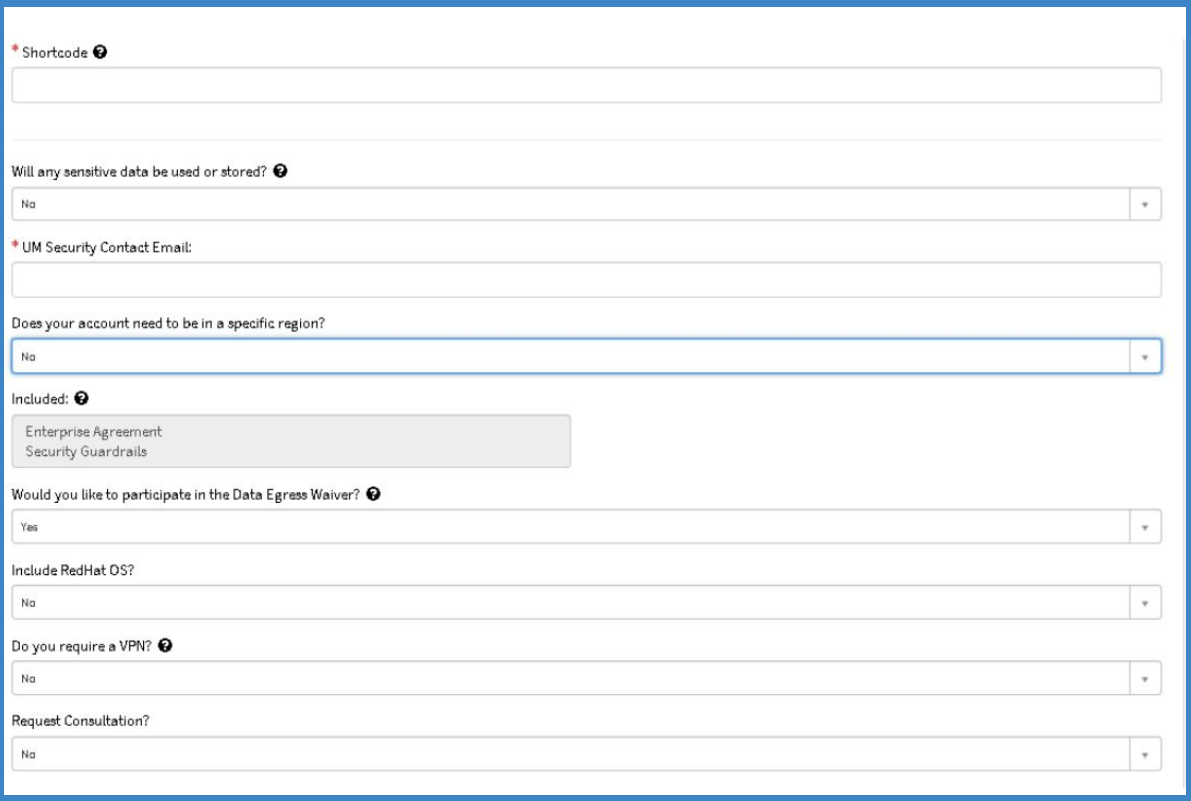


Figure 6

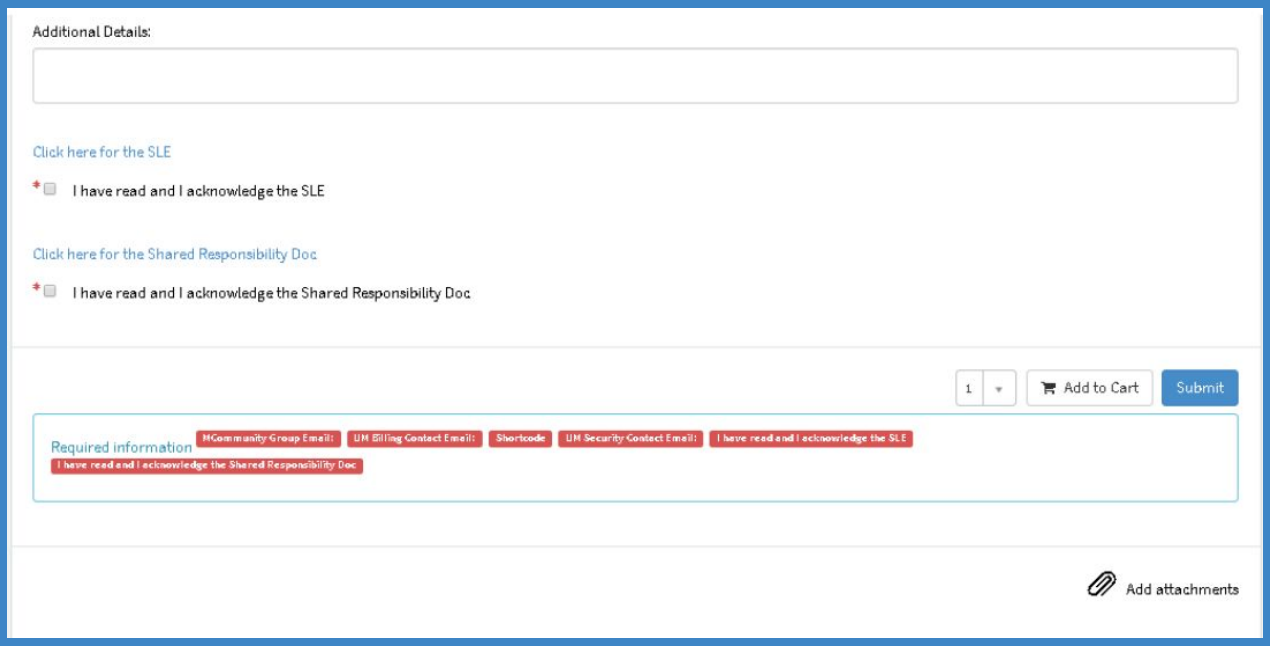


Figure 7

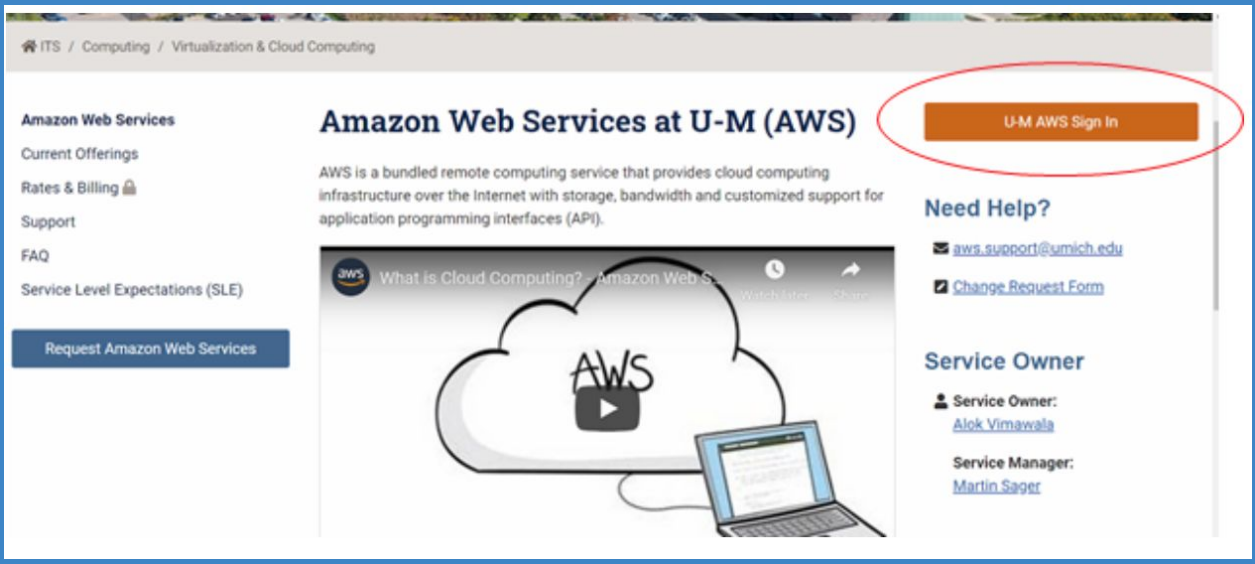


Figure 8

We would like the tool to be placed in an accessible location in the same spot where users can access their account. This would be within the login link where they frequently sign into their account. The top of the last page of the consumer journey (expanded in Figure 8) in the user journey is where a user would login to their cloud vendor account. We advise that our client put our tool right under the sign in on the top right hand side.

INSIGHTS

After conducting research through the above mentioned methods, we found seven key insights; three insights from our survey responses and four from our interviews.

Through our Qualtrics survey questions, we discovered:

1) **Most customers use Amazon Web Services.**
   Of the three platforms (Amazon, Google Cloud Platform, and Microsoft Azure) there is a large population of users already subscribed to AWS as their primary cloud vendor. This indicates that our focus for distinguishing user responsibility should be slightly higher for this platform compared to the other two.
2) **Most customers are IT Staff or Students.**
   This highlights the different levels of technical literacy between our customers.
3) **Most users believe that they are not handling sensitive data.**
   There appears to be a lack of motivation in users to care about security protocols because they do not believe the data they are handling is sensitive enough or even sensitive at all.

Through our in-person interviews, we found:

1) **Most people do not have an alternative form of storage.**
   Even if users wanted to keep their data secure, they must use the storage method provided by their vendor due to a lack of other options. Some users succumb to

the idea that there is not a need to go through a security protocol (sometimes understood as a 'terms and services' contract).

2) **UM ITS' presence provides a feeling of an extra security layer.**
   Many people feel that their data is stored more securely under the UM ITS Cloud vendors than if they were alone as an individual with the AWS account.
3) **Cost is a big issue when it comes to choosing vendors and IT Tools.**
   When choosing a service, most users decide based on the function and the price. After making their purchase decisions, users do not read through the shared responsibility guidelines. This might be due to the fact that people have to look through costs and uses before the responsibility aspect.
4) **Some users feel unprepared when they are given access to a cloud environment.**
   Our interviews primarily covered people who are administrators with high technical literacy, but there are also users who have no idea what cloud vendor they utilize or what it is meant to accomplish. They are simply given access from an administrator and told to complete a task. They usually learn how to complete the task by 'messing around with the system' until they learn how to accomplish it.
5) **We learned about the CLAP guidelines, an acronym for a model that will be further explained throughout this paper.**

REQUIREMENTS

Our research also helped us accumulate six main UX requirements to focus on so that we can design our tool in the most efficient and accessible format.

