bluelock®

6 *Questions to Secure a Successful* DISASTER RECOVERY PLAN

Bluelock, LLC 5303 Lakeview Parkway South Dr, Indianapolis, IN 46268 888-402-2583 www.bluelock.com

IN THE HOT SEAT

When you're in the hot seat, will you have the answers to the questions your leadership is asking? Everyone at your company counts on the success of the disaster recovery (DR) plan when it's needed. When your C-level executives and Board of Directors ask about your company's DR plan, they want to be confident that the business will continue to be successful and secure, no matter what.

Be fully prepared for a conversation with your leadership team about your current continuity plan, and potentially, which gaps need to be filled. This will ensure proper buy-in, awareness, and therefore, adequate budgeting and coverage to ensure your plan will be successful. This guide will help you answer the most important questions about your DR plan. Just like in DR planning, preparation for this conversation is key to a successful outcome.

QUESTIONS COVERED

1. What is the economic risk if core applications go down for a day, a week or even longer?
2. What were the results of our latest full recovery test?
3. Is our disaster recovery data and site secure?
4. How are our applications currently protected and are they all protected the same way?
5. What will happen to our key data in the event of a disaster?
6. Against which types of disasters are we guarding?

#1 What is the economic risk if our core applications go down for one day, one week or even longer?

YOUR GOAL

Know the cost of downtime to the business. Understand the full impact of each type of outage and justify the need to guard against the varying possibilities.

HOW TO FIND THE ANSWER

Not every application has the same value to the organization. Some applications are revenue-generating, some are used for internal support and others are revenue-supporting. Work with the business to determine each application's value on a per-minute, per-hour and per-day basis so you can better communicate each application's economic risk.

If the application is used to process financial transactions, or it is an actual revenue-generating application itself, downtime is a direct hit to the company's bottom-line. If the application is not directly related to the bottom line, but supports a number of workers who will be unproductive without that application, you could need to send those workers home due to an application disruption, which is an added cost to the business.

Create an **Outage Impact Document** that lists your critical applications and the economic cost to the business for hourly, daily and extended outages. The document should include what the outage will cost the company as well as the large-scale impact on staffing, revenue and any potential long-term known and quantifiable damages. We have provided a template at the end of this document.

#2 What were the results of our latest full recovery test?

YOUR GOAL

Validate the effectiveness of your DR plan based on the results of a DR test. Be able to tell your business what type of test was run, what the results were and how you'll do things differently if you found errors in the process.

HOW TO FIND THE ANSWER

When investing in DR planning and technology, you are responsible for ensuring it works properly. A DR plan that is not tested and does not work when it's called upon is a waste of money for the business.

Not all organizations are equipped, or willing, to take on the risk and man-hours involved in executing tests, especially those that involve full failover and failbacks. Some solutions and vendors enable easier testing than others, so consider this as you evaluate your options.

Twice annual testing is the recommended test schedule for most applications. If your application changes significantly more than twice annually, that testing should be increased to coincide with the updates.

A documented recovery playbook and QA checklist can provide the final bit of confidence and auditable assurance that your DR solution will live up to the promises that you've made to the business and to your leadership.

> *"We were looking for a partner in our DR strategy and have found that with Bluelock. Their ability to handle complex environments and multiple tiers of recovery exceeded our expectations and, their Recovery Assurance program has given us confidence that we will be able to recovery when needed."*
>
> ***– David Walker, Vice President of IT, Walker Information***

#3 Is our disaster recovery data and site secure?

YOUR GOAL

Security needs in your production environment don't go away in recovery. Ensure your disaster recovery solution meets (or exceeds) your needs.

HOW TO FIND THE ANSWER

Thinking beyond tools and technologies for IT security allows you to better apply your top minds, resources and priorities for not only a more effective IT team, but a more effective business.

Establish where your production gaps and vulnerabilities lie. Do the same for your recovery environment and note the differences. If your recovery environment is designed to act as production when you need it the most, ask yourself if it should be any less secure than your production environment.

There are no shortcuts when it comes to securring your production and recovery environemnts. No provider can fully take away the burden of managing security and recovery, and it wouldn't be responsible for you to give up control entirely, either.

