Data Resilience is a Business Imperative for Today's Enterprise

The Veeam Data Resilience Maturity Model guides organizations on a path to lower risk

What and Why:
Data Resilience Maturity Model

As organizations continued to pursue improved data resilience back in 2024, there was a common misconception by senior leadership that their organizations were already well above average in the efficacy of their people, processes, and technologies. Seeing this mindset as a concerning trend, Veeam organized a consortium of industry experts to quantify where organizations are at large and provide a consensus of recommendations for how enterprises can mature towards improved data resilience. This survey revealed that nearly three-fourths of organizations aren't ready to respond to outages. This level of overconfidence resulted in organizations underestimating their actual resilience, leaving them vulnerable.

The Veeam Data Resilience Maturity Model (DRMM) seeks to give organizations the information necessary to help enable them to **recover from disruptions, optimize their resources, and ensure operational continuity.** While data resilience was once looked at as a function of backup alone, traditional backup strategies are insufficient in the face of evolving cyberthreats, regulatory pressures, and the increasing complexity of data ecosystems. Achieving **true data resilience** requires a structured, cross-functional approach that integrates **IT, security, and compliance efforts** into a cohesive strategy.

Most organizations are overconfident in their data resilience.

30%+

of organizations believe they are more resilient than their actual benchmarked capabilities

74%

have data recovery risk exposure

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

The Blueprint for Data Protection

The Veeam Data Resilience Maturity Model provides an empirical framework for organizations to assess their current resilience posture, identify gaps, and implement targeted improvements. Veeam developed the DRMM in collaboration with McKinsey, Palo Alto Networks, and Splunk, and informed by insights from over 500 C-level executives. Findings indicate that 74% of enterprises are not utilizing even half of the best practices identified by resilience research, resulting in heightened financial, operational, and compliance risks. The DRMM provides a structured approach for aligning business and technology strategies, improving risk management, and enhancing recovery capabilities at scale. By leveraging this model, organizations can move from reactive crisis responses to proactive resilience, ensuring that data remains an enabler of growth rather than a point of failure.

Research findings show that top performers generally experience:

7x
faster recovery speed (MTTR)

4x
less data loss (RPO)

3x
Less downtime (RTO)

~10%
higher average revenue growth rate

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Model Dimensions

When Veeam set out to develop the DRMM, it sought the foremost experts in operational efficiency. McKinsey & Company led the effort to create a rigorous, vendor-agnostic framework. This model was designed to assess an organization's ability to ensure data resilience across three core dimensions.

Strategy: Aligning Business and Risk

A clear data strategy integrates **business goals with resilience planning**, ensuring organizations can anticipate threats, enforce governance, and maintain compliance.

People & Process: Empowering Resilience Through Alignment and Action

True resilience is driven by empowered teams and standardized execution. By investing in skilled talent, aligned leadership, and clear cross-functional protocols, organizations can respond decisively in moments of disruption. Defined workflows and governance ensure continuity, while collaboration and training enable teams to adapt and recover with speed and confidence.

Technology: The Backbone of Ensuring Resilience

Technology supports resilience across six key areas:

- **Backup:** Secure protection of data that's located on-premises or across clouds.
- **Recovery:** Agile restoration of critical systems, even at scale.
- **Architecture & Portability:** Scalability across heterogeneous and often hybrid environments.
- **Security:** Prevention and anticipated remediation against cyberthreats.
- **Reporting & Intelligence:** Real-time visibility and insights to support compliance, improve recovery, and optimize operations.

By integrating **strategy, people, process, and technology,** organizations can **reduce risk, accelerate recovery, and strengthen long-term resilience.**

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

The Four Horizons of Data Resilience Maturity

Using survey data across the core categories — strategy, people, process and six supporting technology disciplines (backup, recovery, architecture, security, reporting, and intelligence), the DRMM helps organizations evaluate their ability to ensure their IT-reliant business processes are resilient. This assessment places organizations within one of four horizons in each vector (and overall), reflecting their level of resilience maturity as well as opportunities to improve:

Basic

Reveals a basic foundation with significant opportunities for improvement.

