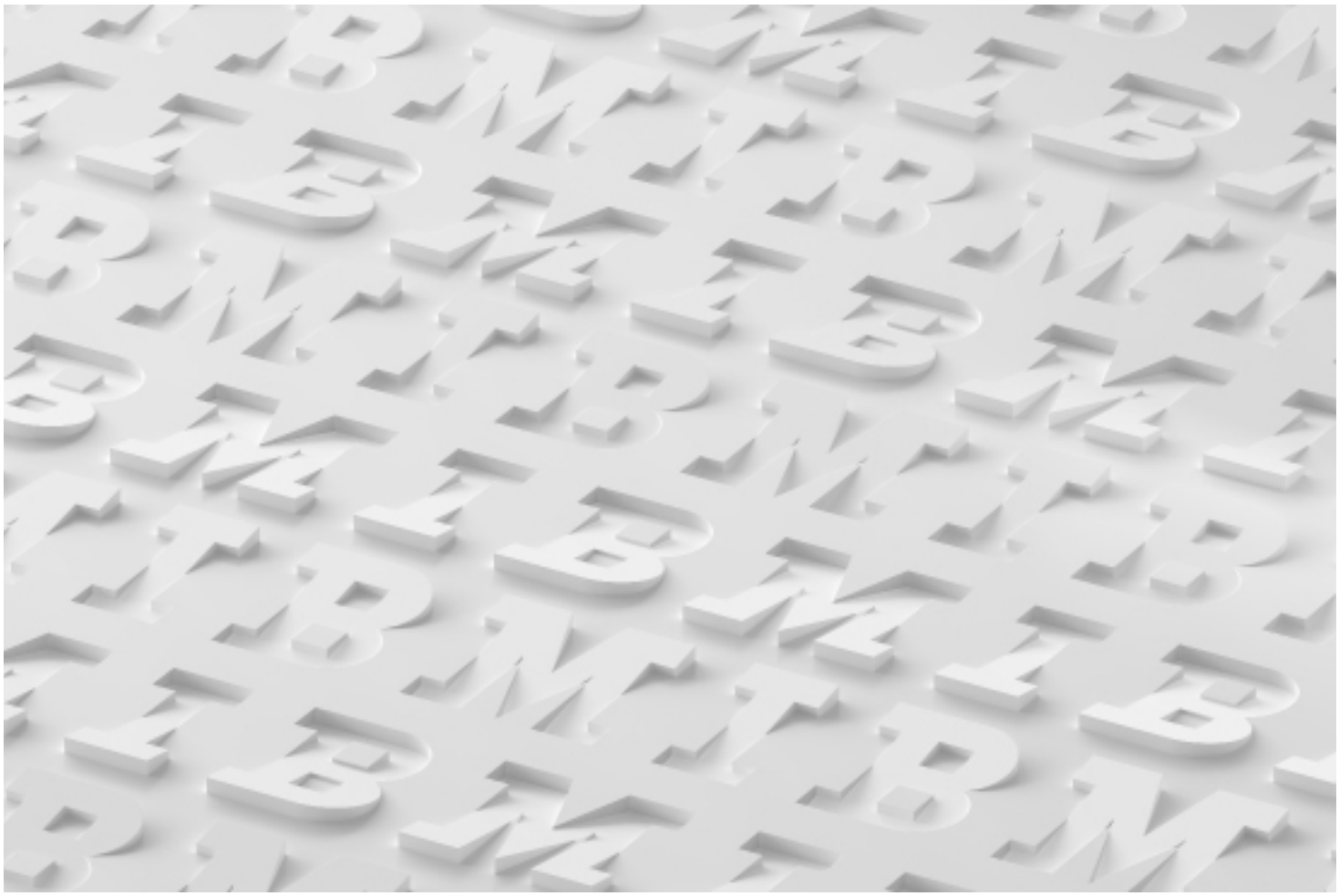
IBM Client Engineering

# Security & Resilience Assessment Report

March 18th, 2024



# Overview

IBM is pleased to present a report based on our findings from the IBM® Security & Resilience Assessment which was completed in collaboration between the Storage and Security teams of CLIENT and the IBM Client Engineering team. This report is designed to help the client leverage effective systems and processes that provide valuable insight into information and events that occur within an environment and provide the confidence for orchestrated security and resilience processes to not disrupt business continuity objectives.

