The Disaster Recovery Maturity Framework

A guide for understanding and improving your company's resiliency

AXCIENT™
Beyond Backup™

www.axcient.com

Climbing The Recovery Maturity Curve

Businesses are critically reliant upon IT systems, which can inflict significant financial harm when they go down. The potential causes of downtime include lost or corrupted files, application failure due to a software virus, server hardware malfunction, temporary power outage, or a natural disaster that takes out an entire facility.

For decades, IT managers have protected their infrastructures using a combination of preventive measures (e.g., backup power systems, off-site data storage, antivirus software) and recovery and restoration activities (e.g., redundant hardware and networks) to bring IT systems back to normal operation as quickly as possible. As companies grow and update their IT infrastructure, different tactics are employed to ensure the critical systems and applications used to run the business are always available. Such tactics are based on business needs, budget, size of the IT department, regulatory requirements, and more. Seldom will two companies in the same industry and of the same size will have the same disaster recovery architecture, as it relates to the technology, their DR plans, and processes.

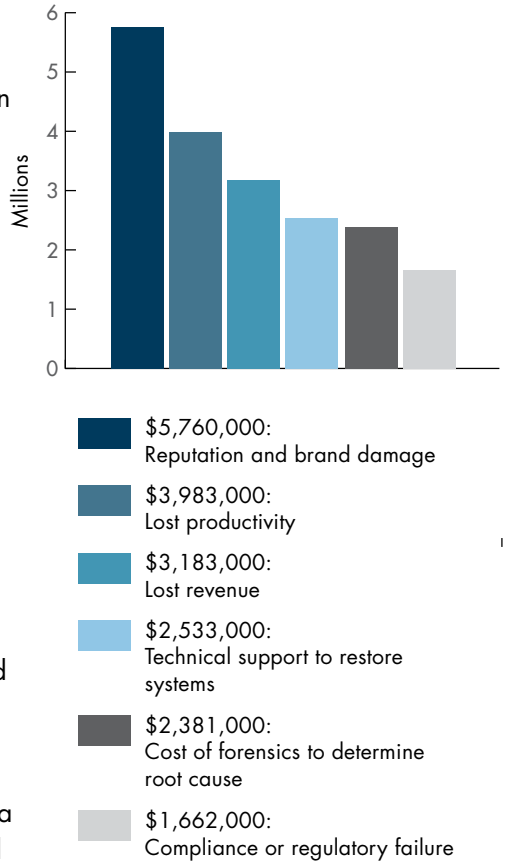
The Cost of Downtime for SMBs

Each year businesses in North America lose $26.5 billion due to IT downtime. For small and medium-sized businesses (SMBs) with less than 1,000 employees, downtime costs $12,500 per day. These financial losses are attributable to multiple factors:

- Inability to generate revenue while data or systems remain unavailable
- Falling out of compliance with contractual commitments or regulatory requirements
- Damage to the company reputation because IT systems were unavailable
- Customer defections due to brand damage

Even worse, downtime can be fatal for a small business. A firm suffering a major data loss has a 70% likelihood of going under within a year ; businesses that survive find it difficult, if not impossible, to regain the market share they previously enjoyed.

