20 Questions – Technological Risk Maturity Assessment Checklist

***Note: This assessment addresses the range of technology risks facing a government organization*. It can also be used to solely address the cyber risk component. Because of the subjectivity of evaluation from one entity to another and the absence of metrics for each of the variables below, the benchmarking is not intended for use in comparing one entity against another, nor the conformity of a particular technology environment against any set of rules or expectations.[1]**

Governance	*1: Does not describe my organization at all ……5: Accurately describes my organization*					
1.	The governing body and senior management (governance team) are responsible for overseeing the development of a Technology Plan and confirming its implementation	1	2	3	4	5
2.	The governance team ensures that the Plan is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued	1	2	3	4	5
3.	The team demonstrate visible and active commitment to the implementation of the Plan	1	2	3	4	5
4.	Executives and managers are responsible for understanding at the appropriate level how technology risks could impact and originate from their activities	1	2	3	4	5
5.	Senior leadership understands who is responsible for managing cyber risk when managing security incidents	1	2	3	4	5
6.	The organization has access to technology and cyber expertise at its highest management levels	1	2	3	4	5
7.	The organization undertakes to continuously improve the integration of its technology risk management with its other risk management initiatives	1	2	3	4	5
8.	The chief executive has a clear decision path for action and communication in response to a significant security failure or accident	1	2	3	4	5
Plan						
9.	The organization conducts comprehensive assessments of its vulnerabilities to internal and external risks appropriate for its size and technological profile	1	2	3	4	5
10.	The organization monitors the effectiveness of its risk management strategy	1	2	3	4	5
11.	The organization periodically internally verifies its compliance with rules and regulations	1	2	3	4	5
12.	The organization's commitment to the Plan is reflected in its policies and practices	1	2	3	4	5
13.	Managers, employees and agents receive specific training on Plan elements, tailored to relevant needs and circumstances	1	2	3	4	5
14.	The organization has identified its data and information as vital assets, and organizes its Plan around the recognition that data and information have value that can be separately recognized and protected	1	2	3	4	5
15.	The risk management elements of the Plan includes all material third-party relationships and information flows	1	2	3	4	5
16.	The organization conducts comprehensive internal short- and long-term cyber risk impact assessments	1	2	3	4	5
Relationships						
17.	The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization's specific cyber risk management standards or industry best practices, in line with the Plan, and formalizes this requirement using contractual obligations	1	2	3	4	5
18.	The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents	1	2	3	4	5
19.	The risk management plan element includes all material third-party relationships and information flows	1	2	3	4	5
20.	Executed plans reflect technology services that meet the needs of the organization's employees, constituents, clients.	1	2	3	4	5
Average (gives maturity stage) – total the numbers for each question and divide by 20. Total: *Match the number to the Stage description in the Supplemental Handbook at http://blousteinlocal.rutgers.edu/managing-technology-risk/*		/20 =				

[1] Adapted from World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist

20 Questions – Technological Risk Maturity Assessment Checklist