The foundation of this assessment has been inspired by the US NIST Cyber Security framework as well as the EU Digital Operational Resilience Act (DORA). By evaluating the client's current operational security, cyber security and resilience environment, the organization now has specific recommendations designed to increase the value of the solutions and services in its environment, meet RTO and RPO requirements and help improve CLIENT's posture against the above-mentioned standards.

Additionally, existing technology 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.

This assessment covers the client's environment at a high level and helps highlight its strengths, weaknesses, and gaps. It serves as a great starting point to prioritize initiatives.

# Executive summary

Based on the information gathered during our initial reviews within IBM as well as the responses on the assessment, CLIENT can realize great value from its investment in cyber resilience and is not yet at the desired target level. There are many areas where there is exposure to risk resulting in unrecoverable data loss or corruption and where more value can be realized.

Senior management must understand that risk is the new normal. Being a digital enterprise in 2024 incurs significant risk, and Cyber Resilience (protection, data vaulting, air-gapping, and recovery) is now an absolute part of the cost of doing business.

The client appears to be developing / slightly below average / highly mature in adopting controls and practices. Most of the improvements will be in reviewing cyber incident specific response plans, improving efficiency, IBM sees necessary improvement in implementing Zero Trust policies like least privilege access, and continuous verification with an 'assume breach' attitude. Also, the areas of protecting critical assets, and amending and testing recovery plans for serious incidents require more attention. Continuous data validation ('golden copy') should be introduced as a standard operational process to ensure recovery data are corruption-free and not affected by any malware. The most critical recommendation for enterprise sized environments is to introduce immutable copies, especially for protecting data supporting CLIENT's critical business processes, and a dedicated sandbox environment used for restoring procedures. To handle an incident which would require a mass restore, such recovery procedures should be regularly tested. In a large enterprise environment, the financial impact of large-scale cyber incidents can be contained by establishing specific RTO/RPO/retention targets for such cases.

Operational security and cyber resilience 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 operational security, cyber security and resilience plan will enable a more proactive approach in detecting, identifying, and protecting your environments, as well as your ability to respond and recover quickly and effectively.


## Assessment Background Information

**Purpose and Reference**
The IBM Security and Resilience Assessment provides a bridge mechanism to assess client's current state and identify gaps against best practice requirements based on well-established requirement frameworks, such as e.g. the NIST CSF, or EU DORA. It helps in the identification of blind-spots and recommended areas for improvement.

The assessment is primarily based upon the requirements laid down in the above-mentioned frameworks and is focused on storage and security. It Contains references to other industry recognized standards & frameworks: ISO, COBIT, ISA, Council on Cyber Security, among others.

**Maturity Level Definitions**
The scores in the boxes above will be referenced throughout this document to match the score with the maturity level.