FINANCIAL IMPACT BY COST CATEGORY

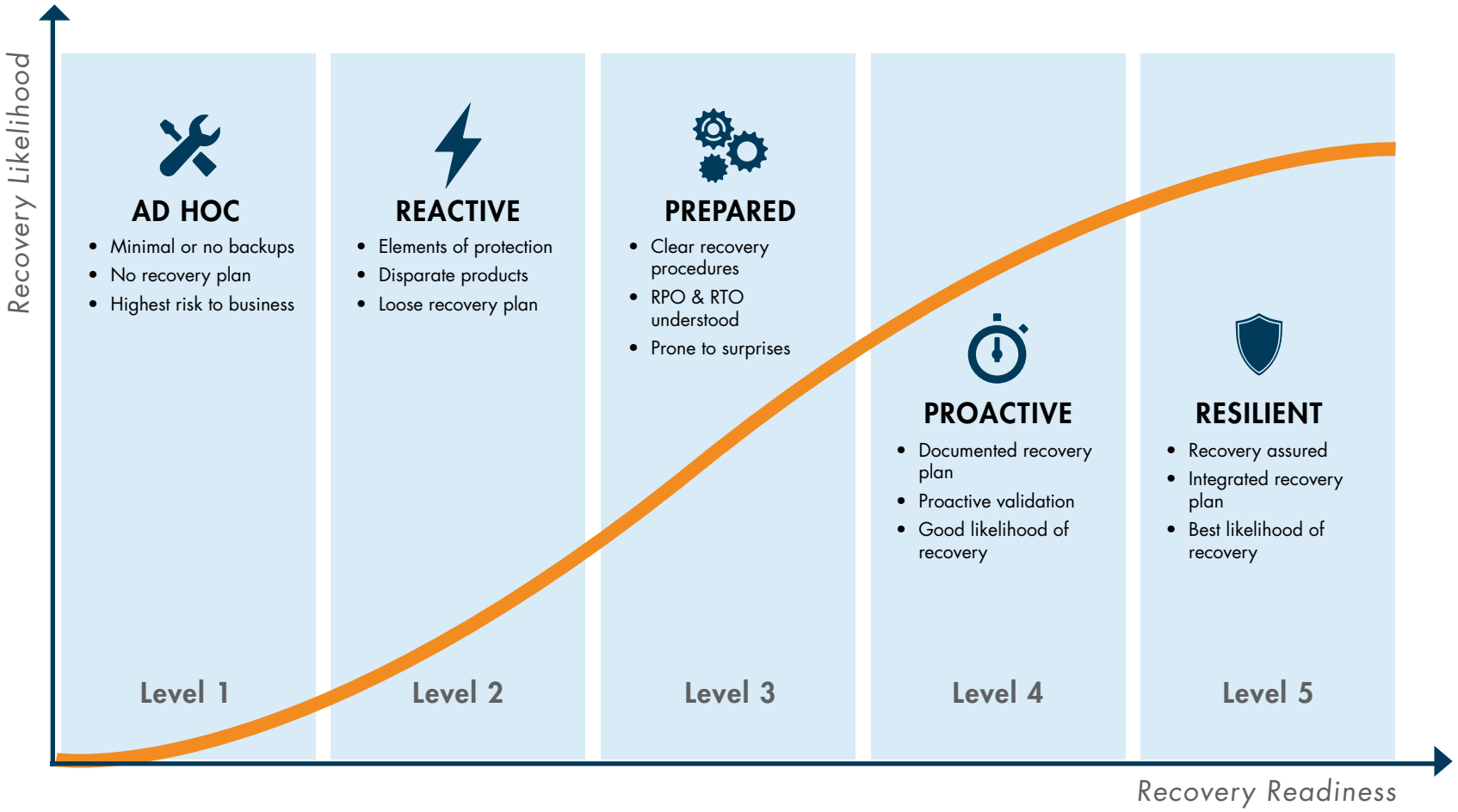


Source: IBM Global Study of the Economic Impact of IT Risk

Recovery Maturity Curve

To avoid these consequences, it's essential for a business to implement a plan that enables rapid recovery from application downtime. Each business has unique needs and tolerance for risk, which factors into how prepared an organization is for dealing with an unexpected outage. Astonishingly, 57% of small businesses don't have a disaster recovery plan in place and only 23% back up their critical data on a daily basis .

A company's state of recovery readiness can be illustrated by a maturity curve, as shown below.



