During 2021, a cyber attack is expected to occur every 11 seconds.

Organizations affected by cyber attacks run the risk of having their normal business operations disrupted, as well as losing valuable data, customers and reputation within their industry.

Is your organization prepared to face this threat ?

Take the cyber resiliency assessment today

Based on the NIST Security Framework, the Storage Cyber Resiliency Assessment Tool (CRAT) provides a bridge mechanism to evaluate the current data protection state of your organization, identify gaps, strengths, weaknesses, and provides recommendations to build an effective cyber resiliency plan.

Storage Cyber Resiliency & Disaster Recovery Assessment Report

IBM Security & Resilience

January 5, 2021

Overview

IBM is pleased to present [a report based on our findings from the IBM® Storage Cyber Resilience & Disaster Recovery Assessment workshop that took place with the [Customer] team on December 5th, 2019. It is understood that an effective cybersecurity resiliency program must be grounded in effective systems and processes that provide valuable insight into information and events that occur within an environment and provide the confidence for an orchestrated storage resiliency process in order to not disrupt [Customer]'s business continuity objectives. By evaluating the current cybersecurity and resiliency environment, the organization now has specific recommendations designed to help increase the value of the solution and services in its environment and meet RTO and RPO requirements.

Additionally, [Customer] will be able to help deliver faster return on investment and higher operational productivity by leveraging time-tested practices and updates to product features and resiliency functions. It will be able to help decrease errors and inconsistency through the implementation of the incremental recommendations we have provided in this document.

Executive summary

Based on the information gathered during our initial reviews within IBM during 4Q 2019 as well as the assessment workshop in Benton Harbor on December 5th, [Customer] has realized great value from its investment in cyber resilience and is generally on-par with other customers that IBM has worked with. However, there are several areas where [Customer] has exposure to risk resulting in unrecoverable data loss or corruption and where more value can be realized.

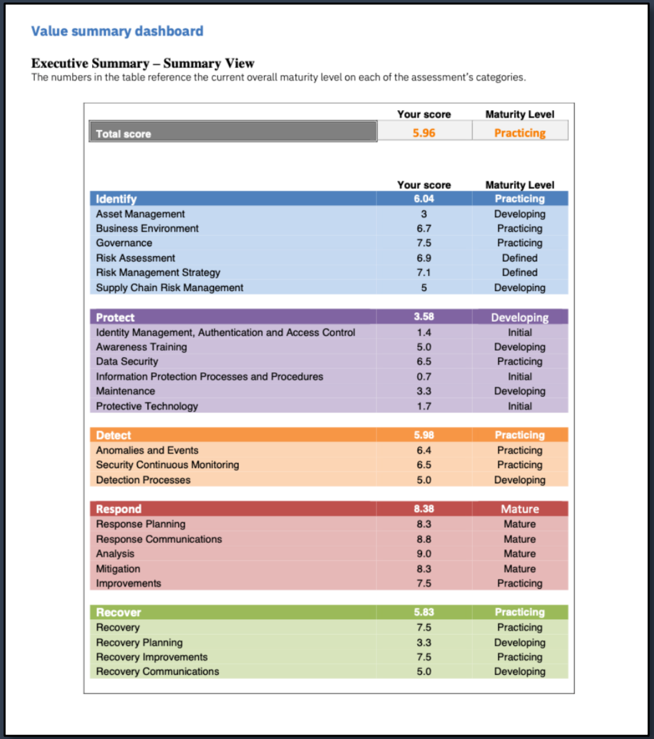
[Customer] has many IT service providers of which IBM is a significant partner. Of the many environments considered and reviewed for this assessment, we have taken an enterprise-view.

Performance in the environment is satisfactory, though [Customer] recognizes that the organization is one cyber breach away from severely impacting business continuity. [Customer] senior management must understand that risk is the new normal. Being a digital enterprise in 2020 incurs significant risk and Cyber Resiliency (protection, data vaulting and recovery) is now an absolute part of the cost of doing business.

Additionally, IBM feels that [Customer] would benefit from the use of Spectrum Insights to measure different performance and capacity areas in order to drive them toward strong outcomes.