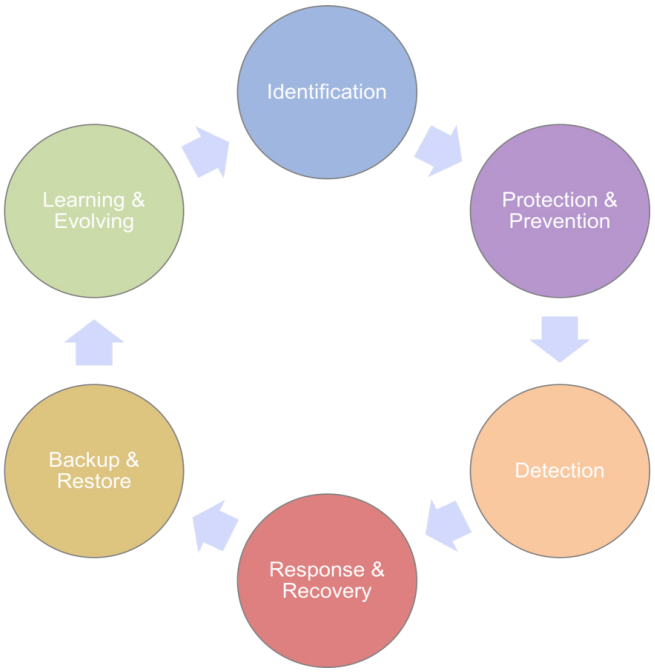
# Value summary dashboard

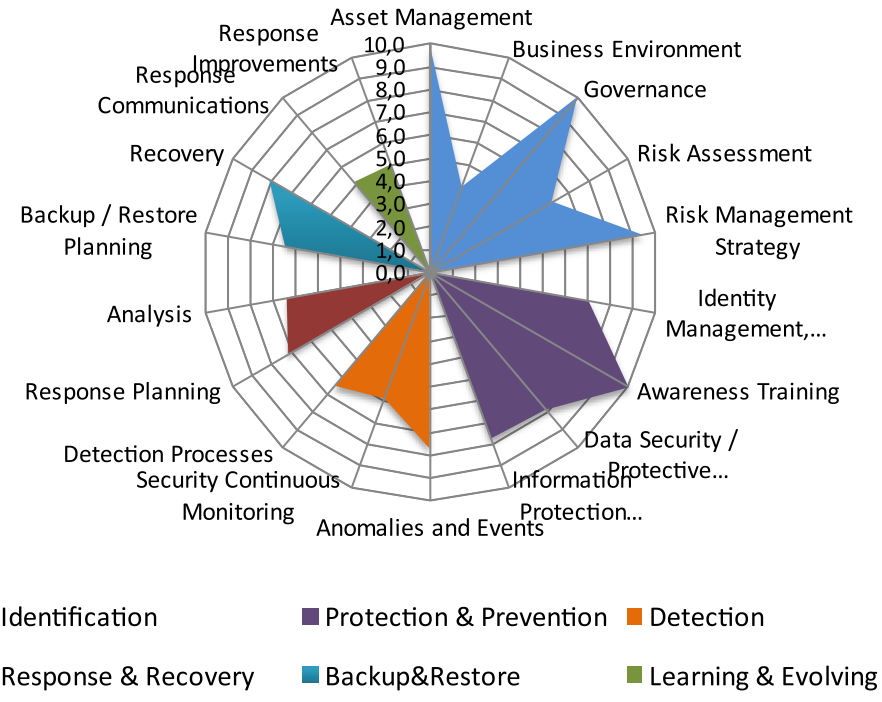
**Executive Summary – Summary View**
The numbers in the table reference the current overall maturity level on each of the assessment's categories.

| | | |
|---|---|---|
| **Total score** | **6,78** | **Practicing** |
| **Identification** | **7,22** | **Practicing** |
| Asset Management | 10,00 | Leading |
| Business Environment | 3,98 | Developing |
| Governance | 10,00 | Leading |
| Risk Assessment | 6,15 | Developing |
| Risk Management Strategy | 9,44 | Mature |
| **Protection and Prevention** | **7,78** | **Practicing** |
| Identity Management, Authentication and Access Control | 7,05 | Practicing |
| Awareness Training | 10,00 | Leading |
| Data Security / Protective Technology | 7,84 | Practicing |
| Information Protection Processes and Procedures | 7,75 | Practicing |
| **Detection** | **10,00** | **Practicing** |
| Anomalies and Events | 7,66 | Practicing |
| Security Continuous Monitoring | 5,86 | Developing |
| Detection Processes | 6,44 | Practicing |
| **Response and Recovery** | **6,91** | **Practicing** |
| Response Planning | 7,17 | Practicing |
| Analysis | 6,36 | Practicing |
| **Backup & Restore procedures and methods** | **6,88** | Practicing |
| Backup / Restore Planning | 6,46 | Practicing |
| Recovery | 8,13 | Mature |
| **Learning and Evolving** | **5,11** | **Developing** |
| Response Communications | 5,15 | Developing |
| Recovery Improvements | 5,00 | Developing |