The Recovery Maturity Curve depicts five levels representing an organization's ability to rapidly get its business back up and earning:

LEVEL 1: AD HOC

Almost nothing is being done to ensure readiness to recover from an outage. Occasional backups may be run by various folks, but recovery is completely ad hoc. The absence of a recovery plan means any event causing downtime will trigger a scramble to try and figure out how to recover. This is how many organizations address the issue of IT recovery. Even documenting a few critical technical and business recovery procedures would be a big help, but most organizations don't take the time for this. A key concern is that there may be little or no senior management support for such an activity, although senior managers will certainly have plenty of questions if their systems suddenly go down.

THE DISASTER RECOVERY MATURITY CURVE

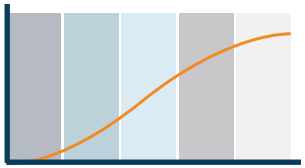
LEVEL 2: REACTIVE

Elements of protection are in place, which may include scheduled local backups, remote copying of data for disaster recovery, and possibly server failover mechanisms for business continuity. These are usually implemented using disparate products that incur overhead charges that are expensive to deploy and manage. Recovery planning consists of loosely sketched guidelines or is completely reactive, which decreases the likelihood of smooth recovery from an outage. Lack of documentation of emergency recovery procedures is also a big concern, and the simple act of writing down specific procedures is often a major step forward in improving the ability to recover.

A common example where Level 2 falls short is a corrupted application database for which a recent backup doesn't exist. After recovering an old version of the database, productivity suffers as the database is manually repopulated from paper records or other data sources.

Another example is the need to save money on the department budget, so the acquisition of certain systems, such as backup power or a backup server, may be deferred or not pursued.

THE DISASTER RECOVERY MATURITY CURVE



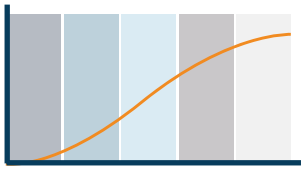
LEVEL 3: PREPARED

The organization is prepared by documenting a plan with clear recovery procedures. The plan is aligned with business needs in terms of recovery point and recovery time objectives (RPO and RTO). However, last minute heroics may be necessary to deal with surprises during a recovery operation.

A real life example where Level 3 had an unexpected wrinkle was with a business that dutifully backed up its server images to the cloud, as specified in its disaster recovery plan. However, due to an oversight in execution, a backup wasn't updated when one of the servers had been replaced. As a result, when Superstorm Sandy hit and the customer needed to virtualize its servers in the cloud, one server was incompatible with the others, resulting in on-the-fly attempts to solve the problem.

Another example emphasizes the need for periodic exercising of DR plans. An IT department was confident it had the skills and resources to recover a critical server. However, the exercise showed that changes in the server's configuration had been made, but the recovery plan had not been updated to reflect those changes. Naturally, the exercise was a failure.

THE DISASTER RECOVERY MATURITY CURVE



LEVEL 4: PROACTIVE

A recovery plan exists, as described in Level 3. In addition, proactive validation of the plan is performed by testing local recovery procedures and performing periodic disaster drills. Routinely exercising the recovery plan ensures the risk of missing an RTO is drastically minimized.

As emphasized in DR standards and good DR practice, DR plans and their associated elements are "living" documents that must be periodically reviewed and re-validated to ensure that they are consistent with the company's business objectives. Additionally, by reviewing and re-validating DR plans, businesses can provide assurance that they will be ready to use and accurately reflect the true state of the systems to be recovered.

THE DISASTER RECOVERY MATURITY CURVE

LEVEL 5: RESILIENT

A detailed recovery plan exists, it is fully integrated with business continuity plans that are also in place, and there is a fully organized disaster recovery program to provide administrative oversight on all activities associated with disaster recovery. Preventive measures to minimize the potential for threats have been established. Senior management of the organization fully endorses the importance of technology disaster recovery planning, and senior managers periodically attend plan exercises as observers. The organization has been able to achieve a state of resilience using a balanced configuration of resources that include on-site hardware and software, virtualized systems and storage, and either an advanced third-party managed services provider or a cloud-based disaster recovery provider. The organization is confident that virtually any incident can be addressed quickly, with minimal damage, and IT systems and business processes can be returned to normal production well within RTO and RPO limits.

