Client Security Risk Assessment Questionnaire

Name of Company:	
Company's Website:	
Contact Person Completing the Assessment:	
Email Address:	
Phone Number:	

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments s

	Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
	Organizational Information Security			
1	Do you have a member of your organization with dedicated information security duties?			
2	Is a background check required for all employees accessing and handling the organization's data?			
3	Does the organization have written information security policies?			
3.1	If yes, please provide copies when responding to this assessment			
4	Does the organization have a written password policy that details the required structure of passwords?			
4.1	How do you verify password strength?			
5	Do all staff receive information security awareness training?			
6	Does the organization have a Data Access Policy and are they willing to comply with the policies as well as the data protection guidelines?			
7	Does the organization have a formal change control process for IT changes?			
9	Will your company be processing credit cards?			
9.1	If yes, is your company PCI DSS compliant?			
	General Security			
10	Is antivirus software installed on data processing servers?			
11	Is antivirus software installed on workstations?			

Client Security Risk Assessment Questionnaire

Name of Company:	
Company's Website:	
Contact Person Completing the Assessment:	
Email Address:	
Phone Number:	

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments s

	Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
12	Are system and security patches applied to workstations on a routine bases?			
13	Are system and security patches applied to servers on a routine bases?			
13.1	Are system and security patches tested prior to implementation in the production environment?			
14	Do employees have a unique log-in ID when accessing data?			
15	Does the organization have security measures in place for data protection?			
15.1	If yes, please describe in the comments section			
16	Is access restricted to systems that contain sensitive data? *(credit card numbers, social security numbers, HIPAA, & FERPA data sensitive)*			
16.1	If yes, what controls or are currently in place to restrict access?			
17	Is physical access to data processing equipment *(servers and network equipment)* restricted?			
17.1	If yes, what controls are currently in place?			
18	Is there a process for secure disposal of both IT equipment and media?			
18.1	If yes, please describe in the comments section			
	Network Security			
19	Are network boundaries protected by firewalls?			
20	Is regular network vulnerability scanning performed?			

Client Security Risk Assessment Questionnaire

Name of Company:	
Company's Website:	
Contact Person Completing the Assessment:	
Email Address:	
Phone Number:	

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments s

	Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
21	Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization?			
21.1	If yes, please describe in the comments section			
22	Are employees required to use a VPN when accessing the organization's systems from all remote locations?			
23	Is wireless access allowed in your organization?			
23.1	If yes, please describe how it is protected in the comments section			
	Systems Security			
24	Are computer systems *(servers)* backed up according to a regular schedule?			
24.1	Has the back-up and recovery process been verified?			
24.2	Does the organization store backups offsite?			
24.3	Does the organization encrypt its backups?			
25	Does the organization replicate data to locations outside of the United States?			
26	Does the organization outsource its data storage?			
26.1	If yes, to whom is the data outsourced?			
27	Is there formal control of access to System Administrator privileges?			
28	Are servers configured to capture who accessed a system and what changes were made?			

Client Security Risk Assessment Questionnaire

Name of Company:	
Company's Website:	
Contact Person Completing the Assessment:	
Email Address:	
Phone Number:	

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments s

	Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
28.1	If no, in case of a security breach, how do you determine who accessed the system and what changes were made?			
	Business Continuity / Disaster Recovery			
29	Does the organization have disaster recovery plans for data processing facilities?			
29.1	What about Business Continuity Plans?			
30	Are computer rooms protected against fire and flood?			
31	Does the organization have a "Hot" recovery site?			
	Incident Response			
32	If an information security beach involving senstive data occurred, what is the defined protocal?			
32.1	If yes, how soon would the Institute be notified?			
33	Does the organization have a formal Incident Response plan?			
34	Has the organization experienced an information security breach in the past three to five years?			
34.1	If so, please document what information was lost in the comments section?			
34.2	If so, please document how the clients were notified and how quickly in the comments section?			
	Auditing / Client Reporting			
35	Does the organization receive an SSAE-16 SOC Report?			

Client Security Risk Assessment Questionnaire

Name of Company:	
Company's Website:	
Contact Person Completing the Assessment:	
Email Address:	
Phone Number:	

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments s

	Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
35.1	If so, please document which type of SOC report is being obtained in the comments section. Please provide a copy of the latest SOC report.			
35.2	If not, does the organization allow clients the right to audit their systems and controls?			
	Additional Security Questions Specific to the Service Offering(s) Provided by the Vendor	**Response**	**Comments**	**Endeavor's Comments/Questions to Client responses**
1				
2				
3				