



**EVALUATION OF ENTERPRISE RISK
 CONFIDENTIAL CYBERSECURITY CHECKLIST**

Name of Applicant’s Holding Company System:
Name of Legal Entities <u>Not Included</u> in the Responses Below:
Explain why the legal entities listed above (if any) are excluded:

		Yes	No	Provide Comments if Response is “No”
1.	Have you recently performed a thorough research on all the operating systems, software applications, and data center equipment used by the holding company system? ENTER DATE PERFORMED:			
2.	Have you recently reviewed the IT policies and procedures used by the holding company system? ENTER DATE PERFORMED:			
3.	Do you have a cybersecurity incident response plan in place?			
4.	Do you have a set of predefined communication guidelines that can be used in the event of a security failure?			
5.	Does your holding company system have appropriate back up procedures in place to minimize downtime and prevent loss of important data?			
6.	Is there a cybersecurity training program in place for current and new employees?			
7.	Do you restrict administrative and privileged access to systems and data through preventative and detective controls to prevent unauthorized access or alteration of systems and/or data?			
8.	Do you allow only trusted software to execute on operations systems?			
9.	Do you prevent the execution of other than trusted software through the use of application whitelists?			
10.	Do you have a patch management application for both your servers and every computer/workstation used in your holding company system?			

Provide complete answers on a separate page if necessary. Identify by item number.

		Yes	No	Provide Comments if Response is "No"
11.	Do you have antivirus installed on your servers and on every computer/workstation used in your holding company system?			
12.	Does your holding company system have a host intrusion prevention solution or a firewall installed?			
13.	Do you periodically perform vulnerability scans on your servers and all the computer/workstations used in your holding company system?			
14.	Do you use local encryption solutions for every computer/workstation, including mobile devices, used in your holding company system?			
15.	Do you employ a password management system for every user in the holding company system?			
16.	Do you enforce robust password security per NIST standards that include:			
	a) Upper and lower case letters, numbers, and symbols			
	b) A minimum of 8 characters, avoiding common words and dates			
	c) Password is not used for any other credential			
	d) Changing passwords regularly			
	e) Deploy multi-factor authentication			
17.	Do you have email filtering and Internet traffic filtering software that protects users from the full range of email threats, including malware, phishing and spam?			
18.	Does your holding company system have a long-term plan concerning its cybersecurity strategy, including plans to mitigate any IT system gaps resulting from merger/acquisition activity?			

Provide complete answers on a separate page if necessary. Identify by item number.