1) **Knowing what the platform expects; knowing your (user's) responsibility in relation to this**
   This was the primary requirement of the project as it allows users to be more secure when using cloud vendors. Our tool needed a clear divide between the user and the platform's responsibilities so that there is minimal confusion about security expectations.
2) **Way to prove if documents are sensitive**
   According to our SME, many users are unsure if their documents are sensitive or not. Providing a method on our tool to clarify this increases motivation in users to care about their information security, and also raises awareness of various types of data.
3) **When should someone report?**
   It is imperative to include some sort of guidelines as to when a user should report and who to report to exactly. This allows ITS to be more cognizant about their users' needs, especially in the case of a security breach..
4) **Less information overload**
   Currently, there is much information overload during account setup for a cloud platform, and too much technical jargon on the sensitive data guide which allows users to only look at a certain subset of options. Finding a way to streamline this information overload facilitates users' choice regarding the right platform.
5) **Are there other options for campus users than their chosen cloud vendor?**

It is important to help users understand that they are not limited to one specific platform and its guidelines. Each user has different storage needs when they are using a platform so they should be aware of all of their options in case they need to make a transition to another cloud vendor.

6) **CLAP Guidelines**
We discovered the CLAP guidelines during our research phase as an essential requirement; CLAP is an acronym that stands for Configuration Management, Logging, Access Control, and Patching. It is a model that helps users understand privacy and security protocols during account setup for a cloud platform. The chart below breaks down how each category influences a user's journey. This will further be discussed throughout the report.

Requirement	Description
Configuration Management	Users need to establish secure accounts, passwords, login information, and instances of cloud services
Logging	Groups or departments using cloud services must understand, review, and update collective understanding of their individual role in using these services and accessing them securely
Access Control	Users need to be able to grant and revoke access to colleagues on campus in a way that is safe, quick, repeatable, and efficient
Patching	Users must be able to detect a threat in the event of a breach or suspicious activity in the cloud services they employ. They must also understand virus protection, system monitoring, and patching of security holes in their respective cloud instances.

DESIGN PHASE

After creating our requirements, our team brainstormed and created a variety of ideas. Our first idea was to change the Sensitive Data Guide as a whole. According to our research, this would be the most efficient solution as well as solve some peripheral problems found in the research such as users not knowing alternatives to cloud vendors. With users not knowing alternatives, they often click through the shared responsibility, privacy agreements, or protocol without reading through since they feel they have no other choice. Therefore, we felt that having the shared responsibility tool on the Sensitive Data Guide allows users to see options and also see the shared responsibility model at the same time they make their choice of cloud vendor. Through the Sensitive Data Guide, users could see all options and compare tools to make the best choice for their circumstance.

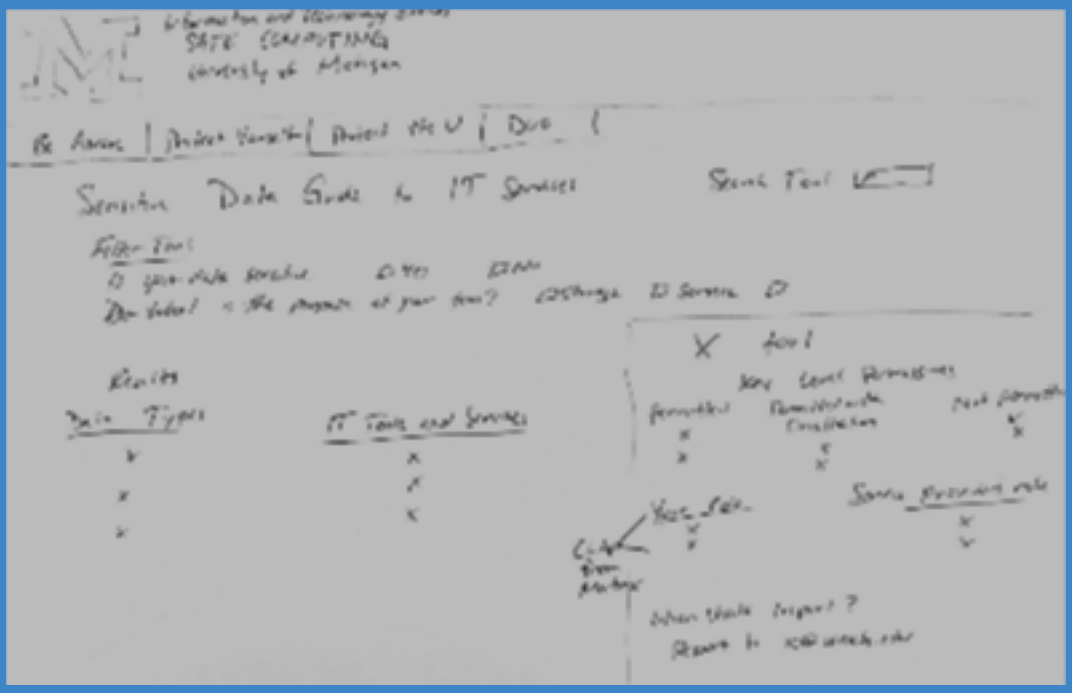


Figure 9

Our first model had:

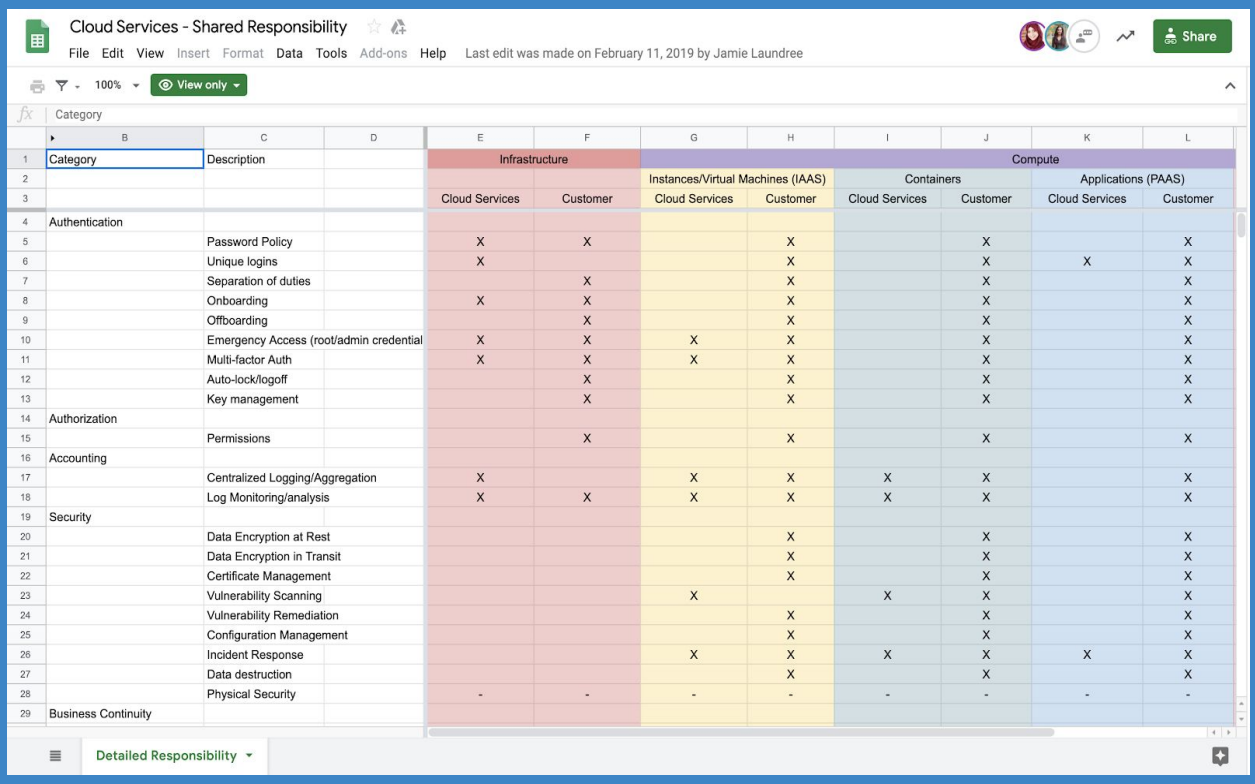
1) Search bar- decreases information overload
2) Filter items- allows users to see alternatives and decreases information overload
3) Services tool- allows users to see their responsibilities and permissions
4) The interactive checklist allows users to become aware that their information is sensitive
5) Clap guidelines will be shown in the services tool to organize information
6) Allows users to understand when and what they should report

After showing this concept to our client, they agreed that it would be a potential solution. This is partially due to it being out of their scope to change the Sensitive Data Guide, and due to the fact that not all users visit the Sensitive Data Guide when applying for cloud vendor access. We narrowed down the scope of our project to focus on the Shared Responsibility Matrix and re-create the tool in a way that met our primary requirement — distinguishing users' cloud vendor security responsibilities in contrast to the vendors' responsibilities — as well as tie in some of our secondary requirements.