# Executive Summary – Maturity Level Graphics

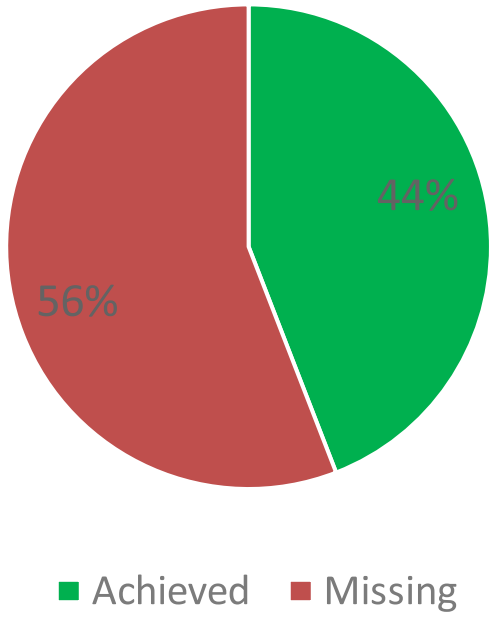
The spider charts below reference the current overall maturity level scores on each of the assessment's categories.



**Executive Summary – Ransomware % Achieved**
The pie chart in the table below represents a percentage of ransomware related questions within the assessment based on Client's answers. Ideally, we want to see a 100% Achieved Score.

## Ransomware Percentage Achieved




## Insights

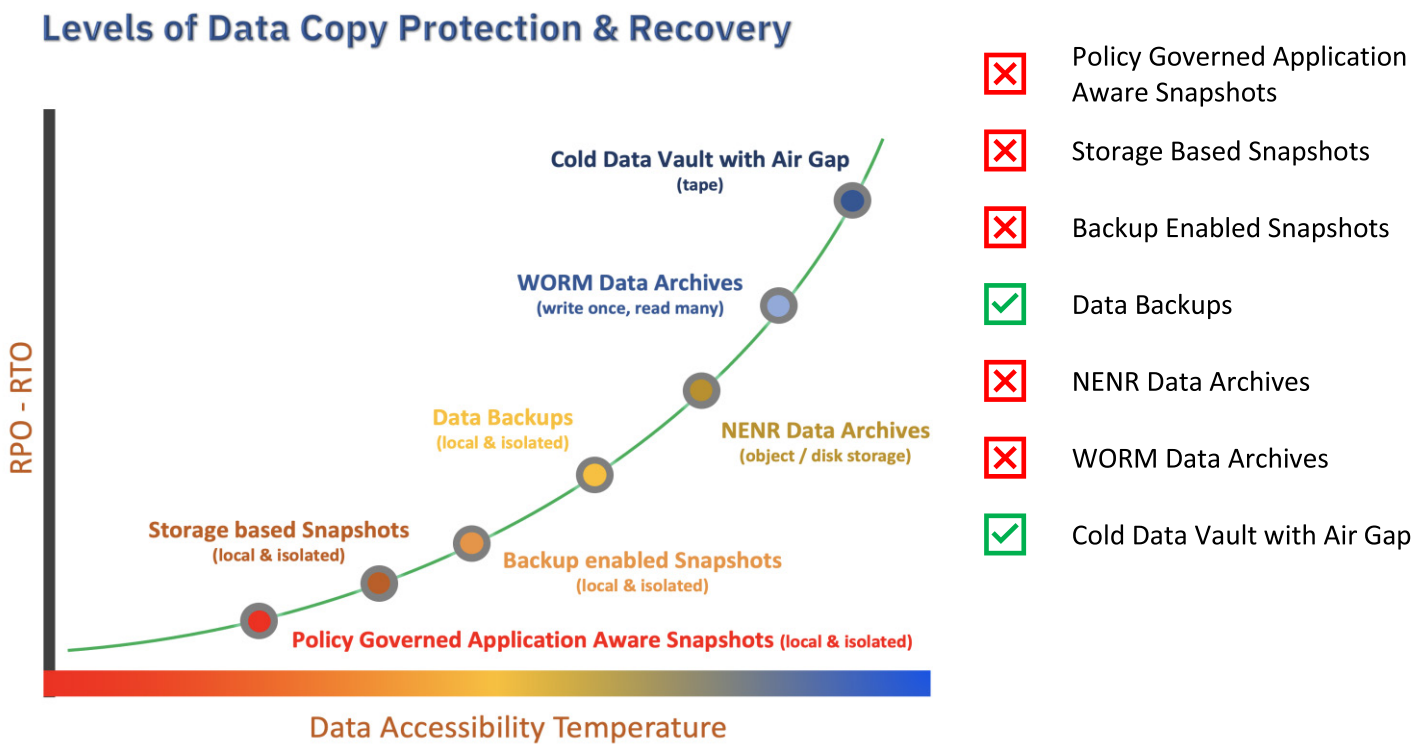
This chart shows some percentage of ransomware readiness. This is evidence that Client should implemented more resilient systems and procedures with the environment to be on a good track to protect the environment from and in case of a ransomware attack. The missing percentage shows a large area for improvements that can be beneficial for the team. Consider fully implementing a physical, or logical air-gap as well as an immutability solution. Retention sets and isolated local vaults could make a big impact. A workshop and follow-up can be scheduled on that topic.