Cyber resiliency should be viewed as a dynamic and ever-evolving practice that requires continuous improvement and focus. With the continued expansion of the threat landscape and pace of technology change, it is imperative that organizations constantly take inventory of how they are doing and where they need to be evolving.

Please review the Recommendation Section for our roadmap, which, if followed, will improve functionality and increase the value realized from implementing resiliency and disaster recovery best practices and solutions. Establishing a mature cyber security and resiliency plan will enable a more proactive approach in detecting, identifying, and protecting their environments, as well as their ability to respond and recover quickly.



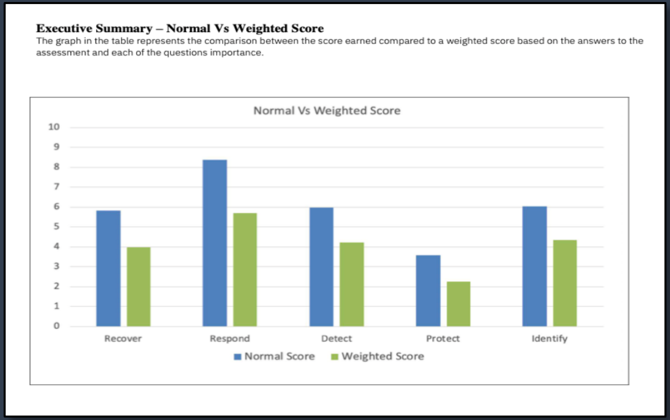
Value summary dashboard

Executive Summary – Summary View

The numbers in the table reference the current overall maturity level on each of the assessment's categories.

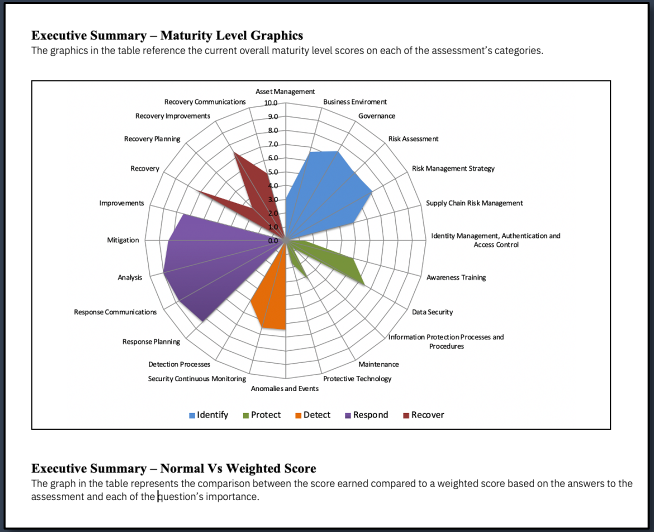
	Your score	Maturity Level
Total score	5.96	Practicing

	Your score	Maturity Level
Identify	**6.04**	**Practicing**
Asset Management	3	Developing
Business Environment	6.7	Practicing
Governance	7.5	Practicing
Risk Assessment	6.9	Defined
Risk Management Strategy	7.1	Defined
Supply Chain Risk Management	5	Developing
Protect	**3.58**	**Developing**
Identity Management, Authentication and Access Control	1.4	Initial
Awareness Training	5.0	Developing
Data Security	6.5	Practicing
Information Protection Processes and Procedures	0.7	Initial
Maintenance	3.3	Developing
Protective Technology	1.7	Initial
Detect	**5.98**	**Practicing**
Anomalies and Events	6.4	Practicing
Security Continuous Monitoring	6.5	Practicing
Detection Processes	5.0	Developing
Respond	**8.38**	**Mature**
Response Planning	8.3	Mature
Response Communications	8.8	Mature
Analysis	9.0	Mature
Mitigation	8.3	Mature
Improvements	7.5	Practicing
Recover	**5.83**	**Practicing**
Recovery	7.5	Practicing
Recovery Planning	3.3	Developing
Recovery Improvements	7.5	Practicing
Recovery Communications	5.0	Developing



Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the questions importance.