EQUATIONS

Extracting information from the matrix was a key process that involved organizing various variables listed on the matrix such as the category, description, IAAS;PAAS;SAAS service models, and the requirements of indicating responsibility. We found an "equation of success" that sorted the information in the Shared Responsibility Matrix:

CLAP + IAAS;PAAS;SAAS + PHI;SSN;HIPAA +
Customer/Server+Category+Description + Responsibilities



Cloud Services - Shared Responsibility

File Edit View Insert Format Data Tools Add-ons Help Last edit was made on February 11, 2019 by Jamie Laundree

Share

100% View only

Category

	B	C	D	E	F	G	H	I	J	K	L
1	Category	Description		Infrastructure		Compute					
2						Instances/Virtual Machines (IAAS)		Containers		Applications (PAAS)	
3				Cloud Services	Customer	Cloud Services	Customer	Cloud Services	Customer	Cloud Services	Customer
4	Authentication										
5		Password Policy		X	X		X		X		X
6		Unique logins		X			X		X	X	X
7		Separation of duties			X		X		X		X
8		Onboarding		X	X		X		X		X
9		Offboarding			X		X		X		X
10		Emergency Access (root/admin credential		X	X	X	X		X		X
11		Multi-factor Auth		X	X	X	X		X		X
12		Auto-lock/logoff			X		X		X		X
13		Key management			X		X		X		X
14	Authorization										
15		Permissions			X		X		X		X
16	Accounting										
17		Centralized Logging/Aggregation		X		X	X	X	X		X
18		Log Monitoring/analysis		X	X	X	X	X	X		X
19	Security										
20		Data Encryption at Rest					X		X		X
21		Data Encryption in Transit					X		X		X
22		Certificate Management					X		X		X
23		Vulnerability Scanning				X		X	X		X
24		Vulnerability Remediation					X		X		X
25		Configuration Management					X		X		X
26		Incident Response				X	X	X	X	X	X
27		Data destruction					X		X		X
28		Physical Security		-	-	-	-	-	-	-	-
29	Business Continuity										

Detailed Responsibility

Figure 10

This complex equation involved categorizing by CLAP control family, IAAS/PAAS/SAAS delivery, the cloud services/customer responsibility, the category, the description, as well as incorporating all the requirements we formulated from this research. We needed to narrow down the scope. With our clients' help, we were able to filter the most relevant variables — the CLAP framework and Category Descriptions — with focus on the distinction of responsibilities in the Instance/Virtual Machine IAAS variable. Thus, our new equation became:

CLAP + IAAS + Category + Description + Responsibilities

INFORMATION ARCHITECTURE

We have brought up the CLAP framework in several sections throughout this paper, introducing it as a model and a variable through which we needed to sort responsibilities. We spent a lot of time understanding the CLAP model and how it can encapsulate all of the protocols necessary for users to follow; and organize these protocols in the buckets of configuration management, access control, logging, and patching. In order for us to properly use CLAP as an architectural framework, we spent a lot of time understanding each bucket and how it fits into the holistic necessities of information security.

We individually began to card-sort the categories in the matrix into the CLAP framework. Our iterative design process included card sorting because we felt it was the most efficient method to categorize the responsibilities from the matrix into the buckets and understand how each component could be interpreted by users.

Figure 11

Figure 12

Figure 13

LOW FI PROTOTYPE UX DESIGN

Our next progression of the design was a **Lo-Fi Prototype** which looked like this:

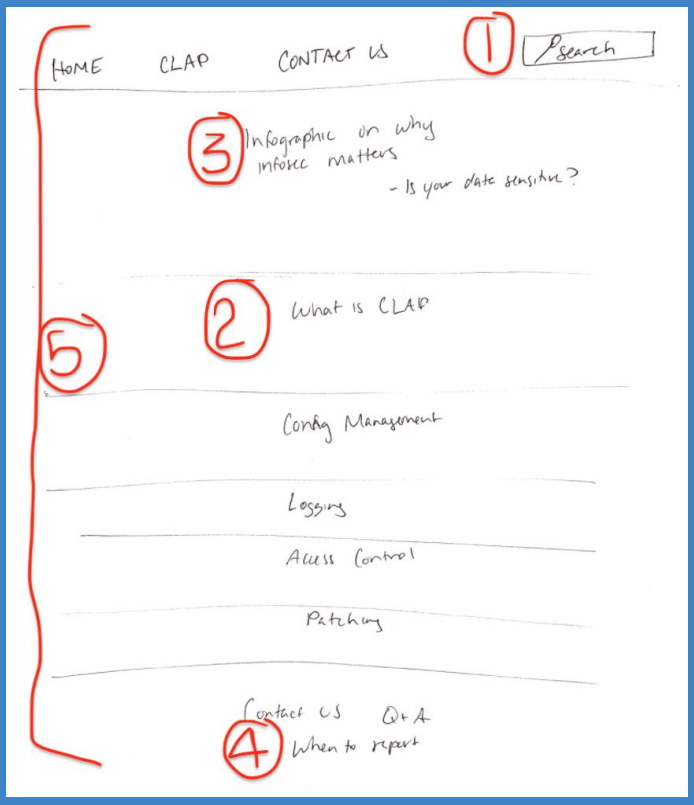


Figure 14

It contains:

1) A search bar that decreases information overload and helps users find security elements
2) Expanding slides allowing users to see their responsibility vs. the cloud vendor's based on CLAP guidelines
3) Section to prove if documents are sensitive
4) A "when to report?" section
5) Less information overload

Our clients agreed that this new design will work better towards their goals. After combining our card sorting of the categories into the CLAP framework with their information security knowledge, we agreed upon the following architecture for the content of our new design:

Configuration Management:

- Documentation, policies, procedures
    - Data flow map
    - Architecture diagram
    - Asset inventory
    - Asset dependency documentation
    - Asset prioritization
    - Determine resource dependencies
    - Process review and improvement
    - Security baseline
    - Risk tolerance
    - Admin/User training
- Business continuity:
    - Backup
    - Disaster Avoidance/Disaster Recovery
    - Resilient Architecture
    - Disaster Recovery Testing
- Networking:
    - IP addressing
    - Routing
    - DNS
    - Firewall
    - VPN
    - Network Segmentation/Separation

Logging:

- Accounting
    - Centralized Logging/Aggregation
    - Log Monitoring/analysis

Access Control:

- Least Control
- Separation of Duties
- Authorization

        - Permissions
    - Authentication
        - Password Policy
        - Unique logins
        - Separation of duties
        - Onboarding
        - Offboarding
        - Emergency Access (root/admin credentials)
        - Multi-factor Auto
        - Auto-lock/logoff
        - Key management

Patching:

- Maintenance
    - Patching
    - Upgrades
    - Testing
- Security
    - Data Encryption at Rest
    - Data encryption in Transit
    - Certificant Management
    - Vulnerability Scanning
    - Vulnerability Remediation
    - Configuration Management
    - Incident Response
    - Data Destruction
    - Physical Security

After reviewing these sections with our group's technical literacy levels, we decided to add sentences for each of the CLAP sections to define them. Though our goal was just to create a tool that could differentiate responsibilities, we wanted our tool to play a bigger role in improving information security in the public cloud. Therefore, we wanted to make sure they were accessible so users can comprehend them as well as be motivated to take action. The process of decreasing the jargon and creating clear definitions and calls to action within each definition took many iterations until we were satisfied. The first iteration is the top bullet, the final iteration is the second bullet per category:

Configuration Management- Creating and maintaining security settings when setting up resources

- Ensure you have a hardened profile and only enable necessary services.
- Enable the minimum services needed to operate

Logging- Collecting, maintaining, and reviewing records of activity

- Ensure you have enabled appropriate levels of logging.
- Ensure you have enabled appropriate levels of logging at each individual layer in your resource

Access Control- Limit access to authorized users

- Ensure you have an account life cycle process.

- Ensure you have an account life cycle process

Patching- Keeping service secure by keeping it up-to-date

- Ensure your systems are being patched
- Regularly update your software to mitigate security vulnerabilities

MID-FI PROTOTYPE UX DESIGN

During our second iteration of this prototype, we thought that the infographic would be placed at the top of this page. It's purpose is to persuade users to read and follow the shared responsibility protocol. Through research, we found that the leading reason why people do not read/follow the protocol is because: they do not feel that their data is sensitive and are thus unmotivated to read through. This infographic addresses the third concern; and our CLAP breakdown will address the first concern.

Figure 15: First Version of Infographic

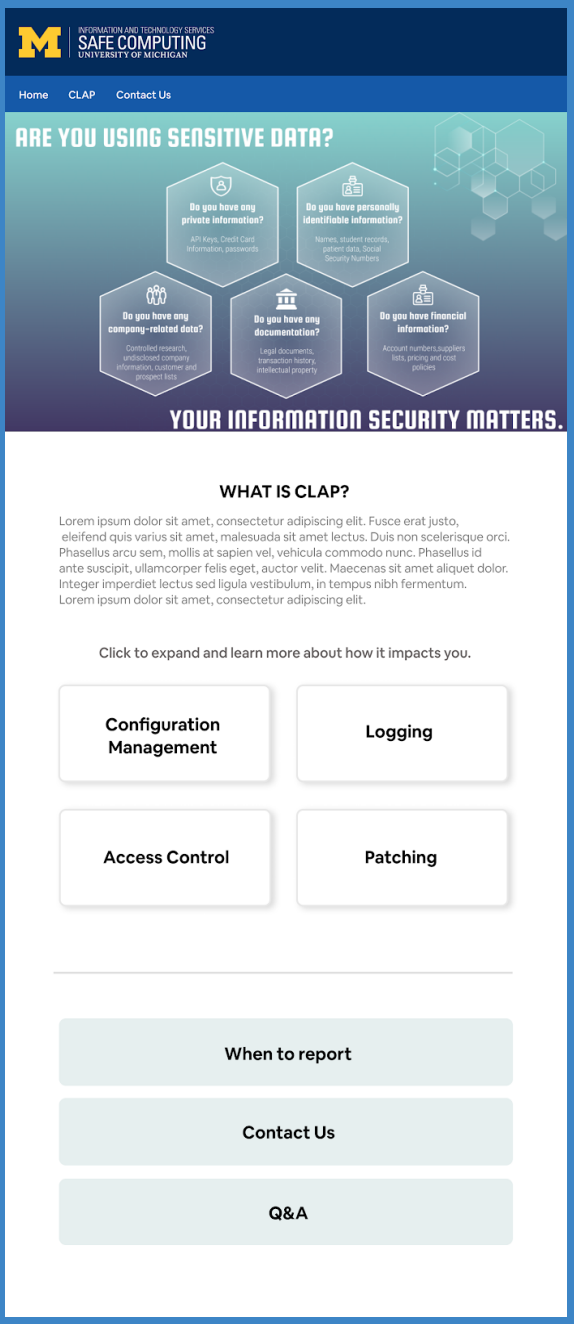


Figure 16: First Version of Tool

Putting the infographic near the control families helps users find relevant security guidance for aspects of logging. Initially conveying the impact of cloud security visually may make it easier to parse C.L.A.P guidelines. We intend for this juxtaposition to provide a more fluid and accessible path through key resources than the previous spreadsheet. According to the feedback and user testing we did with our client, having a visible section for Q&A along with contact information makes users more likely to reach out or submit a ticket to ITS.

