A logo on a blue background

Description automatically generated with low confidence

**UC Tech Awards 2023 Candidate**

**Category**: DESIGN, INNOVATION, IT SECURITY, OPERATIONAL EXCELLENCE

**Name:** Managing Vendor Risk one triage at a time

**Number of people:** (6)

**Location:** UCLA

1. **Person submitting the application/nomination**
   * 1. *Ernesto Carrasco, ITS, University of California, Los Angeles, Staff.*
   1. **Email address:**
      1. *ernestocarrasco@ucla.edu*
   2. **The name of your organization:**
      1. *UCLA*
2. **Award category** 
   * 1. *Design*
     2. *Innovation*
     3. *IT Security*
     4. *Operational Excellence*
3. **Name of person, name of the team, or name of the project to receive the award**
   * 1. *UCLA GRC Team; “Managing Vendor Risk one triage at a time.”*
4. **All project team members** 
   * 1. *Mike Quirk, Manager, ITS, University of California, Los Angeles, Staff, mquirk@it.ucla.edu*
     2. *Anna Santa Cruz, ITS, University of California, Los Angeles, Staff, asantacruz@it.ucla.edu*
     3. *Rohith, Thakkallapally, ITS, University of California, Los Angeles, Staff, rthakkallapally@it.ucla.edu*
     4. *Harold, Shin, ITS, University of California, Los Angeles, Staff, harold@ucla.edu*
     5. *Shun, Tsukazaki, ITS, Deloitte (Staff Augmentation), stsukazaki@deloitte.com*
     6. *Drew Hotaling, ITS, Deloitte (Staff Augmentation),*

*dhotaling@deloitte.com*

1. **Which location was affected by the work?** (the name(s) of the organization affected)
   * 1. *UCLA Campus and UCLA Mednet*
2. **Summary:** *Third Party Risk Management involves a comprehensive analysis of the risks arising from relationships with third-party providers. Through the use of ServiceNow, we’ve been able transform a complex process into a simple repeatable solution that enables us to proactively manage vendor risk.*
3. **Narrative**: **Description of the initiative(s) or portfolio of work that supports the nomination based on the award description.**

The UCLA Third Party Risk Management (TPRM) program supports UCLA campus which has over 40,000 (students and staff). With an organization this size, delays in onboarding vendor’s impacts curriculum delivery, the security of students & staff and faculty support. With that said, in 2021 the Office of the Chief Information Security Officer (OCISO) charged the Governance Risk & Compliance (GRC) team to automate the TPRM process within ServiceNow (SNOW) and officially move away from the manual process that was currently in-place.

The GRC team partnered with the SNOW team to automate the process. In doing so, UCLA was able to: 1) Centrally manage the TPRM process in one tool and eliminate the use of excel spreadsheets and manual processes; 2) All TPRM partners (e.g., IT Security, Accessibility, Privacy & Purchasing) were able to simultaneously work on submitted triages; and 3) The time to complete TPRM triage reviews was cut by two-thirds when compared to the manual process. A huge improvement and well received by the UCLA community.

In 2022 after the release of the first version (TPRM v1.0) we evaluated the feedback and recommendations for improvement from the broader community and immediately began to work on TPRM v2.0. While a number of the recommendation and changes were straight forward, the GRC & SNOW (Team) were challenged with: 1) Improving the interface; 2) Consolidating and reducing the number of questions within the triage form; 3) Implementing the ability to re-purpose previous assessments; and 4) Providing real-time status for submitted tickets. Additionally, we also added “BlackKite” a cyber rating platform with a tool. This enables us to non-invasively quantify and monitor cyber risk across all of our third parties.

In order to meet the challenges, we customized the SNOW portal used for service tickets and developed a user-friendly interface; instead of the out of the box interface provided by SNOW. We then created the triage form within the interface (reducing the number of questions by 66%) and through some really creative and complex scripting on the back end, we were able to repurpose completed assessments, and add versioning to understand how the history of assessments performed. Once we had completed our work and released TPRM v2.0, the broader UCLA community was even more appreciative of new version to the extent we were receiving accolades from Professors; something that had not happened before.

1. **How we meet selection criteria (complexity, impact, and mission alignment).**
   1. *Complexity*

Overall, I believe we are the only school in the UC System that has automated their TPRM process. Aside from the that, our creativity and innovation to repurpose tickets, logic to quantify risk and the centralization of a TPRM function at the program supporting a large complex environment sets us apart from all of the other UC schools. Through our system we’ve addressed the following:

* Legal needs to account for potential risk, data protection and security, and proper contracting.
* Information security needs to ensure IS-3 cyber risk requirements.
* Engineering needs to ensure implementation and integration are done without disrupting environments or slowing down dev work. For example, security needs to ensure will outsourced vendors only have the access and permissions based on level of risk presented by the data being managed.

Lastly, without a third-party party risk assessment and due diligence, will expose UCLA to greater risk. Ideally, as an organization we want to be proactive of managing security, rather than reactive.

