SOC 2 Project Plan

This project plan details the scope, phases, key activities, roles and responsibilities, and timeline necessary to successfully prepare for and undergo a successful SOC 2 examination, ensuring we meet the trust service criteria relevant to our operations and provide our clients with the assurance they require.

JOHANSON GROUP

SOC 2 Audit Activity

- We hold an onboarding meeting with the client to identify the goals for the engagement, set expectations as far as what the engagement entails, and set a regular cadence / medium of communication moving forward.
- Our CS team will then communicate regularly with the client to answer any questions they have regarding the conduct of the audit as well as ensure they remain on track with their desired timeline.
- Once the client is ready to begin the audit, we will confirm their desired audit dates, ensure that evidence at a high level is at an acceptable level (i.e. tests are passing in their GRC platform, we have a proper control matrix and see that evidence has been gathered, etc (NOTE: this is a very cursory view - not a formal readiness assessment or in-depth review of the quality of evidence)), ensure the System Description (Section III) has been prepared by the client, and ultimately ensure our Audit Team has everything they need for their review.
- Our Audit Team will begin their review of the System Description and the evidence that has been collected. If there are any issues or we require additional evidence, our team will submit their requests either through the client's GRC platform or through another medium (i.e. our own tool for controls testing called Fieldguide, via spreadsheets sent over email, etc).
- Once all evidence has been received and reviewed, our management team will conduct an internal quality review to ensure nothing else is required. If there are issues, similarly to the above, they will reach out - otherwise they will prepare the draft report.
- The draft report will be sent to the client for review / approval.
- After the draft report has been approved, we will send the management representation letters via PandaDoc to be signed.
- Finally, after receiving the signed management representation letters, we will issue the final audit report.

Client Responsibilities

Pre-Audit

- Attend the onboarding meeting with all relevant team members / stakeholders.
- Design / implement controls, ensuring you meet all relevant audit framework requirements.
- Prepare your System Description (Section III) and send to our team as a Microsoft Word document.
- Collect relevant evidence for your controls via your GRC platform or manual evidence repository.
- Grant our Audit Team access to your GRC platform / manual evidence repository.
- **For clients using GRC Platforms:**
  - Perform a final review with your GRC platform's CSM to ensure things are in a good place for the Audit Team.
  - Schedule your audit dates with your Johanson Group CSM.
- **For clients doing a SOC 1 Type II or SOC 2 Type II audit**:
  - Maintain compliance for your controls during the identified observation / audit period and collect the relevant evidence.

During the Audit

- Respond to any additional evidence requests our Audit Team has during their fieldwork.
- Review and approve the draft report when it is provided.
- Approve and sign the management representation letters.
- Pay any final / outstanding invoices prior to conclusion of the engagement.
- Receive and distribute final audit report to stakeholders.

Our Responsibilities

Pre-Audit:

- Host the onboarding meeting.
- Provide System Description (Section III) or control matrix templates if needed by the client.
- Answer any client questions about the audit process as they prepare their controls and evidence.
- CS Team: Confirm audit dates and that the client's audit materials are at an acceptable state (from a high level perspective) as soon as the client confirms they are ready to start.
- Review client-provided System Description and provide any relevant feedback.

During the Audit:

- Review evidence and ask for additional samples when needed in a timely manner
- Perform an internal review upon receipt of all evidence to ensure quality.
- Prepare and send the draft report to the client for review / approval.
- Coordinate with the client on any feedback regarding the draft.
- Send the management representation letter for signature.
- Issue the final audit report to the client.