After further user testing, we found that we could make the infographic more accessible with better contrast:

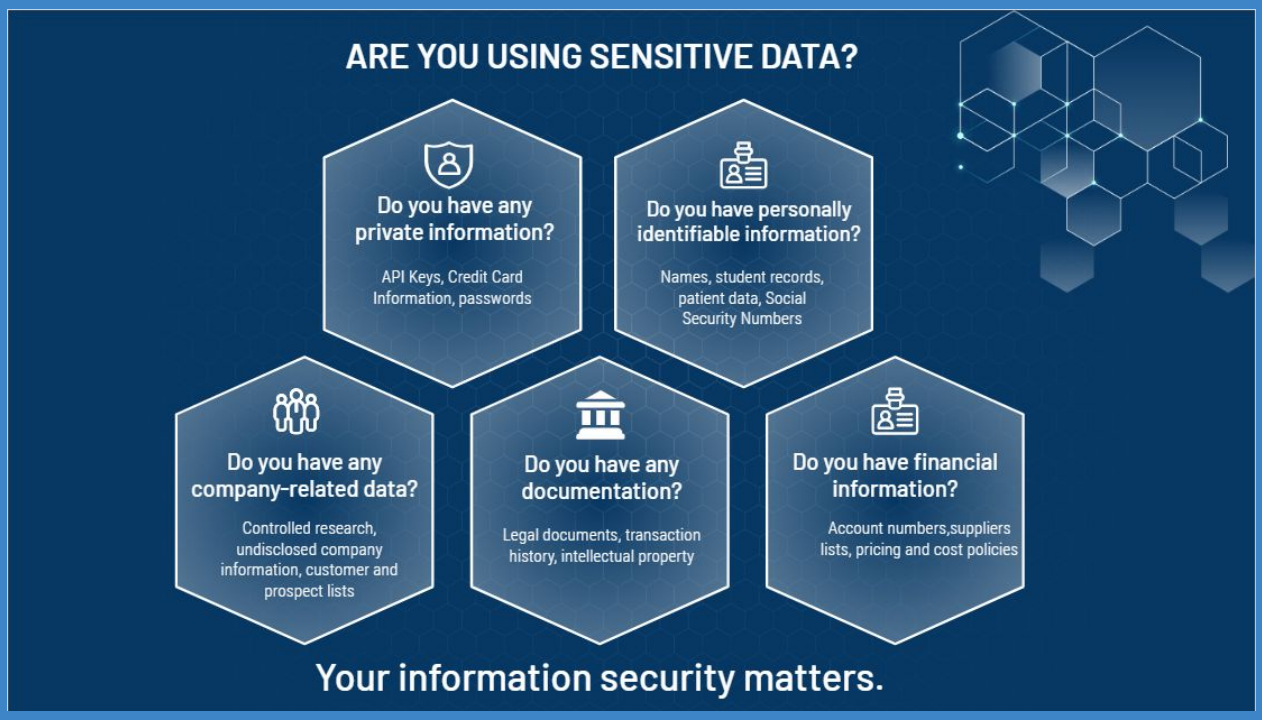


Figure 17: Second Version of Infographic

Along with the expandable feature to clearly convey which security responsibilities fall under which party, we made the tool more aesthetically pleasing and interesting to the user. We chose to put the infographic at the bottom in contrast to the iteration before. We did not want the infographic to act as a filtering mechanism and prevent users who read it and still felt they did not have sensitive data from reading through the rest of the protocols. By putting it at the bottom, every user is encouraged to read through the tool; once they realize they do have sensitive data, they might re-read it again. Below are screenshots that reflect these changes.

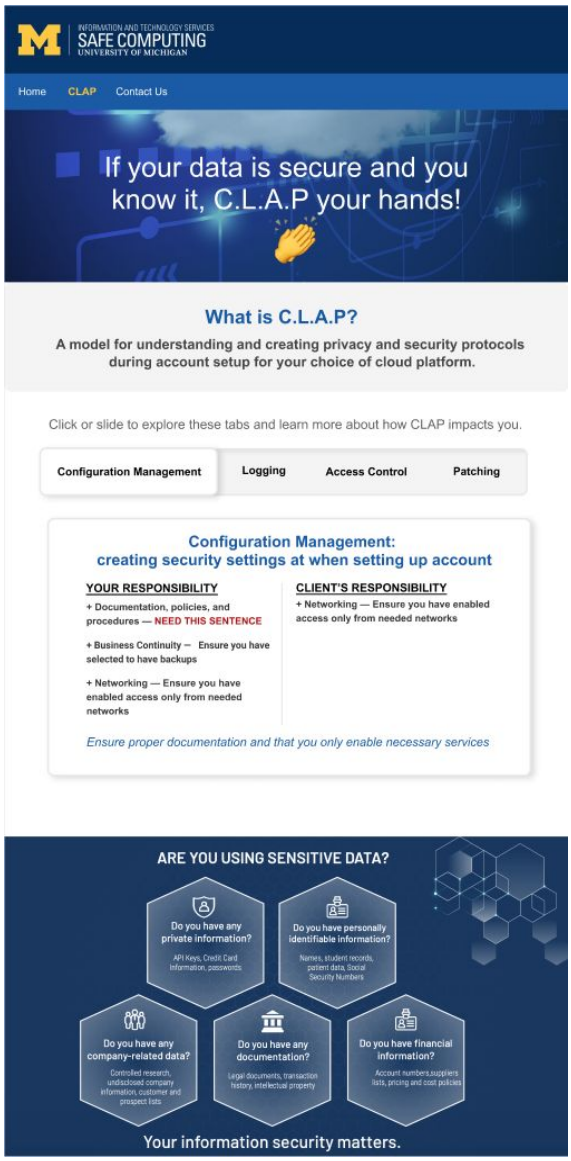


Figure 18: Configuration Management Screen

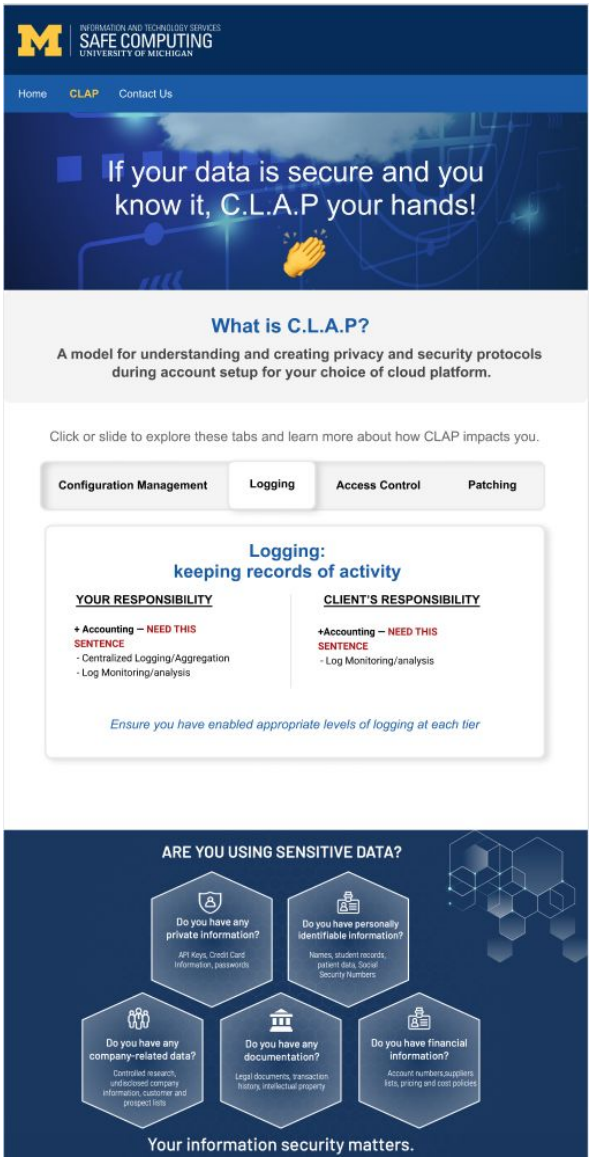


Figure 19: Logging Screen

VALIDATION PHASE

METHODOLOGY & RECRUITING

Since there was no previous version of this tool in existence, we are testing with our users to see if what we created is effective. We focused on four of our UX requirements:

1) **Knowing what the platform expects; knowing your responsibility in relation to this**
2) **CLAP Guidelines**
3) **Less information overload/jargon**
4) **Way to prove if documents are sensitive.**

We aligned these requirements to our user testing tasks to answer our research questions. We conducted five thorough user tests using both A/B testing and task testing for each user. In designing the testing protocol, we sought to answer the following questions:

- *Does the created tool enable users to understand and intuitively explore their security responsibilities and situate them in contrast to the cloud vendor's responsibilities?*
- *Can this understanding be achieved quickly with the ability for users to take action or be directed to resources to clarify in the event of confusion?*

In doing this, we hoped to gauge how our tool engages users in effortful processing of their responsibility and role in securing the cloud. We wanted users to feel motivated and able to devote time and energy into conceptualizing shared responsibility for themselves. To qualitatively measure the effectiveness of our tool, we looked for users' attitudes towards the tool and their perceived usability, their preference in visuals, and their comprehension of the contained information. Quantitatively, we recorded the time taken to complete tasks and find requested information during our interviews — outcomes were documented as either successes or errors.

We used A/B testing for the two versions of our visuals and its placement in our tool. The first version of our infographic had a different layout and presented information numerically. The second version uses different colors, visuals, aesthetics, and a link to convey the same information. We wanted to understand from our sample of users which version best met the 'less information overload' requirement.

The second test was a single system test asking users to place themselves in a scenario and accomplish a few tasks. They were asked to locate certain responsibilities ("who is responsible for backing up files?), retrieve information about the control families ("what is configuration management?") and determine if they had sensitive data in the scenario. Through these tasks, we looked to gain a deeper understanding of the effectiveness of wording and presentation of the CLAP model in our tool. Since we struggled to understand the CLAP model for information security, top priorities included preventing

that tension for users as they read guidelines and discern client and user responsibilities in context. It was imperative during validation that we received feedback on the phrasing used in our tool so that it was accessible to all technical literacy levels. The validation test questions can be found in appendix point 4.

The same five participants completed both types of tests. Participants saw variants in the A/B test when two design versions of infographics were presented to them along with a questionnaire for preferences. Participants saw only one updated version of our tool's prototype on Figma when we did task testing; they were given the freedom to search for and find information however they wanted.