Looking Deeper

The maturity levels described above speak to the overall state of readiness to recover from application downtime, whether due to loss of a single file, complete outage of a data center, or anything in between. A deeper understanding of an organization's recovery readiness can be gained by assessing a number of key factors:

IMPACT OF APPLICATION DOWNTIME

How severely would application downtime impact the business? At what point in time would the business begin to suffer without the availability of critical systems, databases, customer data or network resources? Beyond what point in time would the business be irreparably damaged following an extensive loss of IT resources?

RECOVERY TIME OBJECTIVE (RTO)

How much downtime can the business withstand? Is it minutes, hours, or days? RTOs must be identified for all mission-critical systems, networks, databases, and other IT resources. They are a key metric when preparing DR plans.

RECOVERY POINT OBJECTIVE (RPO)

This metric represents the amount of time data can "age" before it is no longer useful to the company. The shorter an RPO, the more critical the data. The backup process must be robust enough to replicate data in the shortest amount of time between the original and replicated copies.

PROTECTION ARCHITECTURE

Does the protection solution provide local recovery, cloud recovery, or both? Is the solution built from one or multiple products? Does the network infrastructure have sufficient resilience to support the protection architecture with diversely run circuits and sufficient bandwidth to handle normal and emergency traffic demands? Is the protection architecture scalable enough to support an out-of-normal situation where more resources are needed than are available?

PROTECTION SCOPE

Which IT assets are being protected? User files, databases, core applications, server images, IT infrastructure? Will all elements of the IT environment be available and operational during a disaster in a way that allows employees to securely connect and continue working?

DOCUMENTATION

Are recovery procedures fully documented and up to date? Are multiple copies of procedures available in hard copy and electronic versions? Will emergency teams have access to copies of plans in their cars or in their homes? Will collaborative resources such as SharePoint be available to securely store copies of plans? Will emergency teams have copies of DR plans on their smart phones? Will they be able to remotely access their plans using their smartphones?

TESTING SCOPE

Tests can be as simple as a tabletop walk-through of a plan. However, the amount of coverage when testing and validating recovery procedures is important. For example, are files simply spot-checked, are servers failed over, or is secondary infrastructure verified?, These tests are important to ensure that non-technical issues such as evacuation plans can be addressed, and that necessary financial arrangements and office supplies for a new work space can be ready when needed. More rigorous recovery testing of critical systems, data storage and networks is needed to ensure these critical assets can be recovered and returned to production status quickly.

TESTING FREQUENCY

How often are recovery procedures exercised? Experience has shown that a minimum of one test annually is a starting point for most IT systems, but for systems deemed mission-critical, it is advisable to test more frequently, especially if the critical systems have gone through a number of changes. DR plans need to reflect those changes, and this is where many plans fail: not keeping DR plans up to date with system changes.

ORGANIZATIONAL SPONSORSHIP

Is recovery readiness an IT project or a company-wide initiative? Does senior management of the company, and not just IT management, support the need for disaster recovery? Has management approved a budget for DR? Has the IT staff received training in DR procedures from equipment vendors and network service providers? Ideally, DR is set up as a specific function, with a dedicated staff; a budget; an ongoing schedule of activities that includes plan reviews; exercises; and staff training.

An honest assessment of these factors will help reveal where an organization falls on the Recovery Maturity Curve. (Check out the Axcient Recovery Readiness Scorecard for more information.)

Applying the DR factors described above to the maturity model, we obtain the following table, which maps the levels of support and commitment (below) to the five maturity model levels. Achieving Level 3 (Prepared) is an ideal goal for most organizations because it demonstrates an awareness of and commitment to key DR metrics, including RTO/RPO, documentation, testing and sponsorship. Aiming for Level 4 (Proactive) can be achieved by leveraging the unique services from cloud-based providers.

