TOP 5 PITFALLS TO AVOID IN YOUR RESILIENCY STRATEGY AS YOUR BUSINESS ADOPTS THE CLOUD

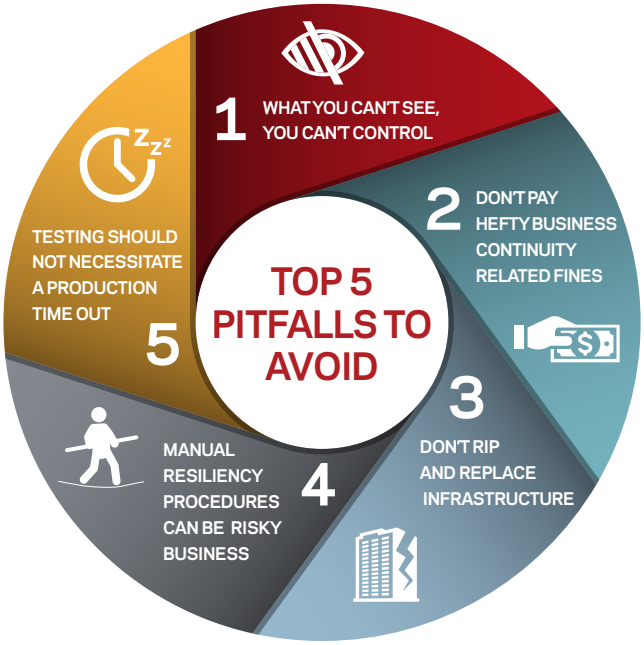
VERITAS

OVERVIEW

As your business adopts public, private or even hybrid clouds it is necessary to ensure that your business uptime doesn't get adversely affected. Done correctly, your resiliency strategy can be a critical differentiator for your business by helping to:

- Accelerate business growth by seamlessly integrating new and profitable technologies.
- Maintain uptime of essential services in the face of cyber-attacks, natural disasters, human error and more.
- Prove your business is compliant to required industry regulations

  Done poorly, it can be costly to your business by creating inefficiencies across teams, complexities of management, reduced visibility across dispersed business applications and more. Below are five critical pitfalls to avoid while building a resiliency plan as your business moves to the cloud.



---

1. WHAT YOU CAN'T SEE, YOU CAN'T CONTROL

As your organization adopts public, private or hybrid clouds, your business-critical applications get spread across a bigger and whole new landscape. Different teams across your organization may be adopting different cloud architectures, but without centralized and real-time visibility across all applications that are crucial to your organization, can you control your business uptime? According to Jason Buffington, ESG Sr. Analyst, "Most of the challenges stemming from protecting virtualized environments still revolve around visibility".[1] Add in cloud to the mix now, and your visibility gets curtailed fast.

To keep your business running, you need to maintain control. And what you can't see, you can't control. Choose a resiliency strategy that gives you real-time visibility of your business health so you can stay informed as you make important business decisions. A bird's eye view of how business applications are meeting defined Service Level Objectives is as necessary as deep dive visibility into the various stages of your resiliency procedures. For example, how things are proceeding during a failover or failback operation.

2. DON'T PAY HEFTY BUSINESS CONTINUITY RELATED FINES

Imagine having to pay millions of dollars in fines to regulators if you err in your business continuity implementation. In late 2014 the Financial Conduct Authority (FCA) **fined global banks 42 Million Pounds** for IT failures. If you are in banking, healthcare or even government industries, you are regularly required to provide proof of implemented resiliency strategies, data security and sovereignty, disaster recovery testing and more. Laws such as the FCA, Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Act (FISMA), National Institute of Standards and Technology (NIST), Federal Financial Institutions Examination Council (FFIEC), Basel II, and Expedited Funds Availability (EFA) Act among others mandate requirements that your business needs to comply to.

As you plan your resiliency strategy, keep in mind explicit as well as implicit requirements within these regulations. If you are consuming a hosted private cloud or a public cloud, do you know where your data is and if you are compliant? Can you failback to your production site seamlessly? Can you prove that you can effectively recover within a stipulated timeframe? You need to ensure you have multi-site visibility along with regular, automated reporting of your business health, disaster recovery strategy and disaster recovery testing to keep your auditors satisfied.

3. DON'T RIP AND REPLACE INFRASTRUCTURE

It's a known fact that the only constant is change. This is true for your organization too. You've moved from physical to virtualization and are now adopting cloud. But how do you transform your business for the future, without throwing out what you already have and going on expensive multi-million dollar shopping sprees?

It's important to deploy a resiliency strategy that will scale and grow as your business grows. You shouldn't have to rip out and replace your existing infrastructure, your underlying availability solutions, data movers or virtualization platforms as you move to the cloud just to support new resiliency procedures. The more technologies your resiliency strategy adapts to, both legacy and forward looking, the greater cost savings and margins for your business.

4. MANUAL RESILIENCY PROCEDURES CAN BE RISKY BUSINESS

If your business continuity procedures are performed manually with reliance on spreadsheet tracking and scripts to start and stop applications, then you are leaving your business wide open to downtime risks. Human error can creep in and be fatal to your uptime. And in the event of a disaster your employees may not even be available to perform their required recovery duties.

Don't leave your business exposed to such risks especially as you move to the cloud. It's important to automate recovery for at least your Tier 0 and Tier 1 applications, if not at a site level. You need the assurance that you can failover and failback business-critical applications including multi-tier applications to and from the cloud, in a minimal amount of time.

5. TESTING SHOULD NOT NECESSITATE A PRODUCTION TIME OUT

A few years ago, calling in your employees to run disaster recovery tests over the weekend was just fine. But with end customers expecting businesses to be online at all times, downtime windows for testing are now minimal or even non-existent. You can't do away with testing your business resiliency strategy — in fact it's more important now than ever. So how do you ensure that your business-critical applications can recover in the event of unexpected downtime without reliance on a lot of employees and a time out from production?

Ensure that your resiliency strategy includes provisions to test recovery of your critical business applications in an automated fashion and without disrupting your production environments. And as Gartner advocates, "Test failback, not just failover, for at least mission-critical applications".[2]

COVER YOUR BASES ALWAYS WITH RESILIENCY PLATFORM FROM VERITAS

Yesterdays' approach to resiliency was complex and costly because of cumbersome manual recovery operations and reliance on multiple point products, and with organizations adopting cloud, IT environments are getting more complex and siloed. This causes reduced visibility, lack of control and increased unpredictability — a risky cocktail of ingredients when your customers expect that your business services be always on. Your resiliency approach needs to be re-defined to ensure your Service Level Objectives will be met.

Resiliency Platform from Veritas is a unified solution that helps you proactively maintain business uptime across your IT environments today and in the future as you innovate to adopt private, public and hybrid clouds. You get complete automation for all resiliency operations including failover and failback for a single virtual machine or application to your entire site. Recovery rehearsals are non-disruptive and can be run at any time from any place, making it easy for you to prove compliance to internal and external auditors. Additionally, Resiliency Platform safeguards your current technology investments by plugging into existing environments and its infrastructure and platform independence gives you the flexibility to innovate on your terms for the future. Say goodbye to old resiliency strategies and hello to Resiliency Platform from Veritas as you move to the cloud.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage.

1. Trends in Protecting Virtualized Environments, ESG Research Report, August 2015
2. Best Practices for IT Disaster Recovery: Reducing Risks On-site and In the Cloud, Werner Zurcher, December 2014 #G00271605

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (866) 837 4827
veritas.com

For specific country offices and contact numbers, please visit our website.
https://www.veritas.com/about/contact.html

V0257 7/16