INSIGHTS

1) **Users intuitively think that the definition of the CLAP framework category is the call to action and get confused**
   We would need to have some sort of indication that this sentence is a definition. This could be in the form of an = sign, a - sign, or even writing out 'definition:' so that users do not mistake this for the call to action.
2) **We still have a wide range of technical literacy that we need to account for in the last stretch. Users still struggle with Task 2 of finding whose responsibility it is to backup files.**
   A search bar would help users who are less technically literate and may not know under which category their question would be in, even if they understand all the categories. It would also help users save time, and encourage users to double check before jumping to conclusions.
   Also, having more hyperlinks with definitions and calls to action are needed.
3) **Our updated infographic is more aesthetically pleasing but harder to read**
   We need to increase the font size on the infographic and give the users the ability to download the image to use for repeated reference. This would make it more accessible as a whole.
4) **Users would not re-open the tool for future reference**
   Increasing interaction within the tool would allow users to remember content better, personalize it, and make it seem less like another terms and services agreement. Adding checkboxes might help with this by allowing the user to choose what content is relevant and applicable to them so that, in the future, they can look back on what they checked and make sure they're following the guidelines they chose for themselves.
   Also, we need to put the tool in a more accessible location so that users are constantly reminded that it exists and are encouraged to keep checking and opening it. We could also extend this further and encourage users to print a copy of everything they checkmarked to hang by their desk. However, this would be more something we encourage our client to do during the implementation of this tool.

UX SPECIFICATIONS

During the validation study, one of our insights was that users generally did not feel the need to return to the tool regularly. Though the information is broken down much more, it seemed similar to a Terms and Services document. If this is a tool that users look at before setting up their accounts and using cloud platforms, they also may not know what to look for. As we found in our interviews, they skim through with the intention of going back and re-reading when it would make more sense and be applicable to their service. To prevent this from happening, we would like to offer our client's advice on the implementation of this tool such as making the sensitive data infographic downloadable. We have also added an interactive feature of checkboxes by each category under the CLAP guidelines. This allows each user to think for themselves and determine which content is personally relevant. We would suggest that the clients implement a way for the users to be able to print off a list of what they checked, and keep a copy on their desk or in files that are accessible so that they have a personalized copy which they can keep referring to. Below are our interaction user flows and detailed page specifications.

User Flow Diagram

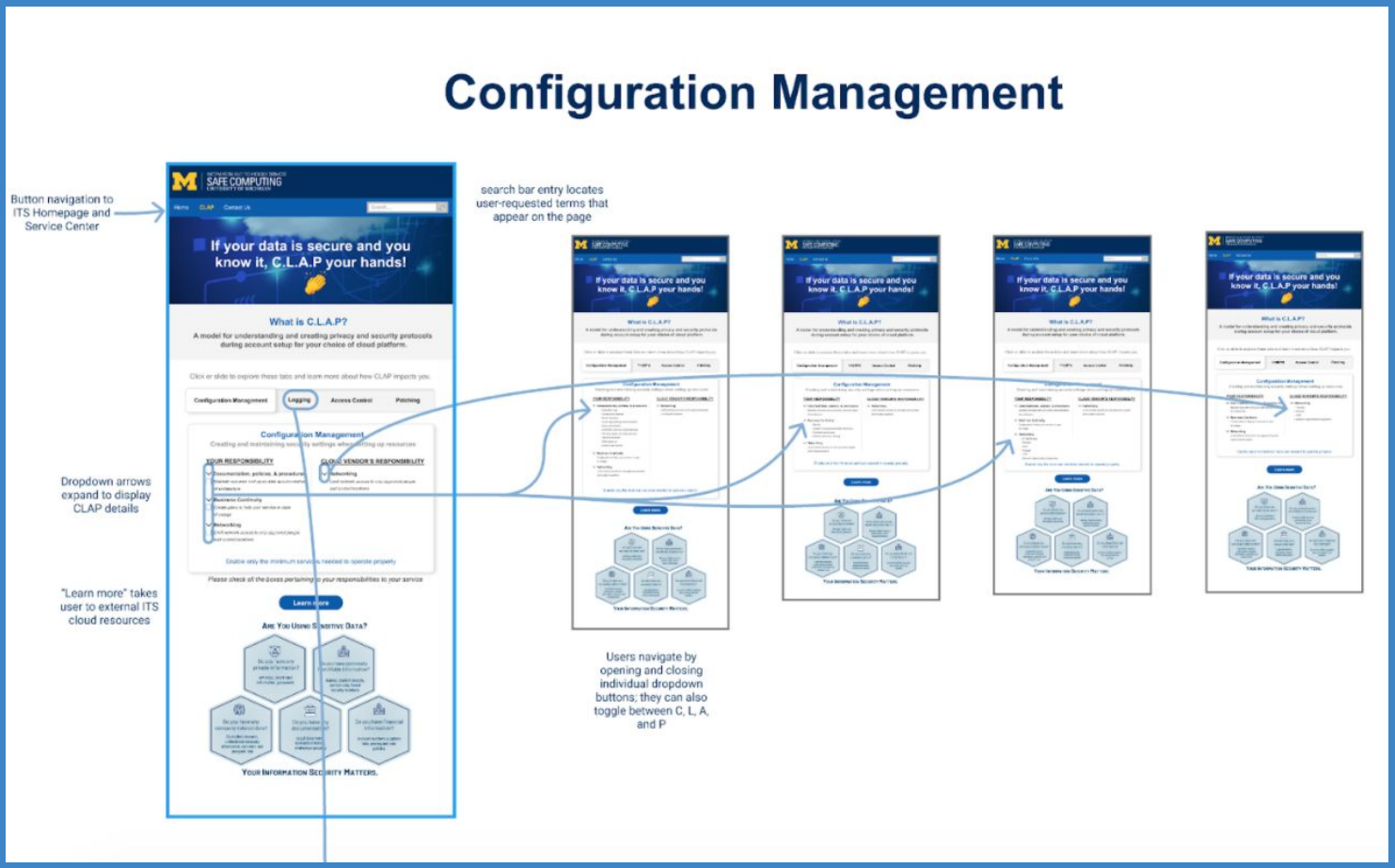


Figure 20

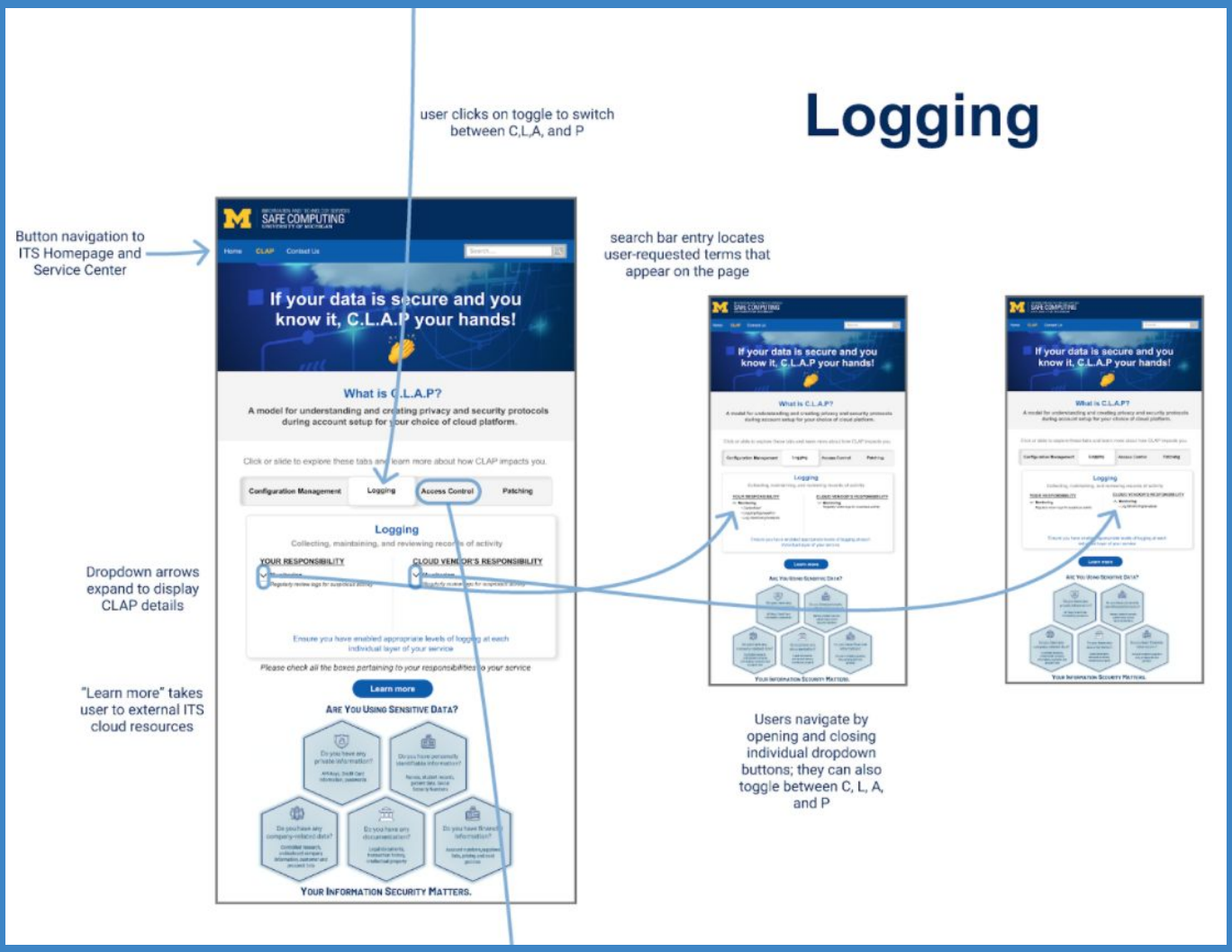

Logging
user clicks on toggle to switch between C,L,A, and P
Button navigation to ITS Homepage and Service Center
search bar entry locates user-requested terms that appear on the page
Dropdown arrows expand to display CLAP details
"Learn more" takes user to external ITS cloud resources
If your data is secure and you know it, C.L.A.P your hands!
What is C.L.A.P?
A model for understanding and creating privacy and security protocols during account setup for your choice of cloud platform.
Configuration Management
Logging
Access Control
Patching
Collecting, maintaining, and reviewing records of activity
YOUR RESPONSIBILITY
CLOUD VENDOR'S RESPONSIBILITY
Learn more
ARE YOU USING SENSITIVE DATA?
YOUR INFORMATION SECURITY MATTERS.
Users navigate by opening and closing individual dropdown buttons; they can also toggle between C, L, A, and P

