

Security & Resilience Assessment Report

July 6, 2026

Transport Industry

Prepared by: **Firstname Lastname**, role
mail: firstname.lastname@ibm.com
phone: +99-123-456-789



Overview

This report presents the findings of the IBM® Security & Resilience Assessment, conducted in close collaboration with both the Storage and Security teams at Customer. The assessment highlights existing strengths in systems and processes that support visibility into operational events and provide the foundation for coordinated security and resilience efforts—ensuring alignment with business continuity objectives.

The assessment is grounded in industry-recognized frameworks, primarily the NIST Cybersecurity Framework (CSF) and the EU Digital Operational Resilience Act (DORA). By evaluating the current state of operational security, cybersecurity, and resilience, this report delivers targeted recommendations aimed at enhancing the value of existing solutions, supporting recovery time objectives (RTO) and recovery point objectives (RPO), and improving Customer’s alignment with these standards.

In addition, the assessment identifies opportunities to leverage existing technologies more effectively - accelerating return on investment and improving operational efficiency. Incremental improvements based on the recommendations provided can help reduce errors, increase consistency, and strengthen overall resilience.

This high-level assessment serves as a strategic starting point for identifying key strengths, weaknesses, and gaps. It provides a foundation for prioritizing future initiatives and guiding Customer toward a more mature and resilient cybersecurity posture.

Executive summary

Based on insights gathered from the assessment responses, Customer demonstrates a mature cyber resilience posture overall, with an aggregate maturity score of 8.47. Strong governance, risk identification, protection, detection, and response capabilities are in place and well embedded across the organization. These strengths significantly reduce the likelihood and impact of cyber incidents across Customer's transport and logistics operations.

Business leadership at Customer clearly recognizes that cyber resilience is a foundational requirement for business continuity, operational reliability, and regulatory compliance in a highly interconnected and time-critical industry. Cybersecurity risk management is treated as a business risk, supported by defined accountability, established processes, and consistent executive oversight.

The primary opportunity for improvement lies in recovery-related capabilities, which currently sit at a practicing maturity level. Enhancing recovery assurance, automation, and large-scale recovery readiness would further strengthen Customer's ability to withstand and rapidly recover from ransomware or destructive cyber events.

Governance

Customer demonstrates a strong and effective governance model. Cybersecurity roles, responsibilities, and decision-making authorities are clearly defined, actively enforced, and supported by senior leadership. Cyber risks are integrated into broader enterprise risk management processes, enabling informed prioritization and accountability. Supply-chain risk management is present but would benefit from deeper operationalization across third-party relationships.

Identify

Capabilities to identify assets, dependencies, risks, and potential business impacts are well established and mature. Customer has comprehensive visibility into

infrastructure, applications, and critical services, supported by structured risk assessments. Opportunities remain to further quantify financial impacts of outages at system and application levels to enhance decision-making during crisis situations.

Protect

Protective controls are consistently applied and well maintained. Strong identity and access management practices, security awareness training, encryption, logical and physical air gaps, and immutable backups collectively provide a robust defense against cyber threats. Data security practices are effective, though greater maturity in enterprise key management and separation of administrative duties would further reduce insider and lateral-movement risks.

Detect

Detection capabilities are a clear strength. Customer leverages extensive monitoring, anomaly detection, and event correlation across infrastructure, endpoints, and storage layers. Detection processes are well defined, tested, and continuously improved, enabling timely identification of both active and latent threats.

Respond

Incident response capabilities are mature and operationalized. Roles, procedures, and communications mechanisms are clearly defined, and analytical depth during incidents is strong. Continued focus on cross-team orchestration and automation will help reduce dependency on manual coordination during high-pressure events.

Recover

Recovery is the least mature capability relative to other domains. While key elements such as validated recovery points, clean recovery environments, and recovery communications are in place, recovery testing, automation, and mass-recovery preparedness are not yet consistently executed. Advancing these areas will materially improve confidence in Customer's ability to restore services quickly and safely following a severe cyber incident.