Look for partners and solutions that focus on the same things that are important to your business. Challenge your provider to tailor a solution to your needs rather than forcing your business into their rigid molds. The ideal solution should should address the security needs of your production environment and criticality of your data.

#4 How are our applications currently protected and are they all protected the same way?

YOUR GOAL

Identify which applications need the highest level of protection and which can withstand the lowest level of protection.

HOW TO FIND THE ANSWER

Critical applications that require a very quick Recovery Time Objective (RTO) and Recovery Point Objective (RPO) will require additional cost. Documenting why applications need to be protected at the higher or lower tier is critical to balancing risk and economics in your DR plan. Tiering your applications helps to explain that balance.

Sort your applications into a 4-level tiering structure. Tier 1 applications will require near instantaneous RTO and RPOs and may best be served with a high-availability solution. Tier 2 applications will have less aggressive requirements, for example requiring minutes-long RPOs and hours-long RTOs.

Tier 3 applications require 24-hour RPOs and RTOs between 24–48 hours. Tier 4 applications would be the minimum required, likely requiring 24-hour RPOs and RTOs of 48 hours or longer, depending on the scenario.

Use the included **Impact / Time Diagram** to help decide which applications belong in which tier, and map those tiers to the appropriate providers and technologies.

#5 What will happen to our key data in the event of a disaster?

YOUR GOAL

Sort applications in the tiering process based on the sensitivity and importance of the data within the applications to ensure the right protection for the data, as well as the application.

HOW TO FIND THE ANSWER

If your organization is concerned about data retention or the integrity of the data itself, those needs should be a separate consideration from the application.

Your solution should adequately secure your key data, but also provide for accessibility of resources like decryption keys and pass phrases that allow you to access encrypted backups. This will allow your team to access the important data even if the primary application is compromised and should remain a separate part of the DR plan from protecting the primary application itself.

When addressing the protection needs of your data it can shift your initial placement of the application in the tiering structure. Perhaps you placed an application in Tier 3 based on RTO and RPOs. If data retention is key to the success of the company, it justifies a higher spend on protecting it, and thus, a higher tier classification.

Higher tier solutions will provide more protection for your data. More robust Disaster Recovery-as-a-Service (DRaaS) solutions guard against data corruption by allowing a testing of the RPO and a rollback to an earlier copy of the data without losing critical transactions.

If corruption is not caught early enough it could be replicated to your DR site. For this reason, it is important to also have separate, offsite backups with long-term retention. Backup-based DRaaS can solve for this.

#6 Against which types of disasters are we guarding?

YOUR GOAL

Identify the types of disasters (geographic, infrastructure, human error, etc.) that you are guarding against at each tiered level.

HOW TO FIND THE ANSWER

Each tier of disaster protection needs to be qualified by the type of disaster and what could occur during that disaster. There are five types of disasters you should consider as a threat: application-level, infrastructure-level, datacenter-level, metro-level and regional-level. The relative geographic size of the disaster you choose to guard against will impact how far your recovery center is from your production center.

TYPES OF DISASTERS

Application Disasters – Exclusively impacts the application or applications.

Infrastructure Disasters – Impacts the infrastructure the application is hosted on and potentially the application.

Datacenter Disasters – Impacts the entire datacenter, infrastructure within the datacenter and likely the applications hosted within the datacenter.

Metro Disasters – Impacts more than just your datacenter and therefore your infrastructure and application, but also the metro area. This could include tornados that run a path miles-wide and long or brownouts impacting a grid.

Regional Disasters – Wide-spread disaster impacting an entire region and therefore multiple metropolitan areas. This could include hurricanes and floods.

Choosing a recovery site that is farther away is a balance between protection, latency and long-distance data replication. However, physical distance is the best way to guard against a regional-level threat like an ice storm or earthquake.

If you're excluding a regional failure from the protection of Tier 3 protected applications, that should be called out in the plan along with your justification. Choosing which types of disasters each tier should be protected against is also a balance of economics and likelihood of potential risks.