* 1. *Impact*

The impact has been huge. Not only have we reduced the overall assessment time by 66%, we’ve also improved the experience for end users. Submitting requests for TPRM reviews can be has been reduced by 50% or more. What used to take on average 30 minutes to complete, now only takes 10 – 15 minutes; even less for renewals. All of which services UCLA (Campus & Mednet); or 40,000 + personnel.

* 1. *Mission Alignment*

Our efforts embody the value of “collaboration”. Through collective insight and action, we’ve produced greater results than that of any UC School and we’ve demonstrated quality outcomes.  All of which was done through teamwork. Moreover, protecting Institutional Information and IT resources is an IS-3 requirement. Our process proactively accomplishes that and more. We’re honoring our commitment and paving the way to better Vendor Management.

1. **How our success is measured/quantified.**

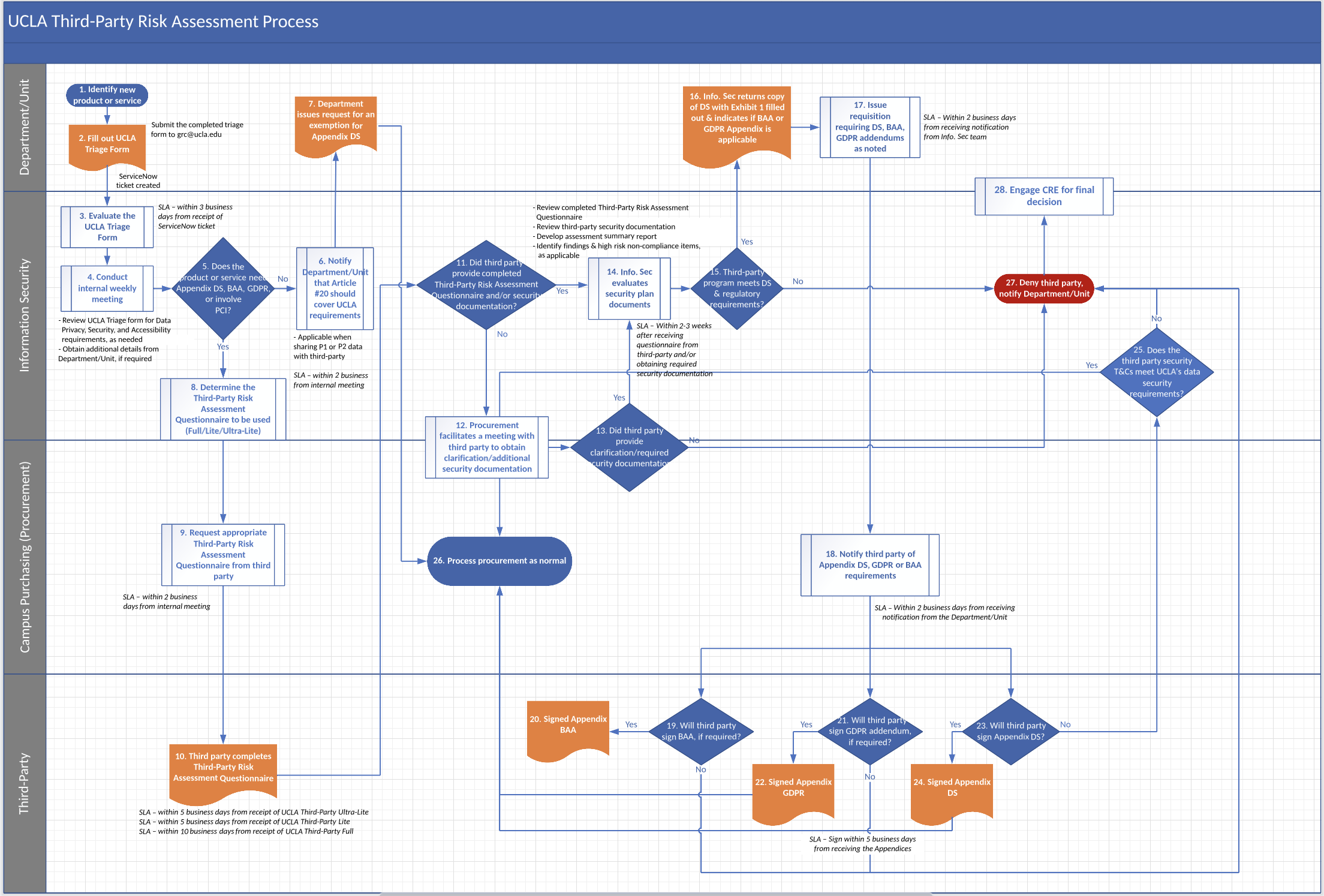
Our success can be measured by the operational impact (please see question B) we have on UCLA while fulfilling our IS-3 security requirements at the program level. To that end, UCLA Medical is now actively performing TPRM assessments using our tool. We are also planning on expanding the use of the tool to other UC schools. Our process protects institutional information and IT Resources, and we take it seriously.