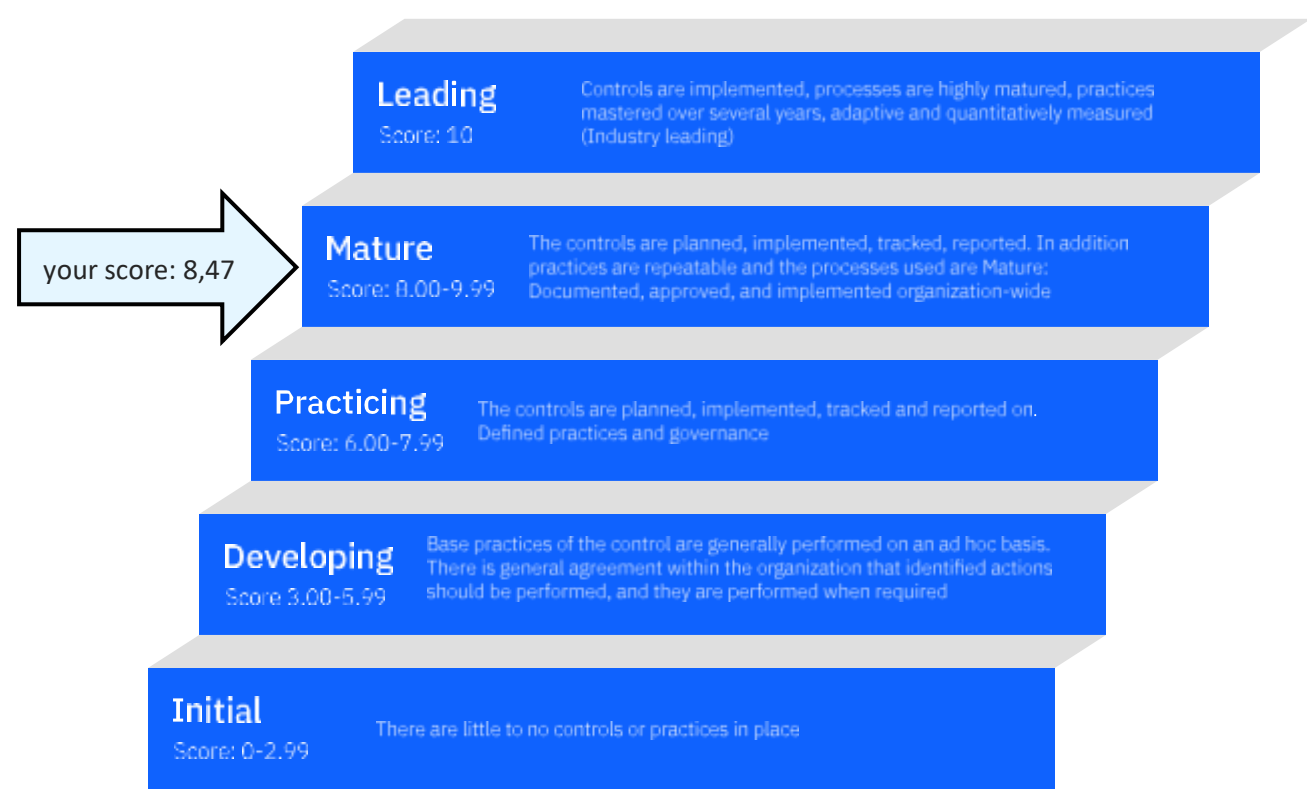
Operational security and cyber resilience must be recognized as dynamic, continuously evolving disciplines that demand ongoing assessment and enhancement. As the threat landscape expands and becomes increasingly complex, it is essential for organizations to regularly evaluate their current posture and define clear paths for advancement.

The Recommendations section at the end of the document outlines a strategic roadmap designed to strengthen critical capabilities, maximize the value of cybersecurity investments, and support the adoption of industry best practices. By establishing a mature and proactive approach to operational security and resilience, organizations can better safeguard their environments and ensure long-term business continuity.

IBM also recommends reviewing the following reports which are updated every year based on the latest information from the market and our customers:

- [X-Force Threat Intelligence Index](#)
- [Cost of a Data Breach Report](#)
- [What is Ransomware?](#)

Overall Maturity Score



Assessment Background Information

Purpose and Framework Alignment

The IBM Security and Resilience Assessment serves as a structured approach to evaluate Customer’s current cybersecurity and resilience posture. It identifies strengths, gaps, and opportunities for improvement by benchmarking against recognized best practices and regulatory frameworks, including the NIST Cybersecurity Framework (CSF) and the EU Digital Operational Resilience Act (DORA). This assessment is particularly focused on storage and security domains, helping to uncover blind spots and prioritize actionable enhancements.

In addition to NIST and DORA, the assessment references a range of globally recognized standards and frameworks such as ISO/IEC, COBIT, ISA, and the Center for Internet Security (CIS), ensuring a comprehensive and industry-aligned evaluation.

Maturity Level Definition

The maturity levels illustrated in the graph above provide a visual reference for interpreting assessment results. These levels are consistently used throughout the report to contextualize findings and align recommendations with the organization’s current and target maturity states.