Figure 21

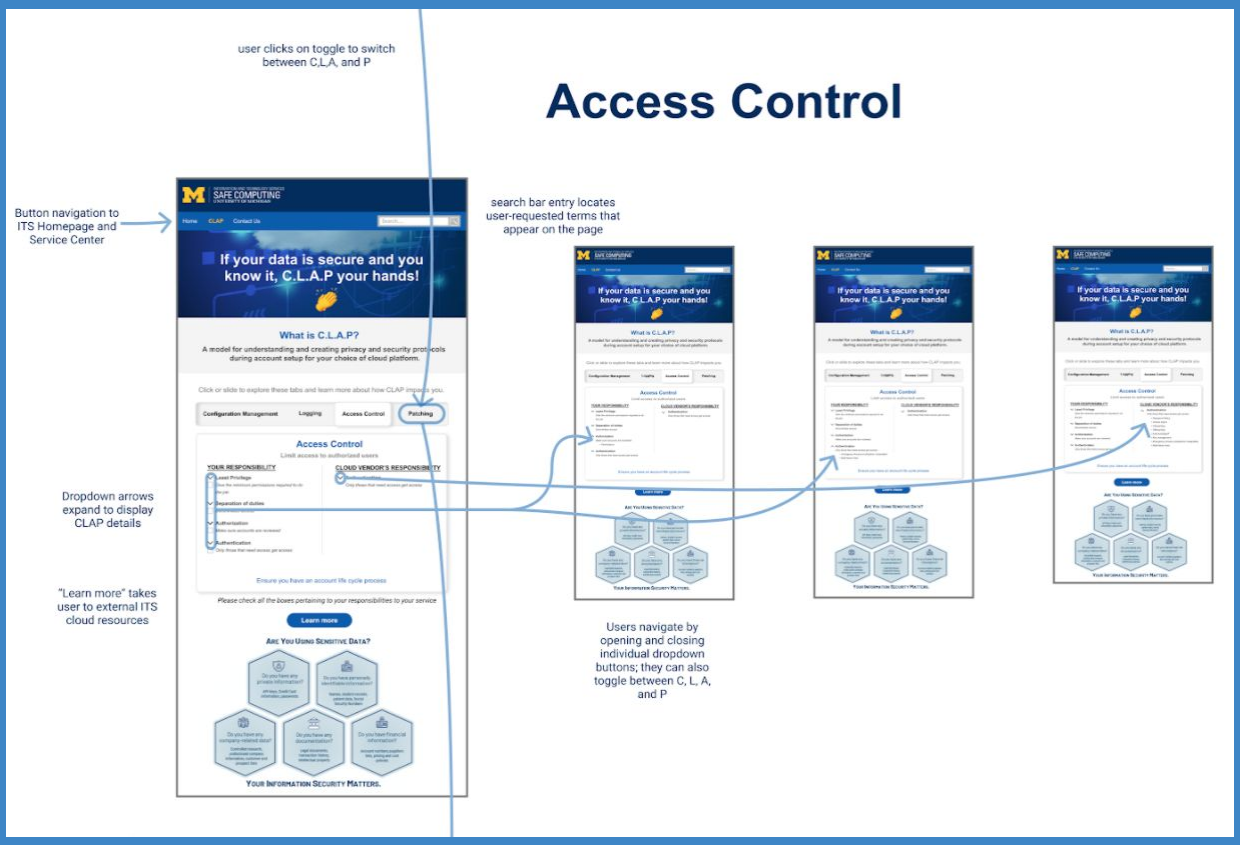


Figure 22

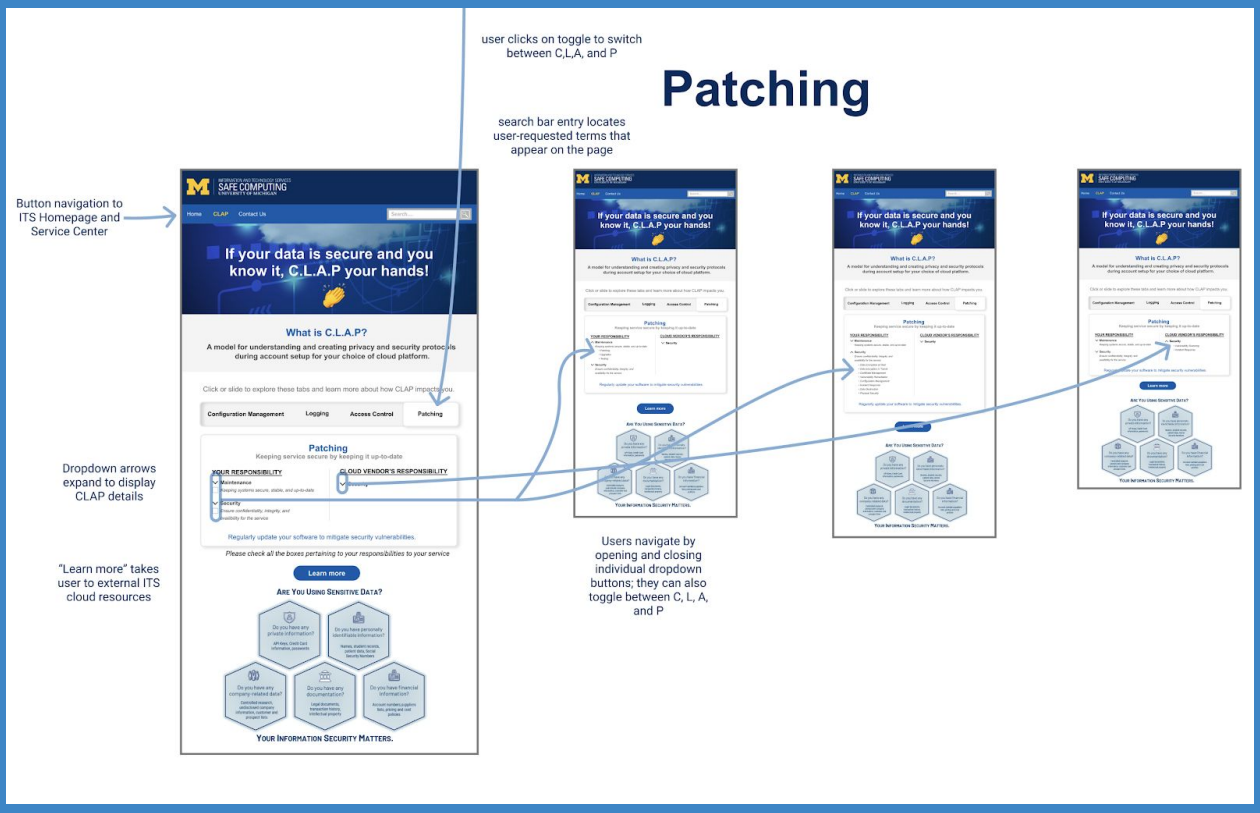


Figure 23

Detailed Page Specifications

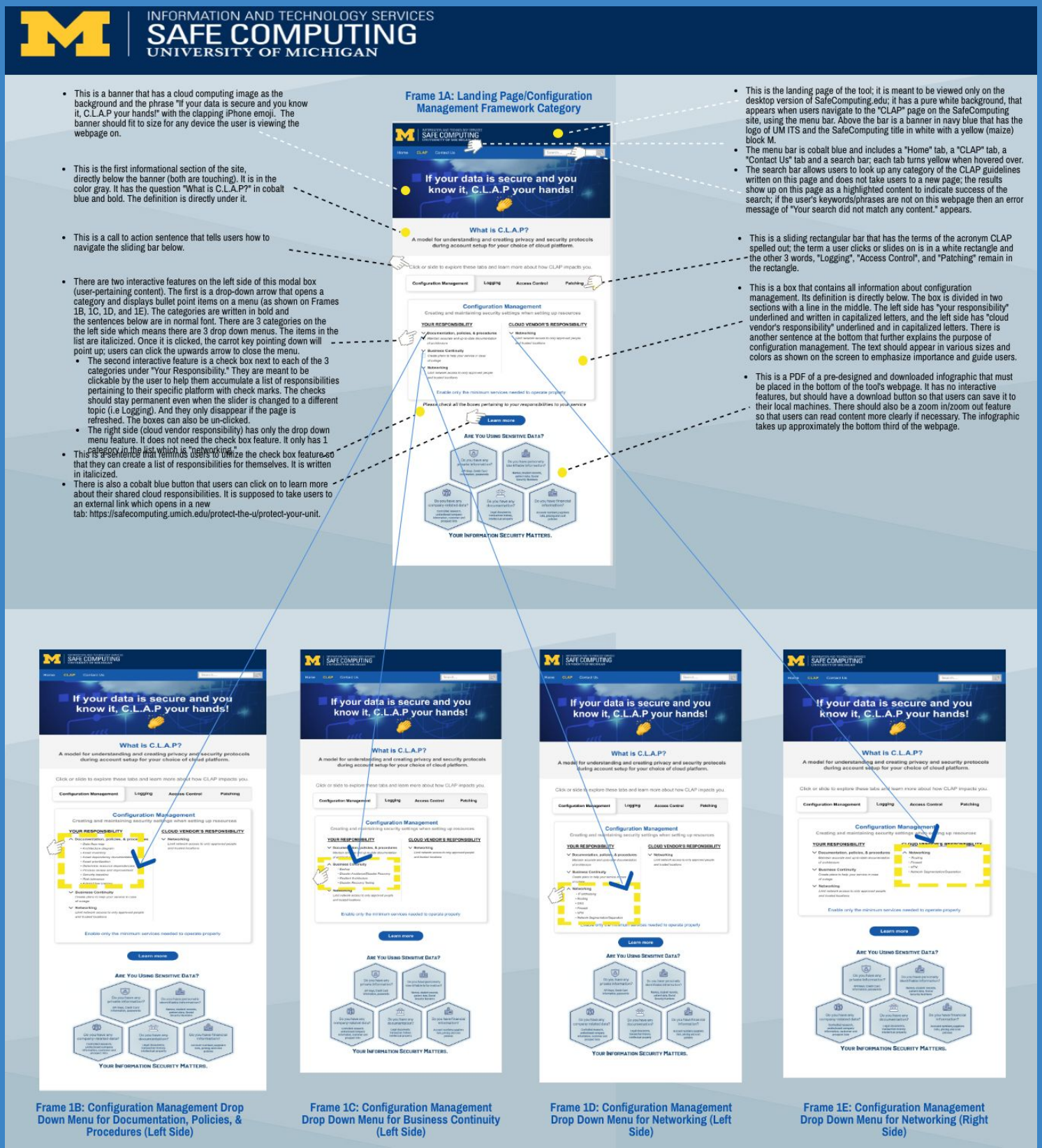
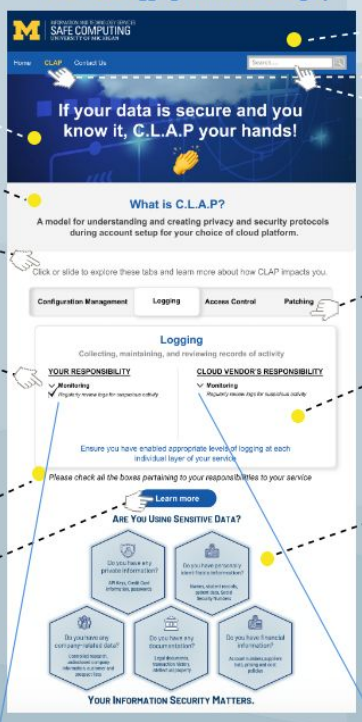