Intermediate

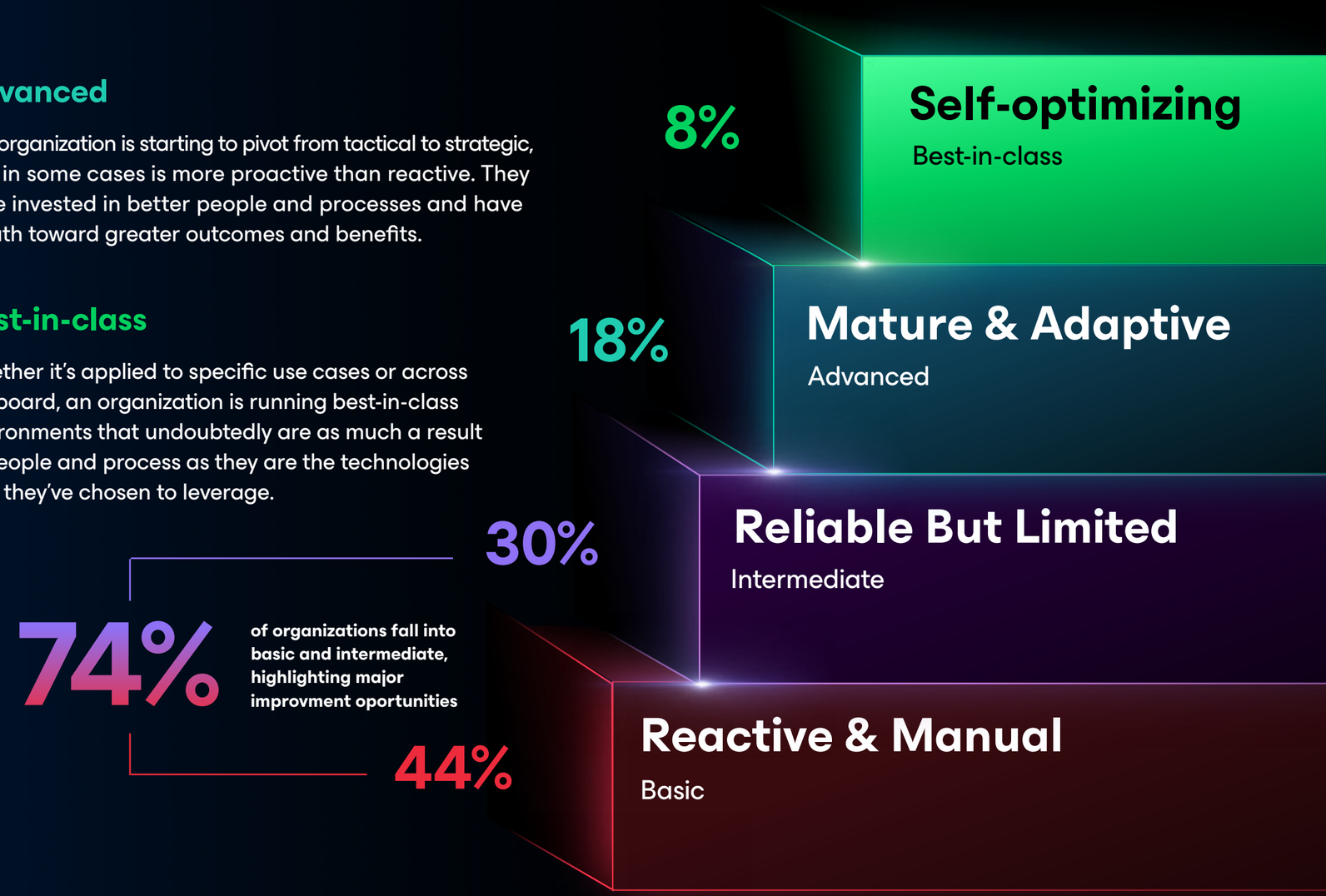
An organization is performing above the minimum, but likely with mostly manual processes or ad-hoc augmentations. There is still much that can be improved upon, but the organization may lack awareness about what is possible and what's worth doing.

Advanced

The organization is starting to pivot from tactical to strategic, and in some cases is more proactive than reactive. They have invested in better people and processes and have a path toward greater outcomes and benefits.

Best-in-class

Whether it's applied to specific use cases or across the board, an organization is running best-in-class environments that undoubtedly are as much a result of people and process as they are the technologies that they've chosen to leverage.



© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Key Benefits of DRMM

Using an industry-centric model that is grounded in independent research can prove to be very useful for organizations who are looking to assess and strengthen their data resiliency posture. Some of the benefits of the maturity model include:

Revenue protection

Strengthening commercial feasibility and competitive defense by responding to market needs and delivering reliable products.

Cost optimization

Minimizing inefficiencies, IT expenses, and incident costs by optimizing operations, infrastructure, and risk management.

Compliance and risk management

Reducing legal, regulatory, and business risks by minimizing cyber incidents, data loss, and associated costs.

Brand integrity and consumer trust

Protecting reputation and customer confidence through reliability, availability, and strong market positioning.

Proof Point

Global Bank improves revenue protection through improved resilience

One global bank that followed recommendations from the maturity model gained the following benefits:

99.99%

Uptime for critical applications

ZERO

Cybersecurity-related outages over the last three years

$300K

In savings per outage due to reducing MTTR for critical IT systems

Learn more about real-world Veeam customer success stories here.