A Tier 1 application may have regional protection, whereas Tier 2 may only include metro-level protection with off-site tapes and a plan for restoration hardware and software as needed. It will increase your RTO for Tier 2, but it will save you money on your DR plan which you can use to better protect your Tier 1 applications.

Use the included **Likelihood of Occurence** matrix to help your leadership better understand which types of disasters are being protected against, and which are deemed an acceptable risk level.

COOL, CALM AND COLLECTED

Don't let your recovery plan fail due to lack of communication or organizational buy-in. A clear matrix of risk, recovery and expense is an ideal way to structure your DR conversation with your leadership team. Look at the following example of an outage impact document that represents an ideal way to structure the discussion with your leadership team to ensure a robust DR plan is in place to protect your business.

Once you've worked through the process, and the Outage Impact Document once, the plan isn't a closed book. Make going through this process with your team at least an annual activity in order to ensure your DR plan is updated and your valuable infrastructure and applications are adequately protected.

APPLICATION TIERS

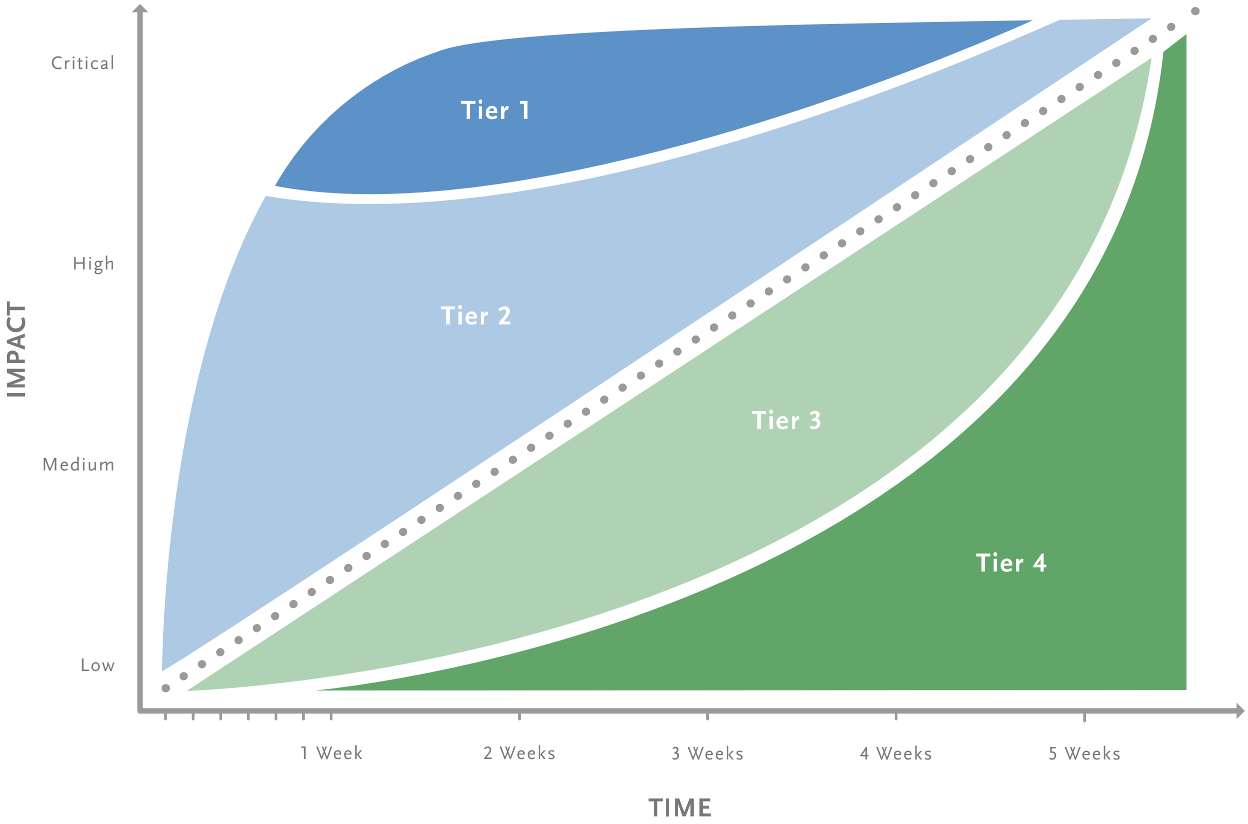
1. Tier 1 applications are the most critical, often requiring a high availability solution to ensure optimum uptime. Always-On DRaaS is ideal for this.
2. Tier 2 applications are business-critical, however they can withstand the risk of minimal downtime of minutes or hours. Replication-based DRaaS is an ideal fit for this.
3. Tier 3 applications may require 24-hour RPOs and RTOs between 24-48 hours, pointing to Backup-based DRaaS as their possible solution.
4. Tier 4 applications are the least critical, likely requiring 24-hour RPOs and RTOs of 48 hours or longer, depending on the scenario. Offsite tape backups are ideal for this tier.

