

SOC 2 RISK ASSESSMENT CHECKLIST

Status key

FC- Fully Completed

IP = In Progress

SOC 2 Risk Assessment: 5 Steps	Status	
Step 1: Define your Business Objectives		
- What are your promising your customers?	FC ☐	IP ☐
- What are you chosen TSCs in your SOC 2 audit?	FC ☐	IP ☐
- Get Management Buy-in	FC ☐	IP ☐
Step 2: Identify In-Scope Systems		
- Which are your critical systems?	FC ☐	IP ☐
- Sift through infrastructure, software, data, people, and procedures	FC ☐	IP ☐
- Make an inventory of the critical systems that dovetail with the TSCs chosen	FC ☐	IP ☐
- Get Management Buy-in	FC ☐	IP ☐
Step 3: Perform Risk Analysis		
- Assess the risks for your business	FC ☐	IP ☐
- Vendors	FC ☐	IP ☐
- Business Partners	FC ☐	IP ☐
- From misuse of the access to information by employees	FC ☐	IP ☐
- Sudden changes in the leadership team, and regulations, as well as changes in economic, physical, and technological landscapes	FC ☐	IP ☐
- Frauds	FC ☐	IP ☐
- Rank the identified risk	FC ☐	IP ☐
- Likelihood of Occurrence	FC ☐	IP ☐
- Velocity of Impact	FC ☐	IP ☐
- Assign Impact values to the risks identified	FC ☐	IP ☐
- Get Management Buy-in	FC ☐	IP ☐
Step 4: Document Risk Responses		
- Assign controls (based on chosen TSCs) to your various identified risks	FC ☐	IP ☐
- Evaluate risk response	FC ☐	IP ☐
Accept the risk	FC ☐	IP ☐
Mitigate the risk	FC ☐	IP ☐
Transfer the risk	FC ☐	IP ☐
Avoid the risk	FC ☐	IP ☐
- Get Management Buy-in	FC ☐	IP ☐
Step 5: Stay Consistent		
- Undertake regular Risk Assessments	FC ☐	IP ☐
- Get Management Buy-in	FC ☐	IP ☐