1. **The time during which the work was done.**

The work was performed over a span of two years. However, what is more impressive is that fact that after we released Version 1, we had already begun work on Version 2; completing our changes in December of 2022. Releasing our product in early 2023.

**Appendix A**

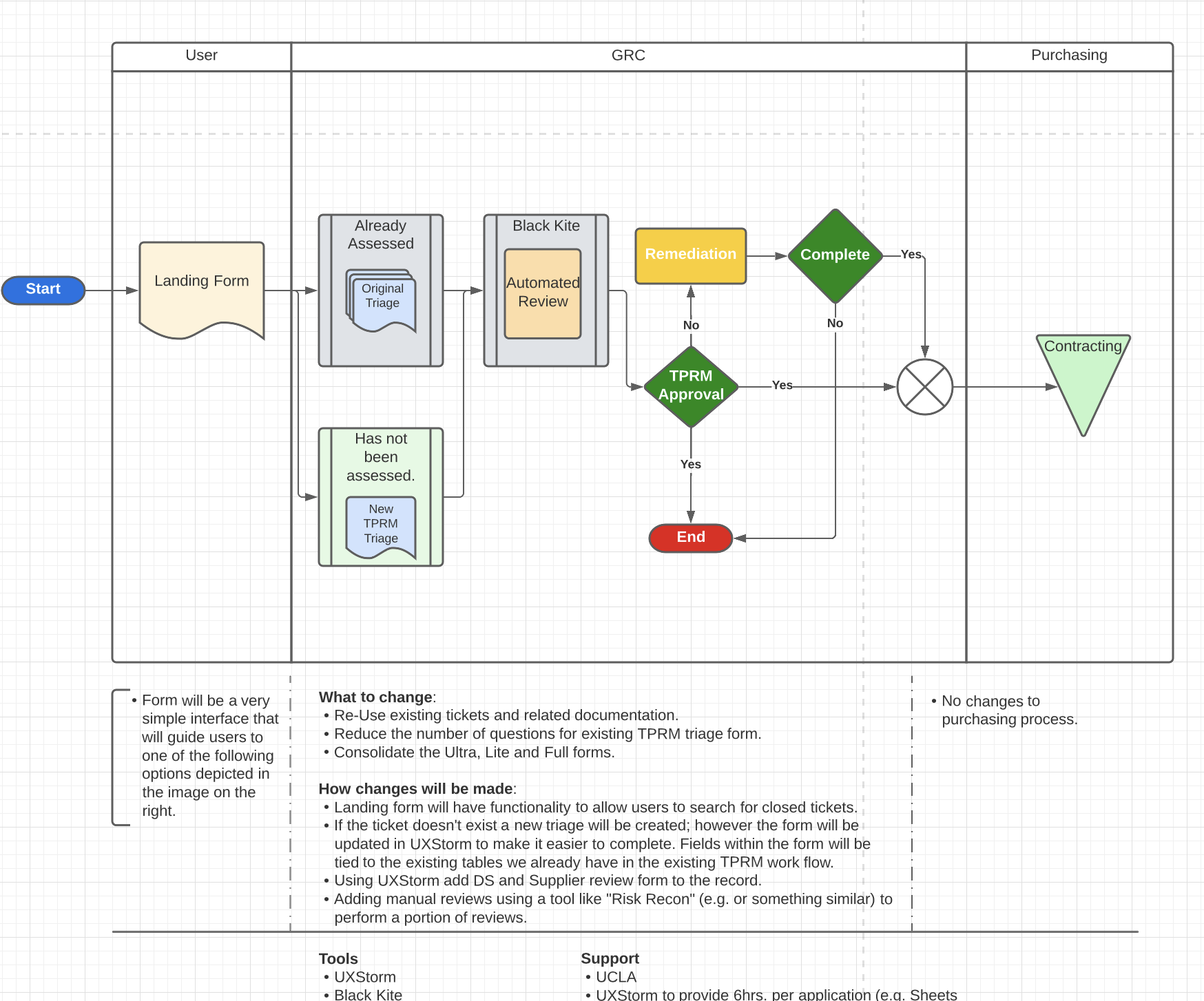
**TPRM Version 1**

****

***Note:*** *All related forms were incorporated into Service Now.*

**TPRM V2.0**

**Note:** This process flow details the changes we wanted to make to TPRM V1.0. Included is our integration of BlackKite our cyber rating platform with a tool.

****

**TPRM V2.0 Video**

[**https://ucla.app.box.com/file/1123215859331?s=u8bw38pvrs7f3z7en4j7kqqndihv5aef**](https://ucla.app.box.com/file/1123215859331?s=u8bw38pvrs7f3z7en4j7kqqndihv5aef)

***\*Please contact me to provide access to folder.***