Value summary dashboard

Executive Summary – Summary View

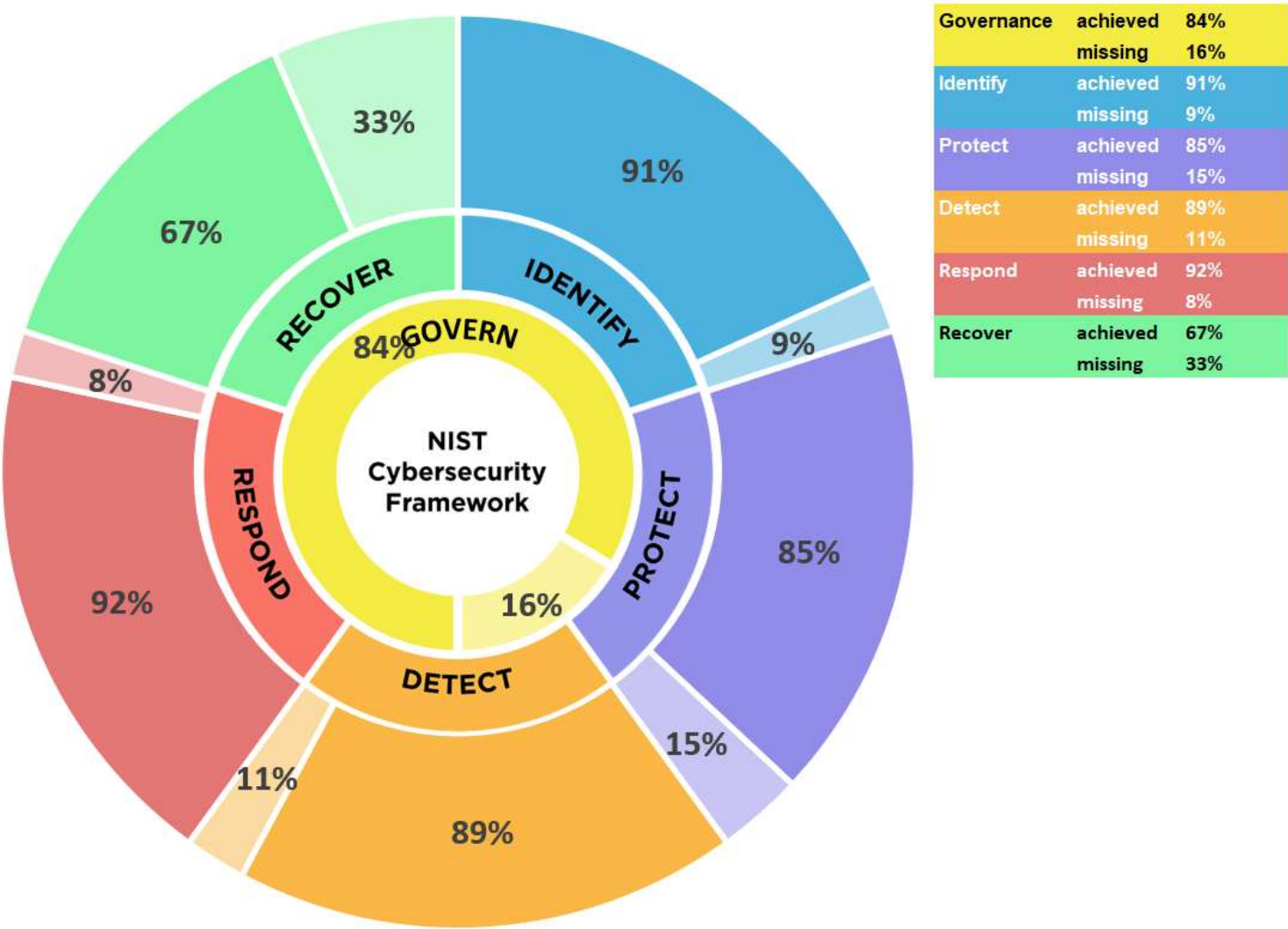
The numbers in the table reference the current overall maturity level on each of the assessment's categories. Since every control has its own weight, the category scores do not necessarily equal the average of the subcategory scores.

	Your score	Maturity Level
Total score	8,47	Mature
Governance	 8,35	Mature
Organisational Context	8,21	Mature
Risk Management Strategy	9,38	Mature
Roles, Responsibilities, and Authorities	8,86	Mature
Cyber Security Risk Management	7,62	Practicing
Identify	 9,09	Mature
Asset Management	9,83	Mature
Business Environment	9,20	Mature
Risk Assessment	9,29	Mature
Risk Management Strategy	8,27	Mature
Protect	 8,48	Mature
Identity Management, Authentication and Access Control	9,42	Mature
Awareness Training	9,07	Mature
Data Security / Protective Technology	7,50	Practicing
Information Protection Processes and Procedures	8,40	Mature
Maintenance	10,00	Leading
Detect	 8,91	Mature
Anomalies and Events	10,00	Leading
Security Continuous Monitoring	7,83	Practicing
Detection Processes	9,89	Mature
Respond	 9,17	Mature
Response Planning	8,09	Mature
Response Communications	7,50	Practicing
Analysis	9,82	Mature
Mitigation	10,00	Leading
Improvements	10,00	Leading
Recover	 6,71	Practicing
Recovery	6,09	Practicing
Recovery Planning	6,86	Practicing
Recovery Improvements	10,00	Leading
Recovery Communications	8,89	Mature

Executive Summary:

Achievement Level of Main Categories

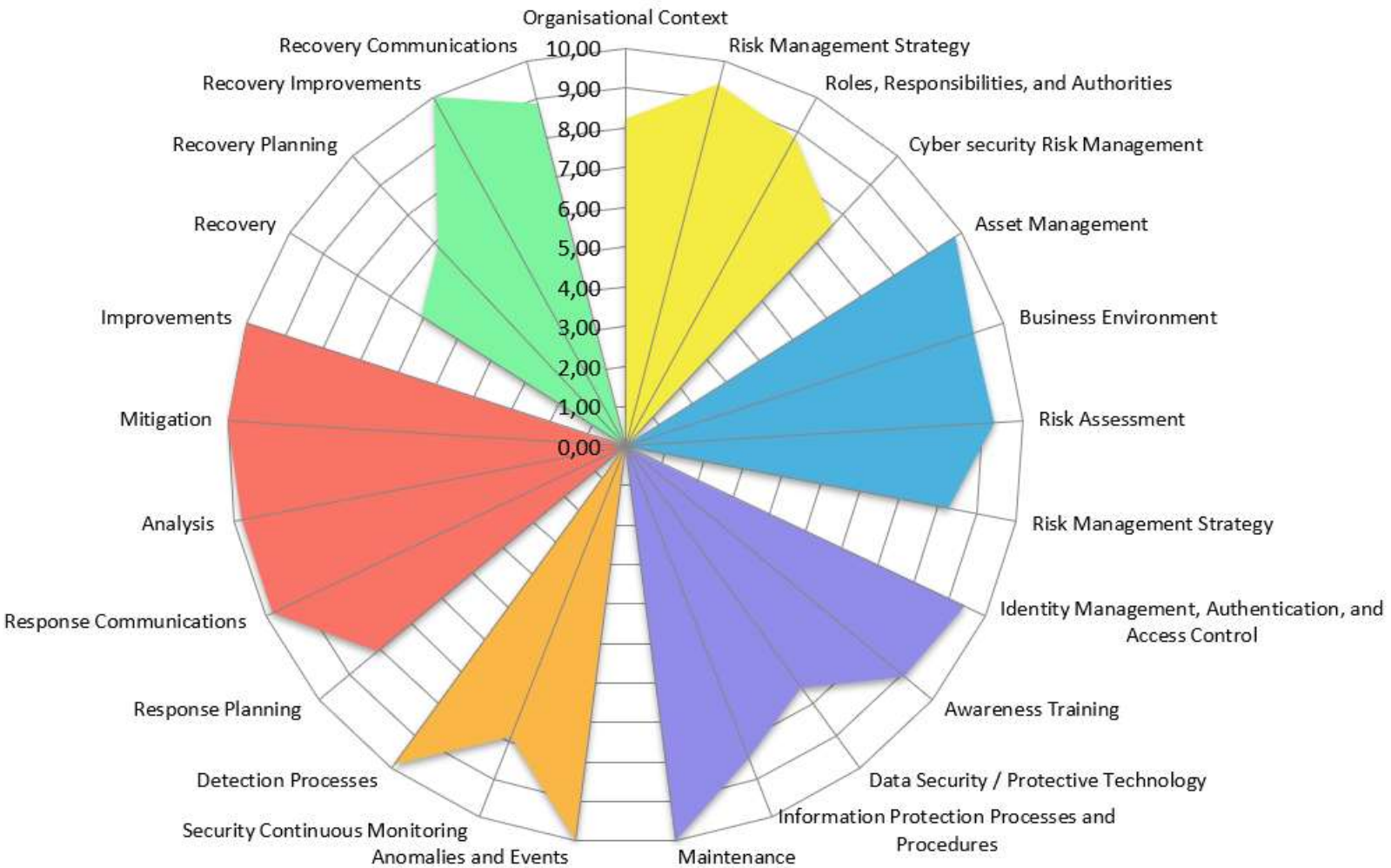
The progress chart below outlines the level of achievement on each of the assessment’s categories and opportunities to improve.



Executive Summary:

Maturity Level Graphics

The spider chart below references the current detailed maturity level scores on each of the assessment’s subcategories. An outside peak shows a good assessment result. Wherever there is a peak towards the middle of the chart there is room for improvement.

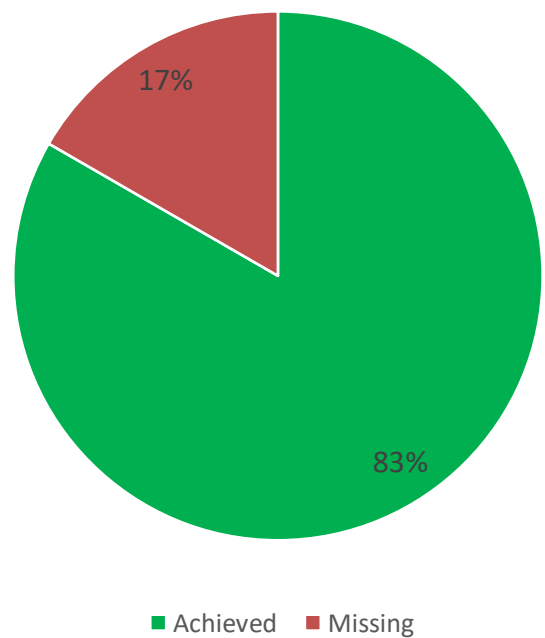


Executive Summary:

Ransomware % Achieved

The pie chart below represents a percentage of ransomware related questions within the assessment based on Customer’s answers. Ideally, we want to see a 100% Achieved Score.

Ransomware Readiness Percentage



Insights

This chart illustrates Customer’s current level of ransomware readiness, highlighting progress made toward building a resilient environment. While a portion of the readiness target has been achieved, the remaining gap underscores significant opportunities for improvement. To strengthen defenses and ensure rapid recovery in the event of an attack, we recommend implementing additional resilience measures such as a fully realized physical or logical air-gap, immutability solutions, retention sets, and isolated local vaults. These enhancements can substantially reduce risk and improve recovery confidence.