In terms of detection, we recommend keeping an eye and setting alert thresholds for virtual machine block change rate, compression, and deduplication. Any sudden or larger than normal changes could be red flags and a warning that Ransomware is in the system and encrypting data. Threat hunts/ assessments can also be performed on a routine basis with current EDR technology in place.

Additionally, simple best practices can have a high impact on this score, preparing for and testing these recommendations is key. For example, during recovery we recommend "coming back" into an alternate environment before going to production. This will enable the company to ensure that the restore won't cause follow on problems as well as make sure that the data is not compromised or corrupted.

Lastly, we recommend reviewing, creating, and updating Response plans (Incident Response, Business Continuity, and Cyber Resiliency) and recovery plans (Incident Recovery and Disaster Recovery) and ensure they include new Ransomware related items.

**Levels of Data Copy Protection & Recovery**
The graph below shows different layers of protection at the storage level in order to meet different RPO and RTO targets based on Data Accessibility Temperatures. The items with checkmarks are currently being leveraged by the client. We recommend implementing a layered protection approach for resilience.




**Copy Separation**
Create a structure of data separation across multiple layers and services including;

- Copy Services
- Backup Services
- Separation of security controls

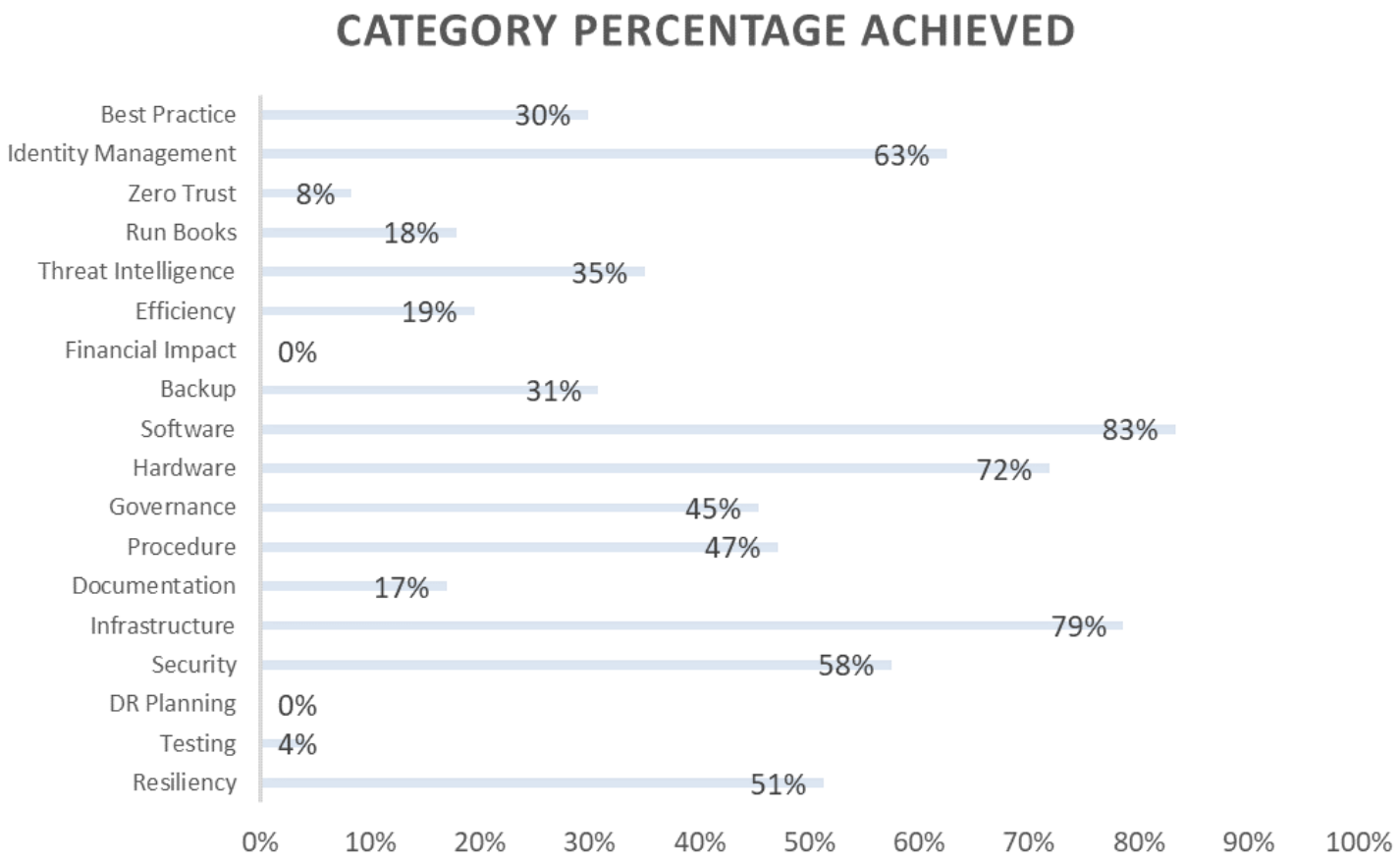
**Immutability & Access Isolation**
Create a structure of data isolation multiple layers and services including;

