



## SOC 2 Requirement Gathering Checklist

Sr.no	Requirement	Response	Remarks
1	Name of the Organization		
2	Nature of Business		
3	IT Environment		
4	No Of Endpoints / IT Assets		
5	No of Applications		
6	No of Employees		
7	Have you ever gone through any IT certification before?		

## Check on Control Environment

Sr.no	Requirement	Response	Remarks
1	Do all your assets follow documented configuration standards?		
2	Is all your sensitive data encrypted at rest?		
3	Do you perform formal quarterly user access reviews for all access to your assets?		
4	Are logs from your IT assets centralized within an enterprise solution?		
5	Is there a formal and followed incident response process?		
6	Do you perform quarterly vulnerability scans?		
7	Are high and medium issues identified by these scans remediated in a timely manner?		
8	Do you have formally documented policies and procedures?		
9	Do you perform background checks on employees?		
10	Do you have a formal third party management program?		
11	Do you have a formally documented BCP/DR plan?		
12	Is the BCP/DR plan tested on an annual basis?		
13	Have you performed a privacy impact assessment on your environment?		
14	Do you consistently perform annual risk assessment?		
15	Do you follow a change management process for all IT changes?		