From a detection standpoint, we advise implementing **real-time anomaly detection** alongside monitoring key indicators such as **virtual machine block change rates, compression ratios, and deduplication patterns**. These capabilities can help identify unusual or sudden changes that may indicate ransomware activity, enabling faster response and containment. Real-time analytics can significantly reduce dwell time by alerting teams to

suspicious behavior as it occurs. Additionally, regular threat hunting and assessments - leveraging existing Endpoint Detection and Response (EDR) technologies - can further enhance early detection and situational awareness.

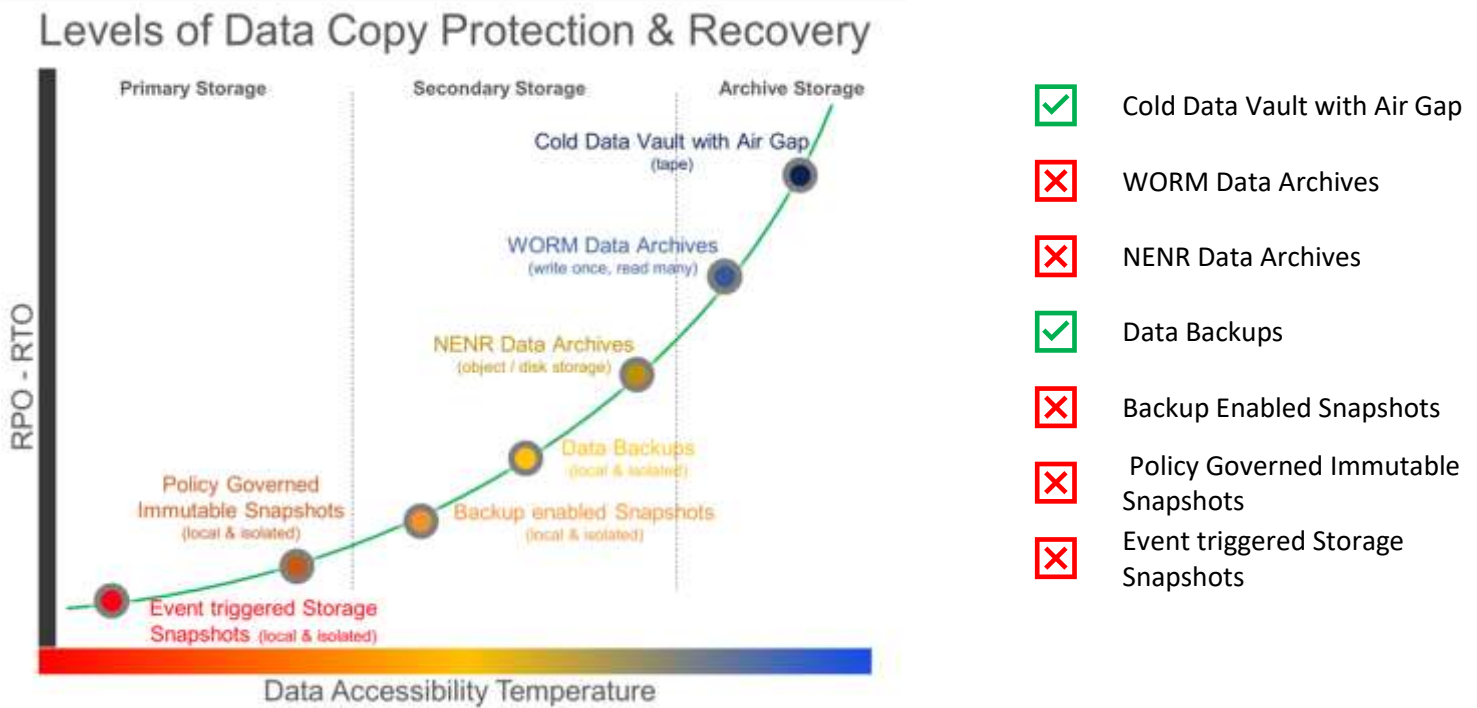
In addition, adopting simple but effective best practices can significantly improve ransomware readiness. For example, during recovery, restoring data into an **alternate environment** before transitioning to production helps validate data integrity and avoid reintroducing compromised files.

Finally, we recommend reviewing and updating all relevant response and recovery plans, including **Incident Response, Business Continuity, Cyber Resilience, Incident Recovery, and Disaster Recovery**—to ensure they incorporate current ransomware-specific scenarios and procedures.

Executive Summary:

Levels of Data Copy Protection & Recovery

The graph below shows different layers of protection at the storage level that help meeting meet different RPO and RTO targets based on Data Accessibility Temperatures. The items with checkmarks are currently being leveraged by Customer. 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:

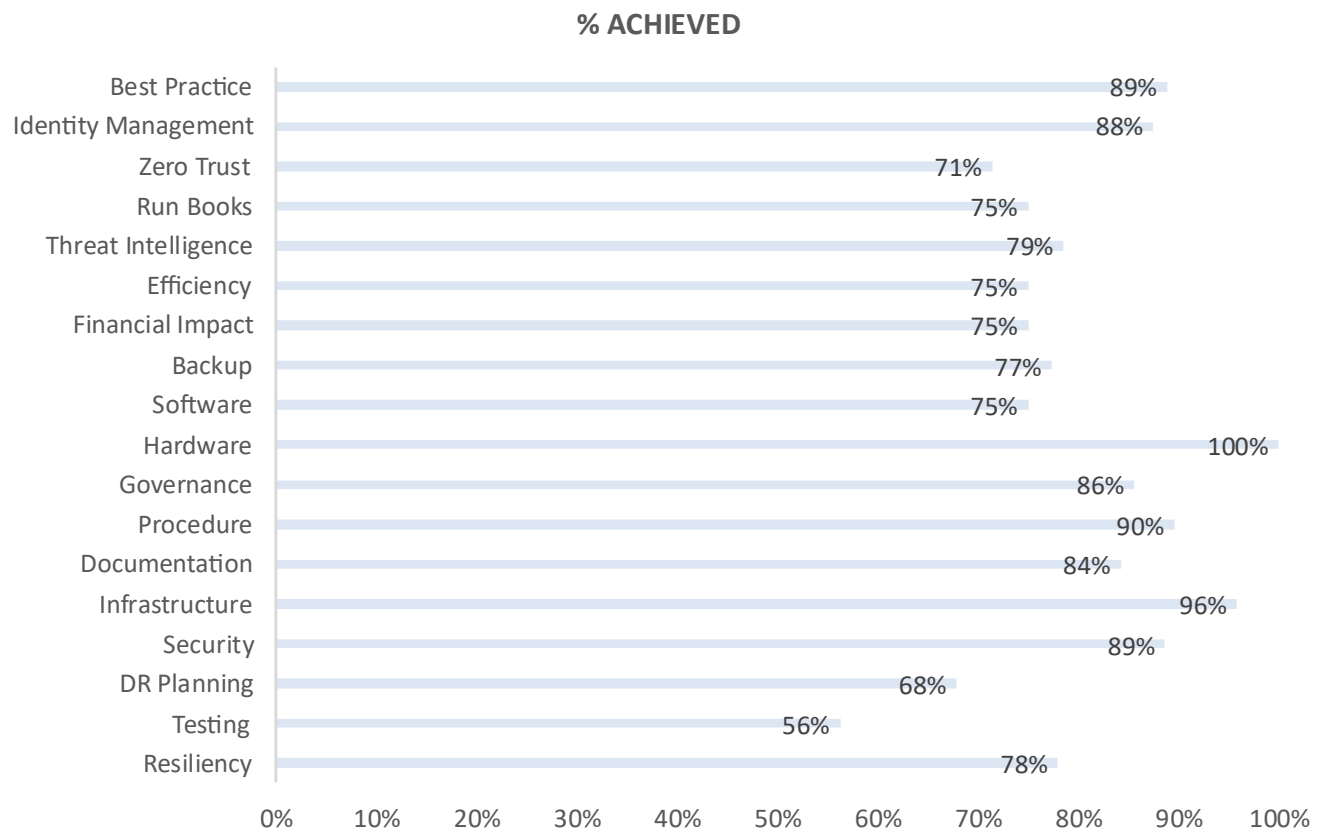
- High snapshot frequency & fastest restores for short-term recovery
- RPO policy governed snapshot frequency for long-term retention and fast recovery

Executive Summary:

Cross Category Analysis

Percentage Achieved Per Category

The graph in the table represents 18 categories that are measured by the assessment and Customer’s percentage of each category achieved.



Insights

Customer 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.

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.

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 incident to check for corruption and malware before restoring to production.

Testing

Recovery testing should be a BAU activity, especially for critical business services. These tests should be done regularly, and surprise tests should be 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.

Resiliency

This can be improved by updating and identifying roles and responsibilities. (Who does what during certain major events, i.e., during ransomware attack, site disaster, DDoS). We also recommend building a template sandbox/test environment for the purpose of mass restore exercises or in case there needs to be a restore after an attack. Lastly, consider implementing some form of airgap or immutability technology.

End-to-end Immutability

To protect critical data against ransomware attacks IBM recommends leveraging immutable copies. For primary workloads, most storage systems, including NAS-based file storage or S3 object storage, offer immutable snapshots that can be reverted within seconds or minutes. Secondary workloads can be protected using immutable or air-gapped backup copies e.g., on physical tape, or cloud-based services. For both kinds of workloads, it is essential to perform periodic data validation to ensure that data copies are consistent, corruption-free, and not affected by malware.

Anomaly detection

Most malware is attempting to compromise data, and the backup infrastructure is a primary target for malicious actors. Real-time detection of anomalies on primary storage, along with continuous data validation in primary and backup storage, will ensure earliest response to such threats, and provide safe recovery in the case of data corruption.

End point protection

End-user devices must as well be protected against threats and vulnerabilities. While virus scanning is a well-established standard, capabilities to block end points from accessing internal networks upon any suspicious behavior are essential for end-to-end security.

Quantum-safe Encryption

As quantum computing advances, traditional encryption methods are becoming increasingly vulnerable, making it essential for businesses to adopt a long-term plan for quantum-safe encryption. This proactive approach not only protects sensitive data against future threats but also ensures regulatory compliance, builds customer trust, and positions organizations as leaders in cybersecurity—ultimately saving costs and avoiding disruption in the long run.