	Level 1: Ad Hoc	Level 2: Reactive	Level 3: Prepared	Level 4: Proactive	Level 5: Resilient
RTO/RPO	1	2	3	4	5
Protection Architecture	1	2	3	4	5
Protection Scope	1	2	3	4	5
Documentation	1	2	3	4	5
Testing Scope	1	2	3	4	5
Testing Frequency	1	2	3	3	5
Organizational Sponsorship	1	2	3	3	4

5 = Very high, 4 = High; 3 = Moderate; 2 = Low; 1 = Very Low

Is the difference between Level 3 and Level 4 worth the potential investment? Based on pricing models and capabilities available from cloud-based DR providers, as well as the ability to initiate recovery activities quickly and efficiently, the answer is "yes." Recovering your IT systems quickly using managed DR services or a self-service cloud provider (aka Recovery-as-a-Service) ensures that you can return to "business as usual" more quickly and are therefore more likely to reduce the financial and reputational losses your organization could sustain with a prolonged loss of IT resources. Moreover, if your disaster recovery strategy anticipates situations that may become threats and initiates measures to shield your organization, you can advance toward Level 5, a fully resilient infrastructure.

Traditional Strategies for Recovery

The principles of IT disaster recovery have been around for more than 40 years. The process of recovering IT resources following a disruptive event has traditionally taken many forms, mostly based on physical solutions. Traditional approaches include backing up data, databases and systems to on-premise tape or disk systems; backing up the same resources to off-site data storage facilities; or data replication using mirroring techniques to managed data recovery services. It is this last option – managed recovery – that provides significant promise to organizations of all sizes.

Recent developments in technology have made DR much more affordable, intuitive and available to companies almost anywhere. The emergence of cloud-based data backup and disaster recovery services provides new opportunities for IT departments to move up on the maturity curve. Users running traditional backup and recovery solutions may never rise above Level 2 maturity. Using managed services can speed up an organization's maturity simply by leveraging the resources of the managed service provider.

Improving Readiness with Recovery-as-a-Service (RaaS)

The historical impediment to climbing the recovery curve has been affordability. In other words, because traditional software and hardware solutions tend to be too costly to deploy and maintain, businesses are forced to accept the risk of potentially dire consequences due to an IT outage. Additional reasons for the inability to climb the recovery curve include the lack of management support, lack of sufficiently trained staff and a perceived lack of need (e.g., "We've never had an outage, so why bother with DR?").

With the emergence of Recovery-as-a-Service (RaaS), SMBs no longer need to settle for risky recovery practices. RaaS offers enterprise-class recovery-as-a-cloud service at a price point that's acceptable to even the smallest of businesses. This affords SMBs the opportunity to cost effectively move up the Recovery Maturity Curve. RaaS not only offers a proven solution for corporations, but also an opportunity for managed service providers (MSPs) to layer their best practices on top and deliver cloud-based recovery to their clients.

What really happens in a RaaS environment? First is the creation of a complete mirror image of the IT system you wish to protect. You can specify all or part of your IT environment, and there's no distinction between physical or virtual environments. Once images of all the IT systems you want backed up and ready for recovery have been created, you are ready to initiate recovery of those IT elements using a very simple Web-based process. Assuming the images created on the RaaS platform are current – and you can specify the level of RPO/RTO you wish for each IT element – you can access the most current version of the systems and data you need to recover. The loss of critical systems and data – and potentially the loss of business – is minimized because you can access literally an exact image of the production environment you were using when the incident occurred. Launching the transition from production to recovery environments is a very simple and secure process, much less cumbersome and complicated than traditional methods. RaaS gathers all the commands you need for a smooth failover and automates them so you can launch recovery from a smartphone, if necessary. Naturally, your DR plan will have many other issues that need to be addressed, but the ability to recover and restart mission-critical applications, databases and other resources quickly and efficiently is probably the most important objective of your DR plans. And now those recovery activities can be fully automated.