- Air Gap
- Non-erasable / Non-rewritable Storage
- Cold Storage / Object Storage
- Data Vaults
- Isolated Infrastructure

**Cyber Resilience**
Requires short- and long-term retention capability;

- High snapshot frequency & fastest restores for short-term recovery
- RPO policy governed snapshot frequency for long-term retention and fast recovery

**Executive Summary – Percentage Achieved Per Category**
The graph in the table represents 15 categories that were measured by the assessment and (Client)'s percentage of each category achieved.




## Insights

Client has proven to have great understanding of the traditional systems and procedures. However, there is potential for improvement in the areas of cyber security and resilience. In addition, governance practices and documentation should be reviewed for currency. The following paragraphs summarize the most important categories IBM recommends analyzing deeper.

**Best Practices**
To improve this category, it is recommended to review the different frameworks and recommendations provided by entities like NIST. A lot of these recommendations do not require a solution and can be implemented through processes and procedures, for example separating the dev and prod environments, cycling/expiring passwords, increasing their complexity requirements, among others.

**Zero Trust**
For this category, we recommend implementing separation of duties for management of data project mechanisms and policy management, in other words leveraging separate admins for each data center. Additionally, we recommend implementing functionality where two actors are required to perform destructive actions, this could be permission based. Lastly, ensure that the security team has visibility into the organization's Shadow and Sanctioned IT.

**Run Books**
This can be improved by implementing, managing and updating Recovery Plans (Incident Recovery and Disaster Recovery) as well as Response Plans (Incident Response, Business Continuity, and Cyber Resiliency).We also recommend to update these to

include new ransomware Best Practices. IBM recommends reviewing those specifically related to Cyber Resiliency. Widely spread ransomware attacks can lead to significant business impact and requires solid and tested recovery procedures to re-establish the most critical business processes (known as the Minimum Viable Company).

**Threat Intelligence**
For this category, we recommend receiving threat intel through information sharing forums and sources. Additionally, we recommend leveraging a SIEM tool in order to do audit logging and keep track of log activity. We also recommend creating or improving the Intelligence Collection Plan to include SANDAs (Sources and Agencies which are used in the Intelligence Collection Plan.

**Efficiency**
To improve efficiency we recommend leveraging a tool that allows you to view your storage system's capacity, performance, and historical data. Additionally, consider automating some parts of the backup and restore processes as well as testing those backups and restores to ensure they work and that the process is as smooth as it can be. We also recommend integrating your storage platform and tooling with your SIEM and SOC for early threat detection.