IMPACT/TIME DIAGRAM

TIER YOUR APPLICATIONS

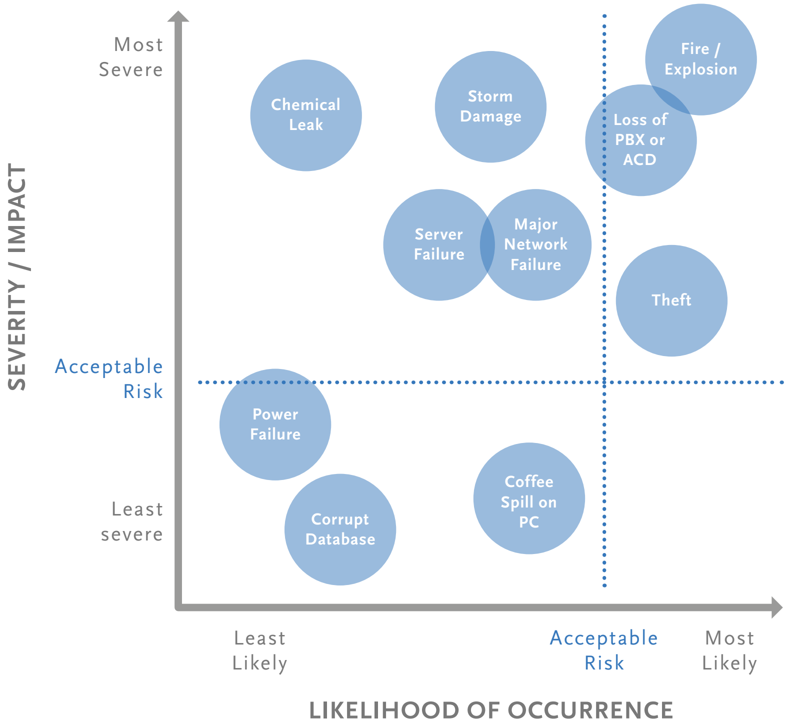
Classifying your applications will require working with various business units to help understand the criticality of each application to the business. There are a number of ways to classify which applications should be in which tier, but ultimately it comes down to the impact downtime would have on your business as a whole. Tier 1 and Tier 2 applications are most likely to have drastic impact on your revenue stream and critical business operations.

When meeting with other business units, it may be helpful to reference the following Impact/Time Diagram to help plot in which tier your application(s) should fall. Applications will land in one of the four following tiers based on their criticality and the amount of time they can withstand being down.