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Moving "Up and to the Right" In Data Resilience Maturity

After the DRMM reveals the state of an organization's resilience, it also prescribes the methods and benefits of moving to the right versus the ramifications of staying where they are. At this point, it's time to look at implementing the steps necessary to move between horizons by taking a closer look at KPIs and other performance metrics to give some insight into company performance.

Strategy

For a data resilience strategy to be effective, organizations should ask how aligned the people (leaders and teams), processes (internal and external), and myriad technologies are to achieve desired outcomes.

People & Process

- Have senior leadership and board members been enabled to oversee and mandate risk resilience and data management?
- Are functional teams identified for each of the technology areas and aligned to the overall processes and strategy of data resilience?
- Is leadership mandating teams to be on standby in order to execute objective, integrated planning, tabletops, and real-world preparedness?

Technology

- Does the data backup architecture ensure comprehensive protection across the heterogeneous enterprise and achieve immutability and policy adherence?
- Do the data recovery technologies enable agile recoveries from heterogeneous protection and production environments to alternative platforms at scale?
- How inclusive are the backup and security technologies in ensuring effective resilience across heterogeneous hybrid clouds, including the accommodation for workload portability across the enterprise?
- **Data security:** Do the data security technologies integrate with backup and recovery in such a way that proactive resilience or proactive prevention and reactive resilience are aligned within policies and teams?
- Do the data reporting technologies provide adequate visibility, proactive prevention, and governance?

  Is data intelligence integrated with and accelerating all technology stacks within the data resilience model?

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

A Prescriptive Approach for Driving Continuous Improvement

The DRMM is grounded in concepts that some leaders inherently agree with, but surprisingly few organizations embrace these ideas in their core strategy and processes.

Don't panic, prepare

Don't start in the datacenter; start in the conference room. The key to most organizations' improvements in resilience often hinges on including more people (e.g., stakeholders and implementers) and implementing better processes. Some good next steps to take on the way to up-leveling an organization would include the implementation of processes and practices that are proactive beyond foundational basics.

Who else should join the table?

As mentioned above, data resilience is bigger than "just IT", and therefore, organizations should be rallying a larger number of stakeholders alongside the CIO and CISO. By significantly broadening the types of senior stakeholders who have a vested interest in the company's data resilience, like chief risk officers and chief data officers, a company can gather a broader assessment from different angles. This ensures that resulting strategies are inclusive of needs across the organization, thus helping to ensure the support needed to move toward better resilience.

Aligning data strategy, people, process, and technology

Once all the different stakeholders are in the room, the DRMM is a way to get them introduced to each other and working together. During these DRMM working sessions, many teams discover that they are working in silos and that some people at the same company are either doing complimentary or counterproductive work in other departments. So, by bringing all these different points of view together in one room with a common goal, organizations can get a full understanding of the reality of their situation and be better prepared to move between horizons.

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

From Foundation to Revolution:
Advancing Your Organization's Data Resilience

Resilience isn't a one-time initiative — it's a continuum of maturity that requires organizations to assess their data strategy, people, process, and technology holistically. Whether you're establishing foundational practices, optimizing existing workflows, or pushing the boundaries of innovation, here's how to take the next step.

Foundation

Build the Core Framework for Resilience

- Define a clear data resilience strategy with dedicated leadership and measurable goals.
- Establish incident and change management processes that align security, IT, and data teams.
- Standardize backup, recovery, and security baselines to mitigate risk across critical systems.

Evolution

Expand Resilience Beyond Compliance into Proactive, Automated, and Scalable Operations

- Conduct annual business impact analyses to refine risk tolerance and track improvements.
- Implement cross-functional incident response training, including simulations and war-gaming.
- Automate data governance and recovery tracking to ensure policies are enforced across business units.

Revolution

Achieve Enterprise-Wide Resilience by Integrating Intelligence, Automation, and Strategic Leadership

- Appoint a chief resilience officer to drive a cohesive, business-aligned approach.
- Develop an end-to-end recovery strategy, including multi-cloud workload mobility and AI-driven risk assessment.
- Deploy real-time monitoring and predictive analytics to anticipate and prevent failures before they occur.

Every organization's journey will look different; some may need remedial efforts, while others are ready for advanced strategies. Where does your organization stand today, and how can you take the next step?

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

How Veeam Can Help

Veeam was the championing vendor who brought in McKinsey & Partners, as well as experts from the IT industry, to develop the DRMM. The DRMM provides prescriptive guidance on how companies can improve their data resilience, focusing on additional capabilities that would improve an organization's resilience. Those recommendations are vendor-agnostic due to the original nature of the model. To help, Veeam can provide specific recommendations from its portfolio of products and services that align to the prescriptive guidance found in the DRMM. Please contact your Veeam partner or Veeam account team to learn more.

For more information about Veeam enteprise solutions [click here.]

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it.

Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam.

Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.