Container and cloud workloads

These new technologies may impose new vulnerabilities and entry points for cyber-attacks. They require the same level of protection like traditional, on-premises workloads. While a compromised container can easily be deleted and restarted, such environment requires good protection of their code source repositories and secrets. For cloud workloads it is important to understand vulnerabilities within the provider's environment, and their capabilities for enterprise-level data protection and immutability.

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

Recommended Initiatives - Table 1: Immediate Priority

This table highlights the major projects that IBM recommends be done as soon as possible to reduce the most significant risks and increase the overall resilience of your organization. Any or all these items may be addressed as per 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)

Immediate Priority

	Rank	Recommendation
Protect	2	Separate duties for management of data project mechanisms and policy management (separation of admins per data center)
	3	Implement functionality where “destructive” actions require 2 actors (Zero Trust, dual admin, quorum, two person integrity checking - TPI, command approval, volume protection)
	3	Monitor and perform data masking / obfuscation of non-production data
	4	Leverage enterprise key management practices for regular key rotation
	5	Consider implementing self-service policies (efficiency)
Detect	2	Monitor deduplication and compression rates for unexpected changes
	3	Monitor and validate virtual machine block change rate
Respond	3	Consider cross training and dual-rolling each role within the Respond capability
Recover	2	Establish a periodic process to identify valid copies or for latent threat detection
	2	Establish a plan to periodically conduct mass workload recovery testing
	3	Define and implement a process to identify and protect “Good copy” of backup images
	3	Test and execute business continuity and disaster recovery plans
	5	Consider implementing automated recovery processes
	5	Review expected recovery times for various outage periods

Recommended Initiatives - Table 2: Important Priority

This table highlights a prioritized list of additional 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 risk appetite and budgetary constraints.

Important Priority

	Rank	Recommendation
Identify	4	Quantify cost of system outage per system
	4	Quantify cost of application outage per application
Protect	1	Investigate about quantum-safe encryption technology and begin planning a phased transition towards quantum-safe solutions
	2	Review standard SaaS provider data protection policies and align with business guidelines for data protection, retention, and recovery.

Recommended Initiatives - Table 3: Medium-term Priority

Medium-term Priorities

	Rank	Recommendation
Governance	2	Develop the cybersecurity supply chain risk management program, including a plan for implementation and improvement of the program, and share the policies and procedures with the organizational stakeholders
	2	Evaluate third parties' evidence of compliance with contractual cybersecurity requirements, such as self-attestations, warranties, certifications, and other artifacts
Identify	4	Establish, document, and manage risk management processes
	5	Consider leveraging "Single pane of glass" management for storage, and / or recovery of applications
	5	Conduct response planning, recovery planning, and testing with suppliers and third-party providers
Protect	2	Align data classification information from security with data protection policies including restore and cloning restrictions at the backup layer
	3	Ensure third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities
	3	Test response and recovery plans
Detect	1	Detect malicious code
	2	Leverage anomaly / data corruption detection for active threats on storage snapshots and or backups
Respond	3	Implement cross silo coordinated runbooks and / or tooling e.g. SOAR
	3	Ensure personnel know their roles and order of operations when a response is needed
	4	Manage and update ransomware event playbook
	5	Implement and manage response Plans (Incident Response, Business Continuity, and Cyber Resiliency) and Recovery Plans (Incident Recovery and Disaster Recovery)
Recover	1	Test restores periodically
	1	Implement and manage recovery plans (Incident Recovery and Disaster Recovery)
	4	Consider leveraging an Incident Response Retainer for that team to assist in the event of an incident

Recommended Initiatives - Table 4 - Low Priority

Long-term Priorities

	Rank	Recommendation
Governance	2	Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority
	3	Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders
	3	Determine communication plan to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals
Identify	2	Assess and determine cloud-based workload data to be backed up, and establish a process for revalidation
	2	Determine, assess and update Recovery Point Objective (RPO) and consider implementing by system/application
	2	Determine, assess, and update Recovery Time Objective (RTO) and consider implementing by system/application
	2	Determine and assess Maximum Tolerable Downtime (MTD)
	3	Establish and map dependencies and critical functions for delivery of critical services
	4	Establish resilience requirements to support delivery of minimum viable company
	4	Identify and document potential business impacts and likelihoods
	4	Use threats, vulnerabilities, likelihoods, and impacts to determine risk
Protect	2	Consider leveraging snapshots and protecting them
Detect	4	Continuously improve detection processes
Respond	3	Be prepared to take copies of corrupted environments for legal or forensic investigation without impacting recovery or production
Recover	2	Ensured that recovery won't cause follow-on problems (recover to testing/sandbox environment prior to restoring to production)
	2	Execute recovery plan during or after incident

Summary

With an overall cyber resilience maturity score of **8.47**, Customer performs well above average and exhibits a strong, business-aligned cybersecurity foundation. Governance, identification, protection, detection, and response capabilities are largely mature and reflect a well-integrated approach to managing cyber risk across critical transport and logistics services.

To strengthen its posture, Customer should prioritize tighter integration between **Disaster Recovery, Business Continuity, Governance, and Security** functions. This alignment will foster greater collaboration and ensure a unified approach to resilience planning and execution.