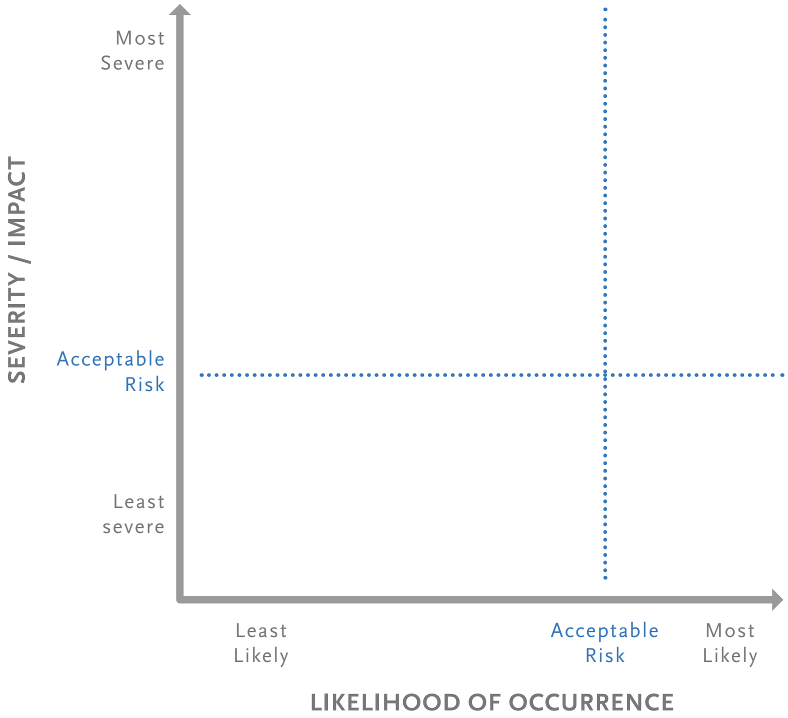


LIKELIHOOD OF OCCURRENCE MATRIX

EXAMPLE:



CREATE YOUR OWN:



OUTAGE IMPACT DOCUMENT

INSTRUCTIONS

This worksheet is designed to help you compare applications side-by-side based on their needs, requirements and unique risk qualities. Use the 6 Questions to Secure a Successful Disaster Recovery Plan guide to help you better understand the questions this worksheet asks about.

EXAMPLE APPLICATION: eCommerce App

Application Tier: *(select one)*

● Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): 10,000

Risk/Day ($): 240,000

Risk/Week ($): 2,000,000

Qualitative Impact:

Reputation loss in the market; reduced sales in the next few quarters.

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

High availability between two geographically disparate datacenters.

Data Sensitivity: *(select one)*

● Compliant ○ Standard

Disaster Protection: *(check all that apply)*

☑ Regional ☑ Infrastructure
☑ Metro ☑ Application-level
☑ Datacenter

Application Data:

Sales order information, credit card transactions, customer data and purchase history.

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

Live synchronous replication between datacenters via application replication.

APPLICATION NAME: ____________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ____________________

Risk/Day ($): ____________________

Risk/Week ($): ____________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional
□ Metro
□ Datacenter
□ Infrastructure
□ Application-level

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____

APPLICATION NAME: ____________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ____________________

Risk/Day ($): ____________________

Risk/Week ($): ____________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional
□ Metro
□ Datacenter
□ Infrastructure
□ Application-level

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____

APPLICATION NAME: ______________________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ______________________________

Risk/Day ($): ______________________________

Risk/Week ($): ______________________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional □ Infrastructure
□ Metro □ Application-level
□ Datacenter

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____

APPLICATION NAME: ______________________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ______________________________

Risk/Day ($): ______________________________

Risk/Week ($): ______________________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional □ Infrastructure
□ Metro □ Application-level
□ Datacenter

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____

APPLICATION NAME: ______________________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ______________________________

Risk/Day ($): ______________________________

Risk/Week ($): ______________________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional

□ Metro

□ Datacenter

□ Infrastructure

□ Application-level

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____

APPLICATION NAME: ______________________________

Application Tier: *(select one)*

○ Tier 1 ○ Tier 2 ○ Tier 3 ○ Tier 4

Risk over Time:

Risk/Hour ($): ______________________________

Risk/Day ($): ______________________________

Risk/Week ($): ______________________________

Qualitative Impact:

____

____

____

Application Recovery Plan Summary:
High-level overview of the application recovery plan.

____

____

____

____

Data Sensitivity: *(select one)*

○ Compliant ○ Standard

Disaster Protection: *(check all that apply)*

□ Regional

□ Metro

□ Datacenter

□ Infrastructure

□ Application-level

Application Data:

____

____

____

Data Recovery Plan Summary: *How is the application data protected, and how will it be brought back?*

____

____

____

____