Figure 24: Configuration Management screens

- This is a banner that has a cloud computing image as the background and the phrase "If your data is secure and you know it, C.L.A.P your hands!" with the clapping iPhone emoji. The banner should fit to size for any device the user is viewing the webpage on.
- This is the first informational section of the site, directly below the banner (both are touching). It is in the color gray. It has the question "What is C.L.A.P?" in cobalt blue and bold. The definition is directly under it.
- This is a call to action sentence that tells users how to navigate the sliding bar below.
- There are two interactive features on the left side of this modal box (user-pertaining content). The first is a drop-down arrow that opens a category and displays bullet point items on a menu (as shown on Frames 2B and 2C). The categories are written in bold and the sentences below are in normal font. There is 1 category on the left side which means there is 1 drop down menu. The items in the list are italicized. Once it is clicked, the carrot key pointing down will point up; users can click the upwards arrow to close the menu.
  - The second interactive feature is a check box next to the category under "Your Responsibility." It is meant to be clickable by the user to help them accumulate a list of responsibilities pertaining to their specific platform with check marks. The check should stay permanent even when the slider is changed to a different topic (i.e Access Control). And they only disappear if the page is refreshed. The boxes can also be un-clicked.
  - The right side (cloud vendor responsibility) has only the drop down menu feature. It does not need the check box feature. It only has 1 category in the list which is "monitoring."
- This is a sentence that reminds users to utilize the check box feature so that they can create a list of responsibilities for themselves. It is written in italicized.
- There is also a cobalt blue button that users can click on to learn more about their shared cloud responsibilities. It is supposed to take users to an external link which opens in a new tab: https://safecomputing.umich.edu/protect-the-u/protect-your-unit.

Frame 2A: Logging Framework Category



- This is the landing page of the tool; it is meant to be viewed only on the desktop version of SafeComputing.edu; it has a pure white background, that appears when users navigate to the "CLAP" page on the SafeComputing site, using the menu bar. Above the bar is a banner in navy blue that has the logo of UM ITS and the SafeComputing title in white with a yellow (maize) block M.
- The menu bar is cobalt blue and includes a "Home" tab, a "CLAP" tab, a "Contact Us" tab and a search bar; each tab turns yellow when hovered over.
- The search bar allows users to look up any category of the CLAP guidelines written on this page and does not take users to a new page; the results show up on this page as a highlighted content to indicate success of the search; if the user's keywords/phrases are not on this webpage then an error message of "Your search did not match any content." appears.
- This is a sliding rectangular bar that has the terms of the acronym CLAP spelled out; the term a user clicks or slides on is in a white rectangle and the other 3 words, "Logging", "Access Control", and "Patching" remain in the rectangle.
- This is a box that contains all information about configuration management. Its definition is directly below. The box is divided in two sections with a line in the middle. The left side has "your responsibility" underlined and written in capitalized letters, and the left side has "cloud vendor's responsibility" underlined and in capitalized letters. There is another sentence at the bottom that further explains the purpose of configuration management. The text should appear in various sizes and colors as shown on the screen to emphasize importance and guide users.
- This is a PDF of a pre-designed and downloaded infographic that must be placed in the bottom of the tool's webpage. It has no interactive features, but should have a download button so that users can save it to their local machines. There should also be a zoom in/zoom out feature so that users can read content more clearly if necessary. The infographic takes up approximately the bottom third of the webpage.

Frame 2B: Logging Drop Down Menu for Monitoring (Left Side)

Frame 2C: Logging Drop Down Menu for Monitoring (Right Side)