**Financial Impact**
For improved financial impact reports we suggest updating your HW and SW inventories by prioritizing the assets by criticality. It is also a good best practice to understand how the likelihood of threats and vulnerabilities in the environment could impact your business. If there is not a program currently in place, we suggest implementing a risk quantification and vulnerability management program to enhance cybersecurity posture. Lastly, we suggest calculating outage cost for both HW and applications as a good KPI for criticality. This cost metric can be later used to calculate a threshold of when to declare DR and move to an alternate site.

**Procedure**
Procedures need to be well defined and documented and should be included in response and recovery plans. A well-defined set of procedures can help enterprises with more coordinated and purpose-built actions for protection, response, remediation, and recovery.

**Documentation**
A lot of processes are in place, but they lack documentation. It is imperative that enterprises document occurrences, procedures, and processes. It is also important to maintain the documentation up to date and apply updates as timely as possible.

**DR Planning**
For this category, we recommend reviewing expected recovery times for various outage periods, better defining RPOs and RTOs. Lastly, consider setting up a sandbox/testing environment where you can test restores or restore in the event of an incent to check for corruption and malware before restoring to production.

**Testing**
This can be improved by testing the backups and restores. These tests should be done often, and surprise tests should pe part of these activities. Additionally, we recommend conducting mass restore tests to simulate a ransomware recovery event. Lastly, the Incident Response, Business Continuity and other Plans should be tested and updated periodically.

Implementing simple best practices and having deeper conversations in specific areas can improve CLIENT's overall resiliency against cyber incidents.

# Recommended Initiatives

**Table 1 - List of Major Initiatives** highlights a prioritized list of major projects that IBM recommends be done to increase the overall resilience of your environment. Any or all these items may be addressed as per the risk appetite and budgetary constraints. The Rank on the tables following starts at 1 (Critical to protect the environment) and ends at 5 (Non- Critical / Efficiency recommendation)

| Rank | Major Recommendations |
|---|---|
| 1 | Consider leveraging or expanding encryption at rest (project planned) |
| 1 | Consider leveraging Backups that are protected with immutability capabilities |
| 1 | Have a process to identify and protect “Good copy” of backup images |
| 2 | Consider leveraging Snapshots and protecting them |
| 2 | Separate duties for management of data project mechanisms and policy management (separation of admins per data center) |
| 2 | Monitor deduplication and compression rates for unexpected changes |
| 2 | Detect unauthorized encrypted traffic |
| 3 | Implement functionality where “Destructive” actions require 2 actors (Zero-Trust) |
| 3 | Monitor and perform data masking / obfuscation of non-production data (project planned) |
| 3 | Review and monitor historical backup performance |
| 3 | Monitor and validate virtual Machine block change rate |
| 4 | Separate Data backup encryption and key management from enterprise encryption and key management (project planned) |
| 4 | Implement and manage ‘Intelligence Collection Plan’ (ICP) |
| 4 | Conducted mass restore tests to simulate a ransomware recover |
| 4 | Consider leveraging an Incident Response retainer for that team to assist in the event of an incident |
| 5 | Review expected recovery times for various outage periods |

**Table 2 List of Minor Initiatives: High Priority** highlights a prioritized list of minor projects that IBM recommends be done to increase the value of the solutions and functionality already in your environment. This list includes projects that the client is currently participating in but could use some enhancements. Any or all these items may be addressed as per the risk appetite and budgetary constraints.

| Rank | Minor Recommendations |
|---|---|
| 1 | Ensure what, where and how to recover is known by the appropriate party |
| 2 | Separate the development and testing environment(s) from the production environment |
| 3 | Establish and manage a baseline of network operations and expected data flows for users and systems |
| 5 | Consider implementing self-service policies (efficiency) |
| 5 | Consider implementing automated recovery processes |
| 5 | Determine, assess, and manage granularity of restore |

**Table 3 - List of Minor Initiatives: Medium Priority**

| Rank | Minor Recommendations |
|---|---|
| 1 | Detect malicious code |
| 2 | Determine and assess Maximum Tolerable Downtime (MTD) |
| 2 | Execute recovery plan during or after incident |
| 3 | Implement and maintain email anti-spoof technologies (SPF, DKIM, DMARC) (project planned) |
| 3 | Test response and recovery plans |
| 3 | Maintain adequate capacity to ensure availability is maintained |
| 3 | Analyze backup data for corruption and malware prior to restoring to production |
| 4 | Manage Backup data and traffic to utilize isolated networks |
| 4 | Leverage Enterprise key management practices for regular key rotation (project planned) |
| 4 | Implement a business continuity plan that accounts for Ransomware events |