The notion of IT disaster recovery as taking hours and even days has become a thing of the past. Cloud-based DR solutions are rapidly becoming the norm in today's "need it now" business environment. Investing in a RaaS solution is not only an investment in intelligent protection and recovery, but also an investment in compliance with major industry standards (e.g., ISO 22301:2012, ISO 27031:2011, NFPA 1600:2013, NIST SP 800-34), legislation (e.g., HIPAA Security Rule and GLBA), regulations (e.g., NYSE Rule 446) and accepted good practice (e.g., the Business Continuity Institute's Good Practice Guidelines and FFIEC Business Continuity Handbook). RaaS can be a single stand-alone recovery strategy, or it can be part of a blended solution that optimizes both physical recovery assets and cloud-based solutions.

Summary

Availability and scalability of resources plus flexible pricing models have brought managed services into the mainstream of IT organizations. No longer is it considered risky to obtain DR services from specialized service providers. The value proposition – and the track record – of cloud-based services far outweigh the concerns among IT managers and technical staff. IT managers now have the option of building a blended configuration of recovery resources, using a combination of local systems enhanced by cloud-based services. Or they can opt for total cloud-based recoverability – not only for IT systems, but also for the entire company workplace.

If you're thinking perhaps it's still too soon to rely on the cloud for recovery, consider this: The global RaaS market was estimated at approximately $564 million in 2013 with a projected compound annual growth rate of 21% . Combining RaaS with a thoughtful recovery plan that's exercised routinely will ensure an SMB is prepared for the inevitable IT outage, be it due to something as simple as a corrupted file or as significant as a superstorm.

i "The Avoidable Cost of Downtime" report by Coleman Parkes Research Ltd.
ii "2011 SMB Disaster Preparedness Survey" by Applied Research
iii "Contingency Planning" report by Strategic Research Corp. and DTI/PricewaterhouseCoopers
iv "2011 SMB Disaster Preparedness Survey" by Applied Research
v "Critical Capabilities for Recovery as a Service" report by Gartner, Inc.

www.axcient.com

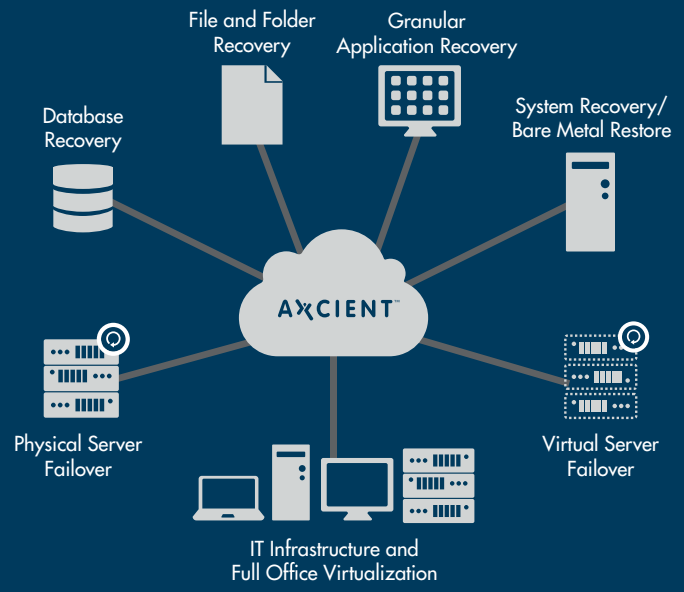
800-715-2339

@Axcient

linkedin.com/company/axcient

axcient.com/facebook

AXCIENT™
Beyond Backup™



The Axcient Solution

Axcient's Recovery-as-a-Service cloud eliminates data loss, keeps applications up and running, and makes sure that IT infrastructures never go down. Axcient replaces legacy backup, business continuity, disaster recovery and archiving products, with a single integrated platform that mirrors an entire business in the cloud, making it simple to restore data, failover applications, and virtualize servers or an entire office with a click. Thousands of businesses trust Axcient to keep their applications running and employees productive.
Learn more at www.axcient.com.