Figure 25: Logging screens

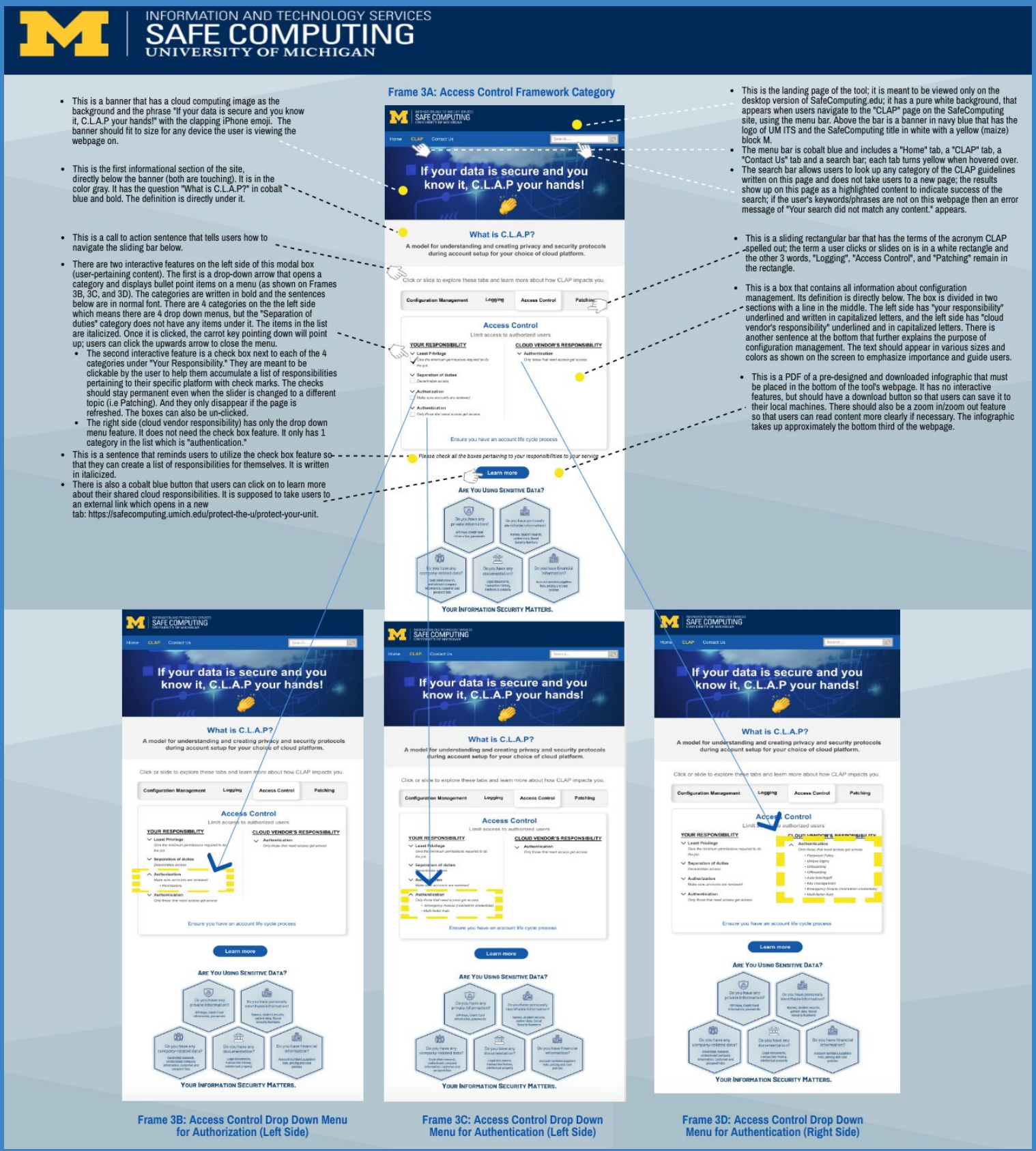


Figure 26: Access Control screens

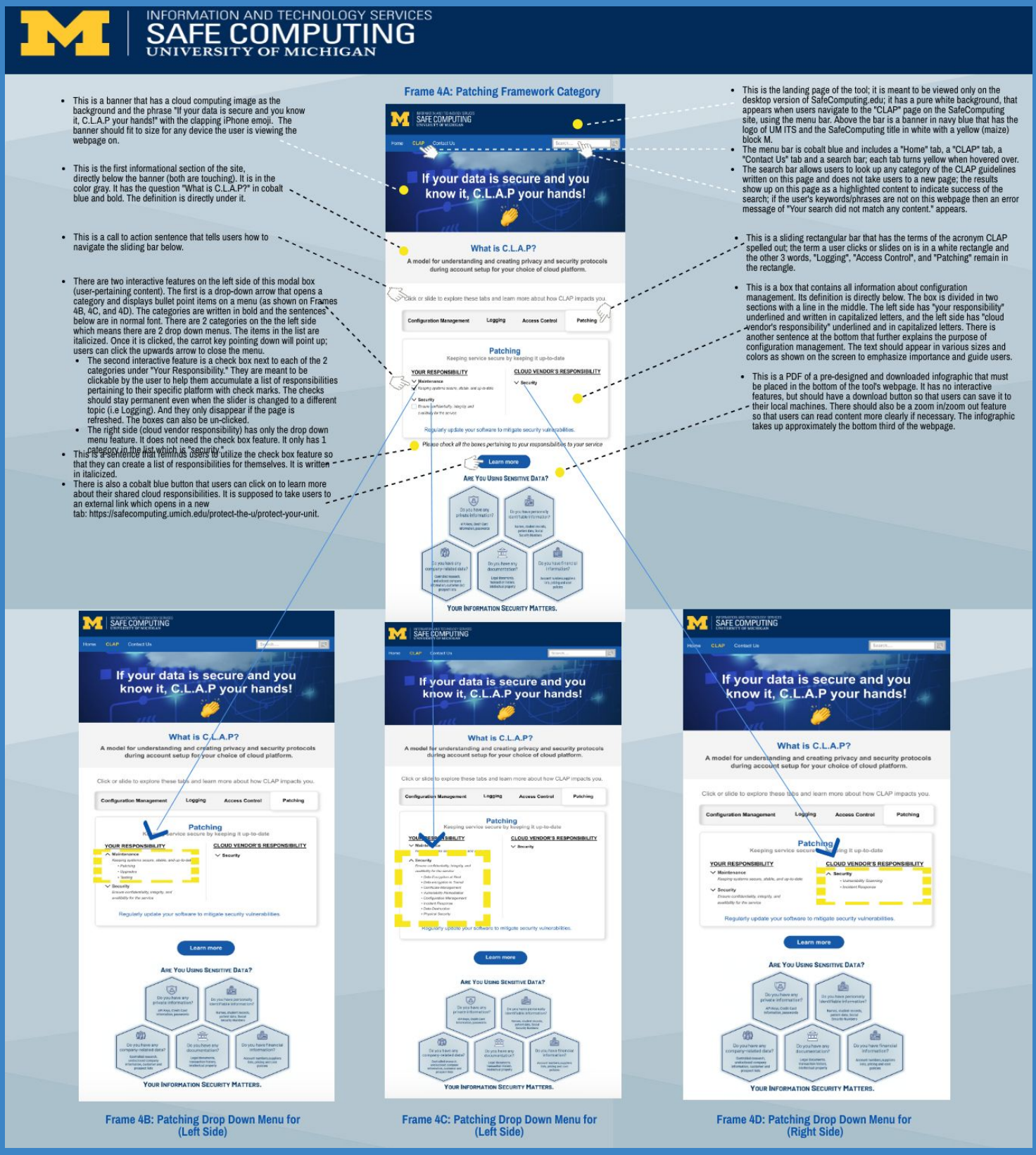
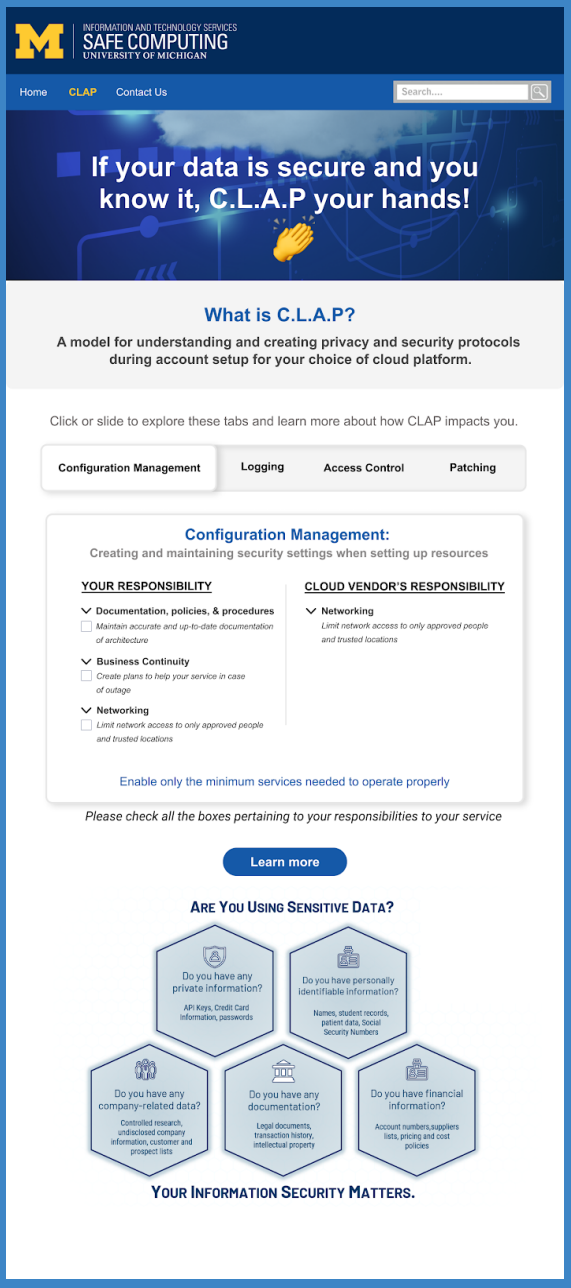


Figure 27: Patching screens

KEY SCREENS



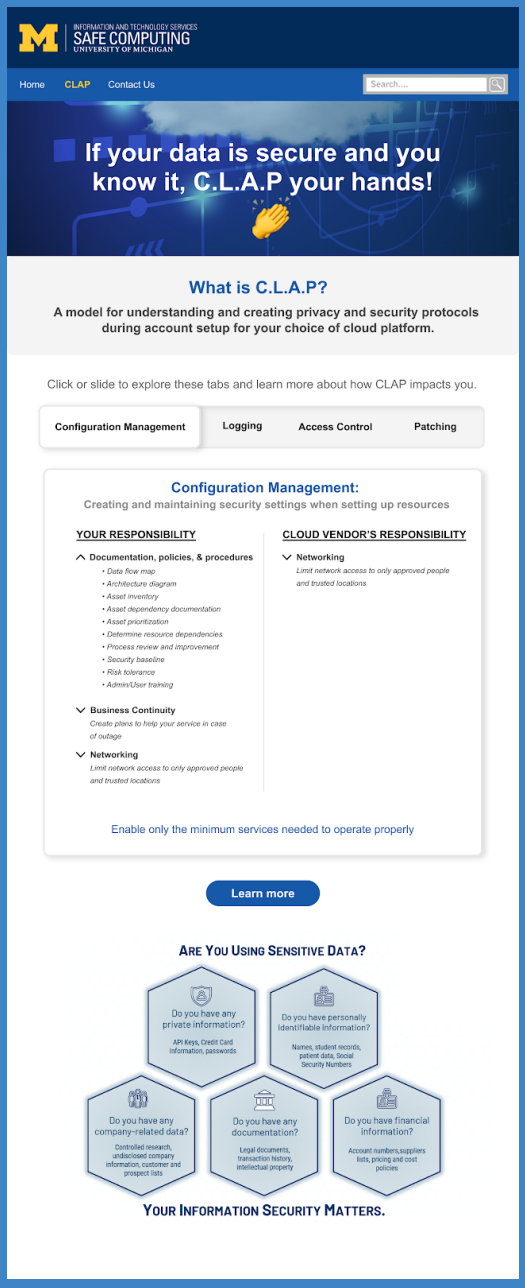


Figure 28 Figure 29

*Screens are only shown for Configuration Management

THE FINAL TOOL AND RECOMMENDATIONS

For the scope of our project, we focused on the overall usability of the tool and making sure that the language used throughout was accessible. Our design rationale and recommendations for the final tool is as follows:

Tool format:

- ITS initially wanted an infographic; however our team ultimately decided that a tool would be more interactive and effective in conveying security protocols than an infographic. Since our scope is information heavy, an infographic would be ineffective as the priority is on information organization over graphic representations of information. It also allowed us to showcase our stakeholder analysis process, and what steps we had to take to understand the context we designed for.

Checkboxes:

- We implemented checkboxes in our tool that allow users to select which protocols are most relevant to them. These offer the user a way to curate their own resources and make the experience more personalized; and also act as a source of feedback for how users feel about specific areas of security. This allows for interaction and decreases the appearance of another ‘terms and services’ guide.

Drop down arrows:

- Drop down arrows hid information but were easily accessible for users who wanted to learn more. This allowed for decrease of information overload, and allowed for more accessibility since users with lower technical literacy levels would be less overwhelmed by information and technical jargon.

CLAP tabs:

- We initially brainstormed displaying all the CLAP information at once; however, showing the information for one section at a time proved to lessen cognitive overload significantly and made the information more easily digestible as well as more visually appealing.

“Learn more” link:

- Originally, the scope of this project was to meet the requirement of conveying responsibility. However, we wanted our tool to be helpful in increasing overall information security in the cloud. Therefore, rather than just conveying the protocols, we wanted to make it so that understanding and acting on these protocols is accessible to users. Instead of adding a ton of extra information, we decided to link the user to pages with additional information.

NEXT STEPS

Moving forward after handing off our tool to ITS, there are several recommendations that we suggest for our client during implementation.

1) **Further validating the tool**
   As our pool for usability testing was limited due to COVID-19, additional validation testing is strongly recommended in order to ensure the tool meets the needs of all potential user groups. We planned but were unable to hear from an optimal breadth of faculty, research assistants, and ITS staff. Feedback from these stakeholders along with communication with cloud vendors would help deliver the tool most effectively.

2) **Juxtaposition of the tool**
   We have suggested a placement spot for our tool; however, further user testing may be needed to determine whether this is the most effective place for the tool to have the largest reach possible.

3) **Implementation/integration**
   The tool itself is close to ready for implementation. In our final meeting with ITS, we will be handing off a spec Figma file that ITS developers will have access to and can utilize when integrating the tool. The Figma file is highly accessible for implementation as it contains a CSS code translation of the design.

CONCLUSION

Secure cloud service delivery and misunderstandings of this effort are increasingly relevant real world problems. The opportunity to design a product addressing this at the enterprise level with ITS was both rewarding and challenging. Our development process began with a complicated matrix and ended with two purposeful tools — an infographic and an interactive prototype on Figma. The project was multifaceted, touching on UX design & research, information security, cloud platform architecture, and the shared responsibility model. As computing on campus and beyond moves to the cloud, we hope that our work will help people educate and innovate for this shift in meaningful ways. We would like to thank the ITS team for their support, cooperation, expertise, and dedication to enabling safe technology use.

APPENDIX

Research Phase:

1) Qualtrics Survey Questionnaire
2) Interview Request Email/ Consent Form
3) Interview Questions

Validation Phase:

4) Validation User Test Questions

Final Product:

5) Figma File