**Table 4 - List of Minor Initiatives: Low Priority**

| Rank | Minor Recommendations |
|---|---|
| 1 | Implement a Logical “Air gap” to protect data |
| 1 | Determine restore processes (off/on site) |
| 1 | Monitor personnel activity to detect potential events (after hours logging, multiple login attempts, etc.) |
| 1 | Contain incidents (Have systems, procedures, and functionality to do so) |
| 1 | Test restores periodically |
| 2 | Authenticate users, devices, and other assets (e.g., single-factor, multi-factor) |
| 3 | Prioritize resources (e.g., hardware, devices, data, time, and software) based on their classification, criticality, and business value |
| 3 | Establish and map dependencies and critical functions for delivery of critical services |
| 3 | Review backup, encryption, and retention policies for data sets in the environment that require additional consideration |
| 3 | Quantify Impact of systems that may be degraded or have data unavailable |
| 3 | Ensure third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities |
| 4 | Establish resilience requirements to support delivery of critical services for all operating states (e.g. under duress/attack, during recovery) |
| 5 | Consider leveraging “Single pane of glass” management for storage |

# Summary

The client's current cyber resiliency posture with an overall score of 4,48 is significantly below average when compared with other organizations supported by IBM in their industry.

Client needs to invest heavily in their security strategy, processes, and tools. They should continue to integrate more tightly, the Disaster recovery, Business Continuity, Governance, and Security functions to encourage collaboration.

Client should improve the adoption of controls and practices. Most of the improvements will be in reviewing cyber incident specific response plans, improving efficiency, and continuous data validation ('golden copy'). The most critical recommendation for enterprise sized environments is to provide appropriate personnel in the primary as well as the disaster recovery site that would be able to perform mass recovery or site switch after a major incident. Immutable copies should be introduced throughout the various data services, especially for protecting data supporting Client's critical business processes, and leveraging existing data services to establish alternate target environments for data analysis or restoration procedures. To handle an incident which would require a mass restore, such recovery procedures should be regularly tested. Today, RTO/RPO/retention targets specific to cyber incidents are not in place. However, in a large enterprise environment financial impact of such events can be contained by doing so.

The client centers are available for round table discussions, workshops, product briefings, futures. There are a handful of topics that may be of interest as it relates to this environment:

- End-to-end cyber / data resiliency workshop to review options for immutability, data flow for primary and secondary workloads, clean room data validation / 'golden copy' , automation & orchestration
- Round table discussion for data protection / monitoring
- Spectrum Protect hardening round table/workshop for securing the backup environment from internal & external threats.
- Insights Pro monitoring workshop for establishing real-time anomaly detection capabilities.
- Vulnerability assessment/threat hunt to uncover potential threats.
- SOC Maturity Assessment
- Zero Trust / X-Force Cyberrange workshops (simulated attacks)
- Custom workshop/topics (leverage SMEs for discussions, brainstorming, Q&A) can be planned based on the client's interests and our recommendations.

Additionally, we recommend implementing the different best practice recommendations highlighted on the Major and Minor Recommendation Tables in order of importance.

Of course, IBM would like to partner with CLIENT and assist with the journey to a more resilient environment.

1. IBM – X-Force Threat Intelligence Index 2022
2. Verizon – 2019 Data Breach Investigations Report
3. Ponemon Institute – The Evolving Role of CISOs and their Importance to the Business
4. NIST – NIST Cybersecurity Framework
5. Harvard Business School – Six Sigma Meets the Service Economy - Six Sigma: It's Not Just for Manufacturing
6. Security Intelligence – What is Threat Modeling and How does it Impact Application Security
7. IOT for All – The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History
8. NIST – Developing Cyber Resilient Systems: A Systems Security Engineering Approach
9. IBM Red Hat – What is DevSecOps?
10. CSO Online – Will your backups protect you against ransomware?
11. Security Exchange Commission – Guidance on Public Company Cybersecurity Disclosures
12. Harvard Business School – CFOs Don't Worry Enough About Cyber Risk



IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
June 2022