Executive Summary – Maturity Level Graphics

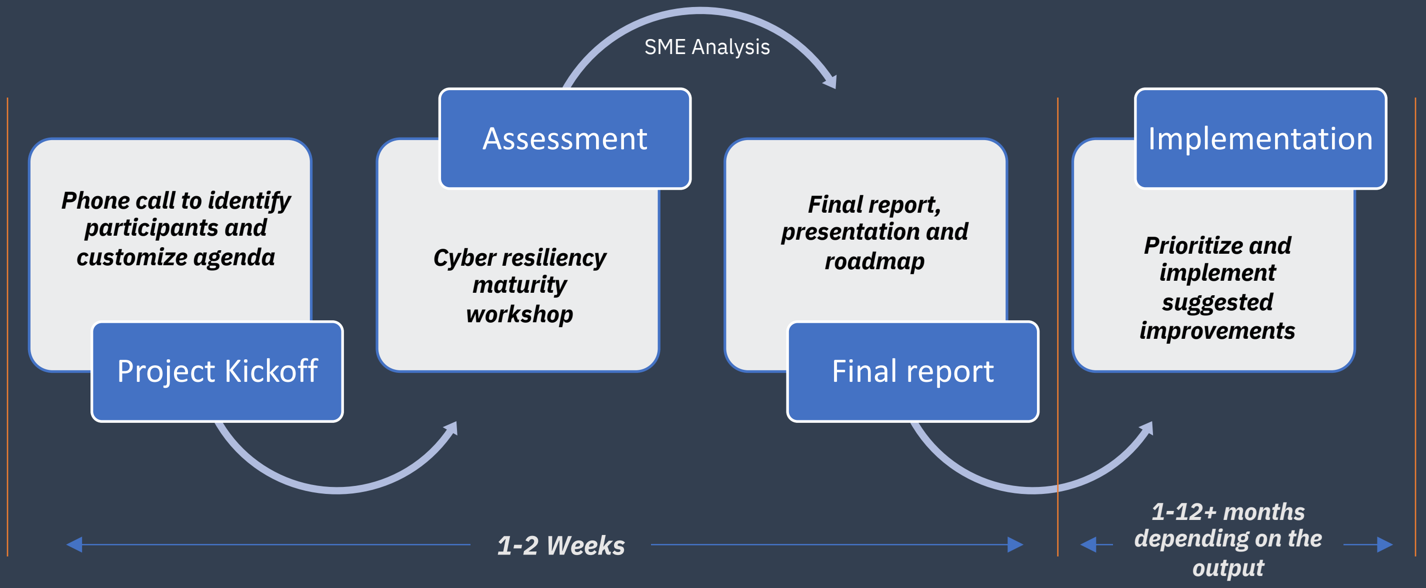
The graphics in the table reference the current overall maturity level scores on each of the assessment's categories.

Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the question's importance.

What can you expect from this assessment ?

- Funded by IBM (no cost to the customer)
- Two-hour virtual assessment workshop
- Only 2 weeks to receive the following deliverables from IBM:
  - Detailed assessment report
  - Management presentation
  - Roadmap of recommended improvements and considerations


SME Analysis
Phone call to identify participants and customize agenda
Project Kickoff
Assessment
Cyber resiliency maturity workshop
Final report, presentation and roadmap
Final report
Implementation
Prioritize and implement suggested improvements
1-2 Weeks
1-12+ months depending on the output

If you are interested in doing the Storage Cyber Resiliency Assessment, please contact:

- Juan Carlos Jiménez
- Storage Client Technical Specialist
- ✉ juan.c.jimenez@ibm.com

- Julio Hernández
- Storage Solutions for Cyber Resiliency Offering Manager
- ✉ julioce@mx1.ibm.com

Why IBM ?

IBM Storage for cyber resiliency provides end-to-end solutions that can efficiently prevent, detect, and respond to cyberattacks as a result of a deep integration between innovative technology and a comprehensive portfolio of software and hardware offerings. By providing multi-layered security and high resilient functionality, this portfolio can maximize the data protection capabilities to help organizations significantly reduce the risk of business disruption and financial losses due to user errors, malicious destruction, or ransomware attacks.