The most significant opportunity for improvement is in **end-to-end recovery assurance**. While recovery planning and tooling exist, recovery execution relies heavily on manual processes and limited large-scale testing. This introduces uncertainty in scenarios involving widespread corruption, ransomware, or multi-system failure.

To further strengthen resilience, Customer should prioritize:

- Establishing **continuous data validation** practices, including the identification and protection of trusted recovery points.
- Increasing the frequency and realism of **recovery and mass-recovery testing**, including restore operations into isolated environments before returning to production.
- Expanding **automation and orchestration** across recovery workflows to reduce recovery time and human error.
- Further refining **financial impact quantification** for systems and applications to support faster, risk-based recovery decisions.

As part of a forward-looking security strategy, Customer should also begin evaluating and adopting **quantum-safe encryption** technologies. These are essential to protect sensitive data against future threats posed by quantum computing and to ensure long-term data confidentiality and compliance with evolving regulatory expectations.

By addressing these areas, Customer can transition recovery capabilities from practicing to mature, aligning them with its otherwise strong cyber resilience posture and reinforcing confidence with customers, regulators, and business stakeholders.

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 Customer and assist with the journey to a more resilient environment.

Next Steps

The IBM Client Engineering team and the IBM client centers are available for Proof-of-Experience (PoX) workshops, round table discussions, MVP development, product briefings and demonstrations, future roadmaps. IBM proposes the following activities to continue your journey towards a fully cyber resilient organization:

Data protection: implement safeguarded and immutable copies

Strengthen ransomware resilience by implementing safeguarded, immutable data copies aligned with Customer's existing storage environment.

What we would do together

- Review the current environment and define target workloads for safeguarded copy implementation.
- Design retention policies and immutability settings aligned with business and regulatory requirements.
- Configure safeguarded copies and integrate them with existing backup and recovery processes.
- Execute controlled recovery tests to validate integrity and recovery performance.

Expected outcome after this initiative:

- Protection against data deletion, encryption, and unauthorized modification.
- Improved recovery reliability through trusted, immutable restore points.
- Reduced exposure to ransomware-related data loss scenarios.
- Clear validation of operational readiness and scalability.

Contact:

Firstname Lastname, role
mail: firstname.lastname@ibm.com
phone: +99-123-456-789

Cyber resilience: conduct an IBM Storage Defender pilot including a clean-room environment

Conduct a joint pilot of concept with Customer's storage team to validate advanced detection, response, and recovery capabilities of IBM Storage Defender, including a clean-room recovery environment.

What we would do together

- Define pilot scope, objectives, and success criteria across detection and recovery capabilities.
- Select 2-3 representative workloads and data sets for realistic validation scenarios.
- Deploy and configure Defender capabilities in a controlled pilot setup.
- Design and establish a clean-room environment for isolated recovery and validation testing.
- Execute end-to-end scenarios, including anomaly detection, ransomware simulation, and clean-room recovery.
- Review results jointly and define next steps for operational integration and scale-out.

Expected outcome after the pilot:

- Validated detection and response capabilities for modern cyber threats.
- Proven ability to recover critical workloads in an isolated and secure clean-room environment.
- Improved collaboration between infrastructure, storage, and security teams.
- Clear understanding of integration requirements and operational impact.
- Evidence-based roadmap for scaling cyber resilience capabilities across the environment.

Contact:

Firstname Lastname, role
mail: firstname.lastname@ibm.com
phone: +99-123-456-789

1. IBM - [X-Force Threat Intelligence Index](#)
2. IBM – [Cost of a Data Breach Report](#)
3. Verizon - [Data Breach Investigations Report](#)
4. Ponemon Institute – [The Evolving Role of CISOs and their Importance to the Business](#)
5. NIST - [NIST Cybersecurity Framework](#)
6. Harvard Business School - [Six Sigma Meets the Service Economy - Six Sigma: It's Not Just for Manufacturing](#)
7. Security Intelligence – [Vulnerability management, its impact and threat modeling methodologies](#)
8. NIST - [Developing Cyber Resilient Systems: A Systems Security Engineering Approach](#)
9. IBM Red Hat - [What is DevSecOps?](#)
10. Security Exchange Commission - [Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#)
11. Harvard Business School [Cyber Risk Is Growing. Here's How Companies Can Keep Up](#)
12. European Banking Authority - [Guidelines on ICT and security risk management](#)
13. European Securities and Markets Authority - [ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification](#)

© Copyright IBM Corporation 2024

IBM Corporation
New Orchard
Road Armonk,
NY 10504

Produced in the
United States of America
July 2026

IBM, the IBM logo, ibm.com, QRadar, and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Microsoft and Active Directory are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The results of this tool are based on the client's subjective responses to questions and statements and help to highlight the strengths, weaknesses, and any gaps in the client's environment. The tool is provided for illustrative purposes to help the client determine whether to consider IBM solutions. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided. Results from the tool should not be relied upon, are not a guarantee or commitment regarding any potential or actual results and may not be incorporated into any contract or quote, used, relied upon, disseminated, or reproduced for any purposes.

This assessment was conducted at a specific date and show the environment's maturity up to that point. Changes in the environment are to be expected and have not been considered in this report. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result

in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

